UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROPUESTA DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE DISPOSITIVOS, COMUNICACIÓN Y PROTECCIÓN DE DATOS BASADA EN LA NORMA ISO/IEC 27001:2022 PARA AUXADI COSTA RICA, UBICADA EN SAN JOSÉ

MODALIDAD PROYECTO PARA OPTAR POR EL GRADO DE LICENCIATURA EN INGENIERÍA EN INFORMÁTICA CON ÉNFASIS EN GERENCIA

Allan Enrique Barquero Gómez

Noviembre, 2025

DEDICATORIA

Dedico este proyecto a mi madre, mi padre y mi hermana, pilares fundamentales en mi vida, por su apoyo incondicional, paciencia y confianza constante en mi capacidad para alcanzar cada meta. Gracias por acompañarme en cada paso de mi formación personal, profesional y académica, por alentarme en los momentos difíciles y celebrar conmigo cada logro. Su ejemplo, amor y fortaleza han sido la motivación que me impulsa a superarme y a continuar construyendo mi camino con determinación y gratitud.

AGRADECIMIENTOS

A la Universidad Internacional de las Américas (UIA), por brindarme las herramientas, el conocimiento y la orientación necesarias para hacer de este proyecto una realidad y cumplir una de mis metas académicas más importantes.

A mis compañeros y amigos de carrera, quienes con su apoyo, colaboración y compañerismo contribuyeron significativamente a mi crecimiento profesional y personal durante todo este proceso formativo.

A don David Jara Zúñiga, integrante del área de Tecnologías de la Información de Auxadi Costa Rica, por su disposición, apoyo técnico y colaboración durante el desarrollo de este proyecto, demostrando siempre compromiso y apertura.

Al profesor Fabián Mauricio Rodríguez Sibaja, por su acompañamiento como tutor de tesis, su orientación constante y por compartir sus conocimientos y experiencia, los cuales fueron fundamentales para la correcta ejecución de este trabajo de graduación.

CONTENIDO

Tablas

Figuras

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del Problema

Hoy en día la seguridad de la información se ha convertido en un aspecto fundamental para todas aquellas empresas que manejan datos confidenciales de clientes y diferentes procesos internos, este es el caso de Auxadi Costa Rica, una compañía que opera como centro de servicios contables y administrativos para clientes a nivel internacional, y que enfrenta posibles vulnerabilidades o riesgos relacionados con el manejo y protección de su información. Respecto al planteamiento del problema, Hernández, et al. (2014) mencionan que: “En realidad, plantear el problema no es sino afinar y estructurar más formalmente la idea de investigación” (p. 36), por lo tanto, esta etapa es clave para enfocar la investigación en los riesgos más relevantes.

Uno de los principales problemas que se han identificado es la dificultad para detectar amenazas, riesgos y vulnerabilidades dentro de la organización, sin este análisis no es posible tomar decisiones acertadas ni se pueden priorizar las mejores acciones para proteger la información. Otro punto bastante preocupante es la deficiencia en la implementación de controles de seguridad, debido a que no se ha realizado una evaluación previa que logre orientar qué tipo de controles aplicar y esta falta de preparación puede hacer que se tomen decisiones erróneas o poco efectivas.

También es importante destacar la falta de lineamientos institucionales claros, lo que genera un uso inconsistente de las herramientas y los protocolos de seguridad, por lo que todo esto causa confusión, deficiencias en los procesos y una mayor posibilidad de errores o fallos de seguridad. Además, la empresa no dispone de un estudio de factibilidad que le permita valorar si la implementación de una propuesta de seguridad puede ser viable a nivel financiero y técnico, esta incertidumbre puede dificultar mucho el compromiso institucional y frenar distintas iniciativas de mejora.

Se desea diseñar una propuesta de políticas y procedimientos de seguridad de la información basados en la norma ISO/IEC 27001:2022, adaptados a las particularidades de Auxadi

Costa Rica y que logren fortalecer la protección de los datos, mejorar los procesos internos y aumentar la confianza tanto del personal como de los clientes. Asimismo, Hernández, et al. (2017) señalan que: “Los elementos para plantear un problema son básicamente cuatro y están relacionados entre sí: los objetivos que persigue la investigación, las preguntas de investigación, la justificación, la viabilidad y las consecuencias del estudio” (p. 41), esto respalda la importancia de estructurar adecuadamente la investigación con el fin de justificar su relevancia.

Objetivos

Objetivo general.

Desarrollar una propuesta integral de políticas y procedimientos de seguridad de la información para la gestión de dispositivos, comunicación y protección de datos para Auxadi Costa Rica, basada en la norma ISO/IEC 27001:2022.

Objetivos específicos.

Analizar el estado de seguridad de la información en la gestión de dispositivos, seguridad en la comunicación y protección de datos, identificando vulnerabilidades y riesgos en la empresa según la norma ISO/IEC 27001:2022.

Seleccionar los controles de seguridad aplicables a la gestión de dispositivos, seguridad en la comunicación y protección de datos, de forma que se asegure su alineación con la norma ISO/IEC 27001:2022, el análisis de riesgos realizado y las necesidades específicas de la organización.

Diseñar una propuesta estructurada de políticas y procedimientos de seguridad según el análisis y selección previos, garantizando medidas efectivas para la gestión de dispositivos, la seguridad en la comunicación y la protección de datos según la norma ISO/IEC 27001:2022.

Evaluar la viabilidad económica y operativa de la propuesta basada en las buenas prácticas establecidas en la norma ISO/IEC 27001:2022, garantizando que su aplicabilidad y sostenibilidad se ajusten al contexto de la empresa.

Justificación

Proteger la información es una prioridad estratégica para cualquier empresa que maneje datos sensibles y procesos digitales, este es el caso de Auxadi Costa Rica, una organización que brinda servicios financieros y administrativos a distintas empresas, y que diariamente tiene que gestionar información crítica como transacciones contables, reportes fiscales, documentos internos y datos personales. En este contexto, proponer una solución basada en políticas y procedimientos de seguridad es fundamental para reforzar los controles existentes, reducir riesgos de exposición de datos y cumplir con las normativas vigentes.

En palabras de Lara (2011), “La mayoría de las investigaciones se efectúan con un propósito definido, no se hacen simplemente por capricho de una persona; y ese propósito debe ser lo suficientemente fuerte para que justifique su realización” (p. 63), esto refleja la intención que debe de tener un proyecto para generar un impacto positivo en el entorno. Además, esta propuesta tiene un valor social importante, ya que en un país como Costa Rica donde la transformación digital avanza rápidamente en todos los sectores, se hace necesario fomentar buenas prácticas en seguridad informática para ayudar a proteger derechos como la privacidad y la confidencialidad de la información, todo esto también fortalece una cultura organizacional ética, responsable y con beneficios que podrían ser replicables en otras empresas con necesidades similares.

El proyecto se basa en la norma ISO/IEC 27001:2022, la cual es reconocida a nivel internacional por su estructura completa para gestionar la seguridad de la información y esto permite desarrollar el trabajo bajo lineamientos sólidos como el análisis de riesgos, la documentación controlada y la mejora continua, además se incluirán herramientas prácticas que faciliten la implementación de controles, políticas definidas y la gestión de incidentes, garantizando que la propuesta tenga un impacto real en las operaciones de la empresa. Como

indican Hernández, et al. (2014), “Además de los objetivos y las preguntas de investigación, es necesario justificar el estudio mediante la exposición de sus razones” (p. 40), en este caso la investigación permite abordar las problemáticas relacionadas con la seguridad de la información y también ofrece un modelo que puede servir de referencia para otras organizaciones con características similares.

Viabilidad técnica.

Auxadi Costa Rica cuenta con una base tecnológica sólida que permite desarrollar este proyecto de forma eficiente y práctica, la empresa opera mediante una red de área local (LAN) que conecta alrededor de 30 computadoras portátiles distribuidas en distintas áreas. A nivel central, se utilizan 6 servidores físicos con respaldo y redundancia en la nube, donde se gestionan servicios como Active Directory, carpetas compartidas y otras funciones esenciales para las labores diarias, todos estos recursos tecnológicos constituyen un entorno donde es posible implementar soluciones de seguridad como firewalls, sistemas de detección de intrusos y herramientas de monitoreo y auditoría sin necesidad de realizar cambios estructurales.

No será necesario disponer de un espacio físico adicional para desarrollar esta investigación, ya que todas las mejoras propuestas se aplicarán directamente sobre la infraestructura tecnológica que Auxadi ya posee. Para llevar a cabo este proyecto, se utilizará una computadora personal con procesador Intel Core i7, 16 GB de memoria RAM y disco sólido de 512 GB, equipada con un paquete de ofimática, navegadores web e internet, herramientas que permitirán realizar el análisis, levantar información, diseñar controles y documentar todo lo necesario para cumplir los objetivos definidos.

Como lo señalan Hernández, et al. (2017), “es parte de la viabilidad de una investigación el tener acceso al lugar o contexto donde se realizará esta (por ejemplo, un laboratorio o simulador)” (p. 45), esta condición se cumple por completo, ya que el investigador tiene acceso directo al entorno de trabajo de Auxadi y al personal necesario para recolectar información. El equipo técnico de la empresa también será clave para validar accesos, revisar configuraciones y apoyar en la creación de las mejoras. Por tanto, la propuesta es técnicamente viable, ya que

aprovecha los recursos ya disponibles y se adapta fácilmente a la operación actual de la organización.

Viabilidad operativa.

Auxadi Costa Rica cuenta con una estructura organizacional clara y bien definida, en donde cada departamento tiene funciones específicas que permiten una operación eficiente, esta organización favorece la ejecución del proyecto y facilita la integración de nuevas políticas y procedimientos sin afectar el ritmo de trabajo. Es importante desatacar que el personal de Auxadi Costa Rica tiene experiencia en auditorías, aplicación de procedimientos internos y cumplimiento de normativas, lo que facilita la elaboración de una propuesta que sea realista y se encuentre ajustada al entorno de la organización. Además, la empresa promueve la mejora continua y ya posee una cultura adaptativa frente a cambios organizacionales.

En palabras de Hernández, et al. (2014), “tenemos que preguntarnos de manera realista si es posible llevar a cabo esta investigación” (p. 41), lo que lleva a valorar si el entorno en el que se desarrollará el estudio cuenta con los recursos y condiciones necesarias. En el caso de la organización, se dispone de una infraestructura sólida tanto a nivel humano como tecnológico, sumado a un equipo con experiencia, acceso a herramientas digitales, plataformas colaborativas y canales de comunicación efectivos. Todo esto crea un entorno favorable para ejecutar la propuesta de forma efectiva, permitiendo que el desarrollo del estudio se adapte a la operación diaria y que los resultados obtenidos reflejen con mayor precisión la realidad actual de la empresa.

Viabilidad económica.

Desde el punto de vista económico, el desarrollo de esta investigación es totalmente viable, ya que no implica costos directos para la empresa Auxadi Costa Rica. Las labores de análisis, recolección de información, diseño de controles y documentación técnica serán realizadas por el estudiante, sin requerir contratación de servicios externos ni inversión en personal adicional, por lo tanto, la colaboración del equipo interno de la empresa se limitará a brindar información clave y validaciones específicas. De acuerdo con Hernández, et al. (2017), este tipo de proyectos también

se fortalecen cuando existe apoyo institucional, respaldo técnico y participación activa de un equipo profesional, todos estos elementos aumentan su factibilidad y permiten superar desafíos propios de la ejecución.

Para la ejecución de estas actividades, se utilizará una computadora personal con las capacidades y el software necesarios, por lo que no será necesario adquirir herramientas adicionales y de requerirlo se utilizaran herramientas gratuitas con fines educativos. En términos generales no se prevé la necesidad de ningún gasto económico inmediato para la empresa, lo cual confirma la viabilidad financiera del desarrollo de la propuesta.

Cabe aclarar que la presente viabilidad económica se refiere únicamente al desarrollo del trabajo teórico y técnico, en caso de que la empresa decida implementar las políticas y controles de la propuesta, se realizará un análisis económico y operativo por separado que contemplará posibles costos de licencias, infraestructura adicional, capacitaciones especializadas u otros. Dicha evaluación se abordará posteriormente como parte del mismo proyecto y según los resultados obtenidos en esta investigación.

Viabilidad legal.

Desde la perspectiva legal, la propuesta es viable dentro del marco normativo costarricense. Su respaldo técnico, basado en la norma ISO/IEC 27001:2022, se alinea con los principios establecidos en la Ley N.° 8968 “Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales”, que regula aspectos como la confidencialidad, el acceso controlado, la integridad de los datos y la responsabilidad institucional, además esta normativa reconoce el derecho de las personas a controlar el uso de su información y exige a las organizaciones garantizar su resguardo, tal como menciona Asamblea Legislativa de Costa Rica (2011).

La creación de políticas documentadas para el manejo seguro de la información es una respuesta directa a los requisitos legales actuales, fortalece el compromiso de la empresa con el cumplimiento normativo y brinda soporte ante posibles auditorías o inspecciones, ya que al contar con controles claros se asegura la trazabilidad y el uso ético de los datos. De forma complementaria

Asamblea Legislativa de Costa Rica (2001) dicta que, la legislación penal costarricense sanciona conductas que atenten contra los sistemas informáticos, lo que refuerza la importancia de establecer mecanismos preventivos como los que se proponen en este proyecto. En este sentido, el proyecto cumple con la normativa vigente y actúa como una herramienta proactiva que refuerza la estructura legal y operativa de la organización.

Proyecciones

Mehdi, et al. (2023) señalan que, “los alcances se basan en precisar hasta dónde quiere llegar el investigador con su estudio o el grado de profundidad” (p. 54), lo cual reafirma que una correcta definición de los alcances y proyecciones del estudio puede fortalecer la aplicabilidad de los resultados en entornos reales. Como resultado de esta investigación se espera entregar una propuesta sólida y aplicable de políticas y procedimientos de seguridad de la información, enfocada en proteger dispositivos, canales de comunicación y datos sensibles dentro de Auxadi Costa Rica, esta propuesta se basará en los lineamientos de la norma ISO/IEC 27001:2022, permitirá fortalecer la gestión de seguridad y promoverá una cultura organizacional más consciente de los riesgos tecnológicos.

La propuesta brindará a la empresa un conjunto de directrices formales que respalden sus operaciones, garanticen el cumplimiento normativo y reduzcan la exposición a amenazas internas y externas. A su vez, los controles bien definidos facilitarán el uso responsable de los diferentes activos tecnológicos y establecerán medidas claras para prevenir incidentes puedan llegar a afectar la confidencialidad, integridad o disponibilidad de la información.

También se generará una base documental útil para futuras auditorías internas o externas en materia de seguridad, así como para la planificación de nuevas iniciativas tecnológicas. En definitiva, esta propuesta aportará valor tanto a nivel técnico como estratégico, mejorando la gestión de riesgos, la toma de decisiones y la capacidad de respuesta ante situaciones críticas donde se vea comprometida la seguridad informática.

Alcance funcional.

Este proyecto se centrará en el desarrollo de políticas y procedimientos orientados a tres áreas clave dentro de Auxadi Costa Rica: la gestión de dispositivos, la seguridad en la comunicación y la protección de datos sensibles, estas acciones se diseñarán con base en la norma ISO/IEC 27001:2022, con el objetivo de analizar primeramente el ambiente actual y de esta manera poder reforzar la postura de seguridad de la empresa y establecer mejores prácticas en el uso de los activos de información. A partir del diagnóstico realizado, se analizarán y definirán propuestas concretas que aseguren el control del acceso a los dispositivos, el uso correcto de los canales de comunicación y la gestión segura de credenciales y datos críticos, además esta propuesta estará adaptada al entorno operativo actual de modo que pueda implementarse de forma progresiva sin afectar la continuidad del negocio.

Se establecerán lineamientos claros para el uso y resguardo de los equipos tecnológicos, aplicando controles preventivos que minimicen los riesgos, también se crearán procedimientos para garantizar la transmisión segura de la información y proteger los medios de comunicación corporativos frente a posibles vulnerabilidades como fugas de datos. Por último, se reforzará el manejo de contraseñas y privilegios de acceso, asegurando que la información sensible esté protegida adecuadamente. Además, el objetivo de esta propuesta no es solo mitigar vulnerabilidades, sino también promover una cultura organizacional enfocada en la seguridad de la información, todos los lineamientos estarán redactados de forma clara y técnica, listos para ser utilizados en auditorías internas o como base para futuros procesos de certificación.

Tabla 1

Descripción del alcance funcional.

Problema	Descripción	Apartado	Descripción del apartado
Dificultad para identificar riesgos, amenazas y vulnerabilidades en la gestión de dispositivos, seguridad de comunicación y protección datos	La falta de un análisis estructurado de riesgos en la gestión de dispositivos, la comunicación y la protección de datos impide una adecuada toma de decisiones y aplicación de controles, generando una gestión reactiva en lugar de preventiva.	1.1 Identificación y clasificación de activos críticos. 1.2 Evaluación de políticas y controles existentes. 1.3 Diagnóstico de riesgos a través de	En los apartados se analizará la seguridad de la información en la gestión de dispositivos, seguridad en la comunicación y protección de datos, y se considerarán los 4 dominios de la norma ISO/IEC 27001:2022: organizativos (5.5, 5.9, 5.15, 5.25, 5.31), personas (6.8), físicos (7.7, 7.10, 7.14) y tecnológicos (8.16): 1.1 Se aplicará una evaluación documental y entrevistas con responsables de TI para identificar

		encuestas a personal clave. 1.4 Evaluación del control de accesos y gestión de usuarios. 1.5 Análisis de cumplimiento normativo y regulaciones locales. 1.6 Análisis de reportes históricos de incidentes.	los activos de información más críticos y su nivel de protección para crear un inventario clasificado de activos con criterios de criticidad. 1.2 Se realizará una auditoría documental mediante listas de verificación y comparación con los requisitos de la norma ISO 27001 para identificar brechas y oportunidades de mejora, con el fin de generar un informe de cumplimiento y desviaciones. 1.3 Se aplicarán encuestas estructuradas a empleados clave para evaluar la percepción sobre riesgos y nivel de cumplimiento de buenas prácticas. Los resultados se analizarán mediante métodos estadísticos y categorización de riesgos, y se entregará un informe basado en gráficas y clasificación de riesgos por impacto y probabilidad. 1.4 Mediante entrevistas con el personal de TI y revisión documental de registros de accesos, se evaluará cómo se administran credenciales y autorizaciones para crear una matriz de control de accesos y permisos. 1.5 Se revisará la alineación de la empresa con normativas locales de protección de datos y seguridad de la información, utilizando listas de verificación, con el fin de generar un informe de cumplimiento regulatorio. 1.6 Se analizarán registros de incidentes de seguridad anteriores mediante revisión documental para identificar patrones de vulnerabilidad y áreas críticas de mejora, y se entregará un resumen de patrones de amenazas y riesgos identificados con recomendaciones.
Deficiencias en la implementación de controles de seguridad, derivadas de una falta de evaluación previa en la gestión de dispositivos, comunicación y protección de datos.	La empresa no cuenta con un proceso formal para seleccionar controles de seguridad en dispositivos, comunicación y datos, lo que incrementa la vulnerabilidad ante amenazas cibernéticas.	2.1 Priorización de riesgos basada en la matriz de impacto y probabilidad. 2.2 Análisis de correlación entre vulnerabilidades y controles ISO 27001. 2.3 Justificación de controles mediante entrevistas con expertos de seguridad. 2.4 Factibilidad técnica y organizacional de los controles.	En los apartados se determinarán los controles de seguridad apropiados, priorizando riesgos y evaluando su aplicabilidad dentro del contexto empresarial, y se considerarán 2 dominios de la norma ISO/IEC 27001:2022: organizativos (5.18, 5.21) y personas (6.5): 2.1 Se aplicará una matriz de riesgos basada en la información recolectada en el diagnóstico para categorizar los riesgos más críticos y justificar la selección de controles para crear un ranking de riesgos por impacto y probabilidad. 2.2 Se realizará un análisis comparativo entre los riesgos identificados y los controles de seguridad disponibles en ISO 27001, seleccionando los más adecuados para mitigar cada vulnerabilidad, con el fin de generar una tabla de correlación riesgo-control. 2.3 Se realizarán entrevistas con responsables de TI o seguridad para validar la aplicabilidad de los controles elegidos y ajustar su implementación a las necesidades de la empresa y se entregará un documento de validación y ajustes recomendados.

			2.4 Se evaluará la capacidad actual de la empresa para adoptar los controles seleccionados, considerando restricciones tecnológicas, capacitación del personal y cambios en procesos internos para crear un análisis detallado de viabilidad técnica y organizacional con posibles estrategias de adaptación.
Uso inconsistente de medidas de seguridad debido a la falta de lineamientos claros en la gestión de dispositivos, comunicación y datos.	La empresa no cuenta con políticas y procedimientos formalizados que regulen la gestión de dispositivos, la seguridad en la comunicación y la protección de datos. Esto dificulta la aplicación de medidas efectivas y consistentes a nivel organizacional.	3.1 Propuesta de políticas y procedimientos para la gestión de dispositivos. 3.2 Propuesta de políticas y procedimientos para la seguridad en la comunicación. 3.3 Propuesta de políticas y procedimientos para la protección de datos y gestión de credenciales.	En los apartados se diseñará la propuesta de políticas y procedimientos basados en los hallazgos previos en los ámbitos de gestión de dispositivos, comunicación segura y protección de datos, y se considerarán los 4 dominios de la norma ISO/IEC 27001:2022: organizativos (5.1, 5.14, 5.23), personas (6.3, 6.7), físicos (7.7, 7.10 y 7.14) y tecnológicos (8.1, 8.5, 8.7, 8.13, 8.22, 8.23): 3.1 Se diseñará una propuesta de políticas y procedimientos para la gestión de dispositivos con el objetivo de mitigar riesgos asociados a su manejo. Estas normativas estarán fundamentadas en los hallazgos obtenidos en la evaluación de riesgos y en la selección de controles de seguridad. 3.2 Se creará una propuesta de políticas y procedimientos para garantizar la integridad, confidencialidad y disponibilidad de la información en la seguridad en la comunicación. Estas medidas se definirán con base en el análisis de riesgos y la correlación entre vulnerabilidades y controles identificados en fases previas de la investigación. 3.3 Se desarrollarán políticas y procedimientos para la protección de datos sensibles y la gestión segura de credenciales. La estructura de estas normativas estará sustentada en el análisis de riesgos y en los controles de seguridad identificados como necesarios para la empresa.
Incertidumbre sobre la factibilidad de la propuesta de seguridad debido a la ausencia de un análisis detallado de costos, beneficios y operatividad.	No se ha realizado una evaluación formal sobre los costos y beneficios de la implementación de las medidas de seguridad, lo que genera incertidumbre en cuanto a su aplicabilidad dentro del contexto financiero y operativo de la empresa.	4.1 Evaluación de costos y recursos para la implementación 4.2 Justificación de beneficios de la propuesta	En los apartados se evaluará la sostenibilidad de la propuesta, considerando costos, recursos disponibles y beneficios en términos de seguridad organizacional, y se considerarán 2 dominios de la norma ISO/IEC 27001:2022: organizativos (5.5) y tecnológicos (8.13): 4.1 Se analizarán costos y disponibilidad de recursos financieros, tecnológicos y humanos mediante entrevistas a gerentes y revisión de presupuestos internos para crear un análisis detallado de costos y recursos con estrategias de optimización. 4.2 Se evaluarán los beneficios esperados en términos de reducción de incidentes de seguridad, alineación con estándares internacionales y mejoras operativas mediante encuestas a directivos y modelos de predicción de ahorro, con el fin de generar un informe de impacto y rentabilidad de la propuesta.

Fuente: Elaboración propia

Alcance metodológico.

La propuesta se desarrolla bajo un enfoque metodológico cuantitativo, centrado en recolectar y analizar información relevante sobre la seguridad de la información en Auxadi Costa Rica. El proceso inicia con un análisis documental de la norma ISO/IEC 27001:2022, con el cual se podrá identificar los controles aplicables que permitan abordar los riesgos existentes, además se revisan las políticas internas y prácticas actuales de la empresa, lo que permite detectar debilidades y oportunidades de mejora. Como técnicas principales se utilizarán diferentes tipos de análisis, diagnósticos y cuestionarios estructuradas a los responsables del área de TI, todo esto con el fin de conocer el entorno operativo, identificar los diferentes riesgos y evaluar los mecanismos de seguridad implementados.

Los datos recopilados para el análisis, la selección de controles y el diseño de la propuesta se organizan según los dominios de la norma ISO/IEC 27001:2022, priorizando aquellos relacionados con dispositivos, comunicación y gestión de credenciales. Cabe destacar que este trabajo se enfoca únicamente en el diseño de una propuesta y documentación de las soluciones, brindando una guía clara y alineada con las mejores prácticas internacionales, sin contemplar su ejecución directa.

Alcance tecnológico.

Esta propuesta se apoya en herramientas tecnológicas que permiten tanto la recopilación de información como la elaboración de los documentos técnicos. Para el análisis normativo se utilizaron fuentes digitales confiables, incluyendo versiones oficiales de la norma ISO/IEC 27001:2022, con el fin de asegurar que la propuesta esté alineada con estándares internacionales aplicables. A nivel de equipo, es necesario una computadora con sistema operativo Windows 10 o superior y el paquete Office 365, esenciales para redactar, organizar y presentar el contenido del proyecto, además de servicios de almacenamiento en la nube como Google Drive para respaldar y dar seguimiento constante a la información durante el desarrollo de la investigación.

También herramientas tecnológicas que podrían ser aprovechadas por Auxadi Costa Rica para fortalecer su seguridad, como soluciones de control de accesos, aplicaciones para cifrado de información, autenticación multifactor, sistemas de respaldo automatizado y otros, todas estas opciones siendo consideradas en función de su compatibilidad con la infraestructura ya existente en la empresa. En resumen, el uso adecuado de la tecnología es clave para estructurar una propuesta viable, basada en recursos accesibles y adaptada a las capacidades actuales de la organización.

CAPÍTULO II: MARCO REFERENCIAL

Enfoque Estratégico de la Seguridad de la Información en la Gestión Organizacional

Importancia de la Seguridad de la Información en Procesos Críticos Empresariales

Las organizaciones deben proteger sus activos digitales ante cualquier acción que pueda comprometer su funcionamiento o generar consecuencias legales, financieras o reputacionales. Hablar de seguridad informática es una necesidad estratégica en un entorno empresarial donde los servicios están altamente digitalizados y los procesos dependen de plataformas tecnológicas, desde esta perspectiva, Vega (2021) define la seguridad informática como:

> La seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Esta definición básicamente significa que debemos proteger nuestros datos y nuestros recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos. (p. 9).

Esta definición nos permite comprender que la seguridad de la información implica mantener el buen funcionamiento de todos los sistemas, proteger los accesos y evitar cualquier alteración que pueda afectar la calidad, exactitud o disponibilidad de la información. En organizaciones como Auxadi Costa Rica, donde el procesamiento de información contable y financiera es una actividad diaria y crítica, este enfoque se vuelve aún más importante, ya que cualquier incidente puede repercutir directamente en sus clientes y comprometer la calidad del servicio.

En este mismo sentido, Vega (2021) señala que “Tres de los conceptos principales en seguridad de la información son precisamente la confidencialidad, integridad y disponibilidad, comúnmente conocida como la tríada de la seguridad de la información” (p. 12), estos tres elementos constituyen los pilares sobre los cuales se construyen los esquemas de protección y control. Su adecuada implementación permite reducir significativamente los riesgos y establecer

una arquitectura segura capaz de adaptarse a los cambios tecnológicos y regulatorios que enfrenta las empresas.

Aplicar estos fundamentos dentro de la organización resulta esencial para mitigar vulnerabilidades, prevenir incidentes y asegurar la continuidad operativa. Es importante que las medidas de seguridad se integren de forma natural en la dinámica operativa y deben orientarse siempre a proteger los datos sensibles que circulan entre usuarios, plataformas y dispositivos, y sin afectar la eficiencia de los procesos internos ni el cumplimiento normativo.

Proteger el acceso a los datos es una de las prioridades en cualquier entorno corporativo, especialmente cuando se manejan activos digitales críticos, Roa (2013) afirma que "La confidencialidad intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas" (p. 15), por lo tanto, este principio debe garantizarse en todo momento para evitar fugas, manipulación o accesos indebidos a la información contable, financiera y administrativa. En el caso de Auxadi, este enfoque se debe reflejar en la implementación de controles ajustados a los perfiles de cada colaborador, lo que permite delimitar el uso de recursos según funciones específicas y fortalecer la protección de los datos sensibles sin comprometer la operatividad ni el cumplimiento interno.

Para que la información mantenga su valor operativo y estratégico dentro de una organización, es indispensable que se conserve completa, precisa y libre de alteraciones no autorizadas, Roa (2013) afirma que "El objetivo de la integridad es que los datos queden almacenados tal y como espera el usuario: que no sean alterados sin su consentimiento" (p. 15), esto implica que cualquier falla, ya sea técnica o humana, podría comprometer decisiones basadas en datos erróneos. En otras palabras, establecer rutinas de validación, copias de seguridad y control interno permitirá reducir las probabilidades de que la información sea modificada sin autorización, protegiendo así la base sobre la cual se fundamentan las decisiones estratégicas de la empresa.

Mantener los sistemas activos, accesibles y funcionales representa un factor decisivo para la continuidad de cualquier operación empresarial, según Roa (2013), "La disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido" (p. 15),

lo que cobra especial relevancia en un entorno como el de Auxadi, donde se manejan datos financieros sensibles y la puntualidad en la entrega de reportes es clave para cumplir con las obligaciones hacia los clientes. Por eso, resulta demasiado importante contar con planes de contingencia, sistemas de respaldo eficientes y una infraestructura capaz de soportar las cargas críticas sin interrupciones, garantizando así el acceso permanente a la información y evitando cualquier impacto negativo sobre la operatividad diaria.

A pesar de contar con principios bien definidos como la confidencialidad, integridad y disponibilidad, el entorno digital en el que operan las organizaciones está en constante riesgo debido a factores internos y externos que pueden comprometer estos pilares, es por ello por lo que resulta fundamental identificar y analizar todas aquellas condiciones que representen una amenaza potencial, ya que su materialización puede afectar directamente los procesos críticos y el acceso seguro a la información.

Gestión de Riesgos, Amenazas y Vulnerabilidades en el Entorno digital

Según Vega (2021), “esto es lo que es una amenaza, algo que tiene el potencial de causarnos daño. Las amenazas tienden a ser específicas de ciertos entornos, particularmente en el mundo de la seguridad de la información” (p. 17), este tipo de condiciones pueden surgir de factores tanto internos como externos y representan un punto clave en los análisis de riesgos, ya que exponen directamente la estabilidad operativa y la integridad de los activos de información. En entornos altamente digitalizados, como Auxadi Costa Rica, detectar estas amenazas de forma temprana permite diseñar respuestas específicas que disminuyan el riesgo de afectación sobre servicios críticos y que protejan la infraestructura tecnológica sobre la cual se sostienen sus operaciones contables y administrativas.

Estas violaciones pueden hacerse realidad sin necesidad de comprometer por completo el activo afectado, pero aun así pueden alterar alguna de las dimensiones sensibles como la confidencialidad, la integridad o la disponibilidad de la información. En este sentido, anticiparse a las amenazas es una necesidad estratégica para una organización que gestiona grandes volúmenes de datos financieros, también implementar mecanismos de monitoreo, auditoría continua y control

de acceso fortalece la postura de seguridad, protege la reputación de Auxadi y mejora su capacidad para cumplir con sus compromisos ante los clientes.

Vega (2021) menciona que, “Las vulnerabilidades son debilidades que pueden usarse para dañarnos. En esencia, son agujeros que pueden ser explotados por amenazas para causarnos daño” (p. 17), esto indica que las vulnerabilidades funcionan como brechas o puntos débiles que facilitan la materialización de una amenaza, ya sea por errores técnicos, fallas de configuración o falta de controles. En Auxadi, estas debilidades pueden comprometer datos críticos si no se identifican y corrigen a tiempo, por lo que su gestión se vuelve esencial para prevenir riesgos que afecten la estabilidad operativa y la confianza de los clientes.

Por lo tanto, la gestión de vulnerabilidades no debe verse únicamente como una práctica técnica, sino como parte de una estrategia preventiva de seguridad que involucra la revisión continua de sistemas, la aplicación de controles correctivos y la capacitación del recurso humano, todo esto permite reducir los puntos débiles antes de que sean aprovechados por agentes externos o por errores internos y refuerza la capacidad de la organización para responder de forma oportuna y efectiva ante cualquier intento de explotación que comprometa la continuidad de sus operaciones.

Baca (2016) explica que, “un ataque no intencionado es cuando un hecho perjudica a la información, a la TI o a la empresa sin que ocurra por las acciones intencionales de alguien” (p. 31), esto nos recuerda que no todas las afectaciones a la seguridad provienen de actores maliciosos, en muchos casos los incidentes son consecuencia de errores humanos, fallos técnicos o condiciones ambientales no previstas, lo que hace necesario considerar todos estos factores en el diseño de los planes de seguridad.

Este tipo de eventos puede presentarse mediante interrupciones eléctricas, fallas en equipos, errores de configuración o fenómenos naturales que alteren el funcionamiento normal de los sistemas. Por ello, es importante para las empresas contar con medidas preventivas que garanticen la continuidad de sus servicios críticos, como sistemas de respaldo eficientes,

protocolos de recuperación y pruebas periódicas de contingencia que minimicen el impacto de estas situaciones accidentales.

Además, reconocer la existencia de estos riesgos no intencionados permite adoptar un enfoque más completo de la seguridad, donde la preparación operativa y la capacidad de respuesta se convierten en factores clave para salvaguardar los procesos contables y administrativos. Este enfoque no solo fortalece los protocolos internos, sino que también promueve una cultura organizacional más enfocada en la prevención y en la identificación temprana de posibles escenarios adversos.

Baca (2016) señala que, "se consideran ataques intencionados los accesos no autorizados al sistema, donde el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, con el fin de robar información o alterar registros" (p. 31), a diferencia de los eventos accidentales, estos ataques son ejecutados con un objetivo claro y deliberado, ya sea comprometer la integridad de los datos, alterar procesos internos o sustraer información confidencial para obtener algún tipo de beneficio y por esta razón representan uno de los riesgos más críticos en los entornos tecnológicos actuales.

En el caso de Auxadi, una vulneración de este tipo podría afectar gravemente su operación debido a la sensibilidad de los datos que gestiona, aparte estos riesgos pueden originarse desde el exterior, a través de ciberataques, malware o phishing, pero también desde el interior, mediante el abuso de privilegios o el descuido de personal que desconozca las posibles amenazas. Ante este panorama resulta indispensable aplicar medidas contempladas en la norma ISO/IEC 27001:2022, como la segregación de funciones, la gestión de accesos, el monitoreo de actividades y la auditoría continua, que permitan reducir las oportunidades de explotación de los sistemas críticos y proteger la integridad de la información y el negocio. En conjunto con lo anterior, reforzar la vigilancia sobre los recursos tecnológicos permite detectar posibles amenazas en tiempo real y fortalece una cultura de seguridad donde cada colaborador comprende su rol dentro del sistema de protección, lo que reduce bastante la exposición al error humano y mejora la seguridad de toda la organización en general.

Infraestructura Organizacional y Tecnológica para la Seguridad de la Información

Implementación del SGSI como Base Estructural de la Seguridad

A medida que las organizaciones enfrentan amenazas más complejas y regulaciones más estrictas, se vuelve necesario adoptar marcos estructurados que permitan gestionar la seguridad de manera completa, en este contexto, los Sistemas de Gestión de la Seguridad de la Información (SGSI) surgen como una herramienta clave para garantizar la protección continua de los activos digitales, especialmente en empresas que manejan datos sensibles como Auxadi Costa Rica, según lo explican Samaniego y Ponce (2017):

> Un Sistema de Gestión de la Seguridad de la Información SGSI o en inglés Information Security Management System, ISMS, según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. (p. 75).

Esta definición resalta el carácter estratégico del SGSI, se trata de una serie de controles técnicos y también es un modelo de gestión que abarca la alta dirección y los procesos operativos. Implementar un SGSI bien estructurado representa una oportunidad para formalizar las políticas de seguridad, establecer responsabilidades claras y fortalecer la protección de los datos tanto internos como de los clientes de la empresa, además permite alinear la gestión de la seguridad con las exigencias legales del país, con las mejores prácticas internacionales y con los estándares que exige el trabajo con información financiera de alto valor.

Tal como indican Samaniego y Ponce (2017), el sistema permite “generar y aplicar planes de mejoramiento continuo en la gestión de la seguridad de la información” y “garantizar la continuidad y disponibilidad de las instituciones” (p. 76), Esto reafirma que la implementación de un SGSI busca proteger datos y establecer una cultura organizacional más centrada en el control, la prevención y la mejora constante. Su adopción permite conocer con mayor precisión el funcionamiento interno de la empresa, identificar amenazas y vulnerabilidades de forma estructurada, y aplicar mejoras respaldadas por evidencia.

Estas capacidades representan ventajas concretas que fortalecen su operación diaria, donde la formulación de políticas claras, junto con procedimientos bien definidos y controles ajustados al entorno permiten minimizar el impacto y aumentar la confianza de los clientes en la gestión de sus datos financieros. Además, los entornos son cada vez más regulado y el cumplimiento normativo se vuelve un factor vital para la sostenibilidad y resulta importante que las medidas de seguridad estén alineadas con la legislación vigente. Samaniego y Ponce (2017) señalan que este sistema ayuda a "cumplir con la legislación actual para la protección de datos, servicios de la sociedad, propiedad intelectual, comercio electrónico relacionados con la seguridad de la información" (p. 76), lo cual es algo crucial al manejar información confidencial sujeta a marcos legales.

En este marco, una gestión de seguridad realmente efectiva requiere identificar de forma continua las condiciones que pueden poner en riesgo los activos más críticos, es aquí donde el análisis de riesgos adquiere un papel central, ya que permite anticiparse a situaciones que podrían afectar tanto la operatividad como el cumplimiento normativo, esta práctica es clave para que las empresas puedan tomar decisiones informadas y ajustar sus estrategias de seguridad según el contexto tecnológico, legal y organizacional que enfrentan.

Condiciones Tecnológicas y Humanas para una Gestión de Riesgos Efectiva

Identificar y anticipar amenazas que puedan comprometer la operación de los sistemas y la integridad de los datos es una práctica esencial en organizaciones modernas que dependen de la tecnología, este proceso conocido como análisis de riesgos permite establecer políticas de seguridad ajustadas a las condiciones reales de cada entorno. Como lo indican Romero, et al. (2018), "La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma" (p. 13). Esto implica reconocer desde posibles ciberataques hasta errores humanos o fallas técnicas, los cuales pueden tener un impacto directo sobre la continuidad del negocio y deben ser gestionados con un enfoque preventivo y proactivo.

Una vez identificados los riesgos, resulta fundamental gestionarlos adecuadamente para reducir su impacto sobre los activos más sensibles. La administración de riesgos en seguridad informática no se limita a un diagnóstico inicial, sino que debe entenderse como un proceso continuo que evoluciona junto con las necesidades del negocio y las amenazas del entorno, según Baca (2016):

> Estas tres etapas (identificación, análisis y medidas para evitar y mitigar los efectos de los riesgos) constituyen la base de la llamada administración de riesgos en proyectos de seguridad informática, aunque con el paso del tiempo y la experiencia adquirida en la ejecución de miles de proyectos de este tipo, la administración de riesgos ha ido más allá de estas etapas iniciales básicas. (p. 24).

Esta perspectiva permite que las organizaciones puedan adoptar una postura más proactiva, donde los controles de seguridad se diseñan para responder a incidentes y se integran estratégicamente con sus procesos operativos y su infraestructura tecnológica. Gracias a ello, es posible asignar recursos de manera más eficiente, establecer prioridades claras y minimizar las interrupciones que puedan afectar tanto la productividad como la confianza del cliente, lo cual también fortalece el cumplimiento normativo y la toma de decisiones estratégicas basadas en evidencias reales.

Para que la gestión de riesgos sea verdaderamente efectiva se deben identificar las amenazas existentes, planificar controles y es necesario considerar todos los efectos colaterales que puedan llegar a surgir al implementar cambios en el entorno organizacional actual. La introducción de nuevas tecnologías, herramientas o metodologías sin una evaluación adecuada puede generar nuevas vulnerabilidades si no se gestiona correctamente el factor humano y el entorno técnico.

Se debe contemplar un análisis completo de los posibles riesgos tecnológicos que pueden surgir al introducir modificaciones en la infraestructura, los procesos o el personal. Este tipo de riesgos tiende a intensificarse cuando se aplican herramientas sin planificación, sin evaluar la compatibilidad con el entorno o sin preparar a los usuarios que deberán operarlas, lo que puede disminuir la efectividad de las medidas de seguridad establecidas.

Tal como lo indica Baca (2016), “Los riesgos de origen tecnológico; suelen ser cometidos por usuarios con muy poca experiencia, quienes no miden la magnitud de las consecuencias” (p. 24), lo cual evidencia la importancia de contar con procesos de capacitación claros y continuos. En el caso de Auxadi, esto implica garantizar que todos los controles definidos estén bien implementados desde el punto de vista técnico y también comprendidos y aplicados correctamente por quienes los utilizan a diario. Alinear la tecnología con la capacidad del recurso humano es esencial para evitar errores operativos y asegurar que las políticas de seguridad se apliquen de la mejor forma en toda la organización.

Una vez considerados los riesgos que pueden surgir por falta de preparación o por una mala implementación de controles, es necesario analizar cómo la infraestructura organizativa y tecnológica influye en la efectividad de las medidas de seguridad. La consistencia entre ambos componentes facilita la ejecución de los controles y también determina la flexibilidad operativa de la empresa ante posibles incidentes.

Un aspecto que suele ser determinante en el éxito de cualquier iniciativa de seguridad es el nivel de alineación entre la arquitectura organizacional y la tecnológica. En el caso de Auxadi, cualquier debilidad en estos elementos puede convertirse en una puerta de entrada para incidentes o vulnerabilidades graves que comprometan la integridad de los datos o la disponibilidad de los servicios.

Romero, et al. (2018) advierten que, “la infraestructura puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan.” (p. 14). Por esta razón, antes de aplicar cualquier propuesta relacionada con la norma ISO/IEC 27001:2022, se debe revisar cuidadosamente su modelo de operación y su infraestructura tecnológica actual, esto incluye identificar brechas, validar compatibilidades y asegurar que los nuevos controles puedan integrarse de forma efectiva sin afectar la dinámica del trabajo diario. Además, la estructura organizativa debe tener la flexibilidad suficiente para responder a cambios normativos o tecnológicos sin comprometer la continuidad de los servicios ni la protección de la información sensible.

La Norma ISO/IEC 27001:2022 como Marco Integral de Gestión de la Seguridad

Fundamentos y Estructura General de la Norma ISO/IEC 27001:2022

La norma ISO/IEC 27001:2022 se reconoce globalmente como el estándar más completo para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) y su propósito principal es permitir que las organizaciones gestionen riesgos de manera sistemática, estructurada y adaptada a sus necesidades internas, integrando la seguridad como parte fundamental de su funcionamiento operativo, según ISO (2022), esta norma "proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información" (p. 2), esto refleja que se trata de un sistema completo que se integra con todos los procesos de la organización. Ademas, la norma se estructura con base en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), promoviendo así la mejora continua en todos los niveles de gestión.

Este enfoque se traduce en una estructura normativa que incluye 10 cláusulas principales y un Anexo A que agrupa 93 controles divididos por dominios, los cuales abarcan desde aspectos organizativos hasta tecnológicos, ISO (2022) enfatiza que, "es importante que el sistema de gestión de la seguridad de la información se tenga en cuenta en el diseño de los procesos, los sistemas de información y los controles" (p. 2), destacando que la seguridad debe estar integrada desde la creación misma de la infraestructura empresarial. También en palabras de ISO (2022), esta versión "mantiene la compatibilidad con otros estándares de sistemas de gestión que han adoptado el Anexo" (p. 2), lo cual facilita su integración con otros modelos y se vuelve clave para organizaciones que gestionan múltiples normas.

Implementar esta norma permite fortalecer los mecanismos de protección de datos, responder a exigencias regulatorias nacionales e internacionales, y al mismo tiempo ofrecer mayor confianza a los clientes y partes interesadas. Este enfoque además ayuda a gestionar riesgos tecnológicos, favorece la estandarización de procesos, mejora la eficiencia operativa y proyecta una imagen institucional sólida y comprometida con la seguridad de la información.

Dado el enfoque estructurado que propone la norma, se vuelve fundamental no solo comprender sus principios generales, sino también aplicarlos de forma concreta en áreas específicas que respondan a las necesidades del entorno organizacional. En el caso de esta propuesta, se partirá de un análisis detallado de la situación actual en Auxadi Costa Rica con el fin de orientar la aplicación efectiva de los controles más pertinentes, esto permite que la gestión de la seguridad esté directamente alineada con las prioridades estratégicas de la empresa.

Los elementos identificados en la tabla de la descripción del alcance funcional permiten priorizar áreas críticas que requieren atención, y por ello se ha definido un marco claro que guiará la selección de los controles más relevantes para esta propuesta, se han organizado según tres ejes fundamentales, que serían la gestión adecuada de los dispositivos tecnológicos, la protección de datos sensibles y la implementación de canales de comunicación seguros, los cuales reflejan los principales riesgos y necesidades operativas de la empresa.

La norma ISO/IEC 27001:2022 proporciona una base sólida para esta estructuración gracias a su Anexo A, que contiene un conjunto amplio y detallado de controles divididos en dominios que abarcan aspectos organizacionales, físicos, tecnológicos y relacionados con el recurso humano. ISO (2022) resalta que, “es importante que el sistema de gestión de la seguridad de la información se tenga en cuenta en el diseño de los procesos, los sistemas de información y los controles” (p. 2), lo cual respalda el enfoque adoptado en esta propuesta, ya que cada grupo de controles será analizado considerando su integración con los procesos reales y con el entorno tecnológico actual de Auxadi.

Controles Organizacionales para la Gestión Estratégica de la Seguridad

La gestión organizacional de la seguridad requiere un conjunto de controles que permitan establecer reglas claras, responsabilidades y mecanismos de supervisión acordes al contexto y las necesidades de cada empresa. En el caso de Auxadi Costa Rica, se han identificado una serie de controles organizativos del Anexo A de la norma ISO/IEC 27001:2022 que resultan claves para fortalecer su sistema de gestión de la seguridad.

Para establecer una base sólida en la gestión de la seguridad de la información es esencial contar con lineamientos claros que sirvan como guía para toda la organización. En este sentido, uno de los controles fundamentales es la definición y aprobación de políticas de seguridad, según ISO (2022), “la política de seguridad de la información y las políticas específicas del tema serán definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante” (p. 15), lo que permite establecer criterios unificados para la protección de los recursos informáticos, además esta política debe ir acompañada de una correcta gestión para evitar accesos indebidos. En esa línea, ISO (2022) establece que, “las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán” (p. 17), permitiendo que los permisos o accesos se asignen en función de los roles y necesidades específicas de la empresa.

Para que las políticas y controles definidos realmente tengan un impacto efectivo es necesario que toda la organización comprenda su propósito y alcance, no basta con definir reglas y procedimientos, también es esencial fomentar una cultura de seguridad basada en la responsabilidad compartida. Controles como la gestión de accesos o el uso de servicios en la nube deben estar acompañados por una comunicación clara hacia el personal, donde se expliquen los riesgos asociados a su incumplimiento y la forma correcta de aplicar las medidas, esto mejora el cumplimiento y fortalece el compromiso del equipo con la protección de los activos digitales.

Una vez establecidos los criterios de acceso, también es necesario controlar el ciclo de vida de los derechos otorgados a los usuarios. ISO (2022) especifica que, “los derechos de acceso a la información y otros activos asociados se aprovisionarán, revisarán, modificarán y eliminarán de acuerdo con la política” (p. 17), asegurando así que los privilegios se mantengan actualizados ante cambios de funciones, rotación de personal o desvinculaciones yesta gestión se complementa con el mantenimiento de un inventario actualizado de los activos informáticos. ISO (2022) indica que “se elaborará y mantendrá un inventario de la información y otros activos asociados, incluidos los propietarios” (p. 16), lo cual brinda visibilidad sobre los recursos tecnológicos críticos y sus responsables, permitiendo una supervisión más eficiente y centralizada.

La capacidad de integrar nuevos servicios o modificar la infraestructura tecnológica sin comprometer la seguridad se vuelve una ventaja estratégica en entornos corporativos como el de Auxadi, donde existe una dependencia creciente de herramientas digitales. La norma ISO/IEC 27001:2022 permite adaptar los controles de seguridad a contextos específicos y en constante evolución, además refuerza la continuidad operativa y alinea la seguridad con los objetivos del negocio.

ISO (2022) señala que, “las reglas, procedimientos o acuerdos de transferencia de información deben estar en su lugar para todos los tipos de instalaciones de transferencia” (p. 17), lo cual resulta indispensable para evitar que la integridad o confidencialidad de los datos se vea comprometida durante su transmisión, ya sea por canales internos o externos, este control se vincula también con el uso de servicios en la nube, los cuales deben estar sujetos a requisitos de seguridad bien definidos. En palabras de ISO (2022), “los procesos de adquisición, uso, gestión y salida de los servicios en la nube se establecerán de acuerdo con los requisitos de seguridad de la información de la organización” (p. 18), permitiendo así que estas tecnologías se integren a la infraestructura organizacional sin poner en riesgo los datos.

Para garantizar la eficacia de estos mecanismos, es crucial que las plataformas utilizadas para la transferencia o almacenamiento de información estén alineadas con los controles definidos en la política interna, todo esto implica creae acuerdos formales con los proveedores de servicios en la nube y realizar evaluaciones periódicas sobre el cumplimiento de los requisitos de seguridad establecidos. También se deben definir criterios técnicos y contractuales que regulen cómo se manejarán los datos en cada etapa de su ciclo de vida y así asegurar que los procesos de migración, respaldo o eliminación de información se ejecuten bajo parámetros controlados y auditables.

En un entorno como el de Auxadi, existen relaciones con múltiples proveedores de tecnología y se vuelve imprescindible gestionar adecuadamente la seguridad en la cadena de suministro. ISO (2022) establece que, “se definirán y aplicarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC” (p. 18), de modo que se debe asegurar que los terceros cumplan con estándares similares de protección y este enfoque se complementa con la necesidad de mantener

contacto constante con las autoridades pertinentes, según ISO (2022), “la organización debe establecer y mantener contacto con las autoridades pertinentes” (p. 15), lo cual resulta especialmente útil en la búsqueda de alineación con las recomendaciones de organismos como el MICITT en Costa Rica.

Además, es importante destacar que la gestión de riesgos no solo se refiere a lo que ocurre dentro de la organización, sino también a lo que sucede en su entorno extendido. La cadena de suministro TIC representa uno de los puntos más vulnerables, ya que cualquier proveedor puede convertirse en un vector de amenaza si no se aplican controles adecuados. Por ello, mantener canales abiertos con las autoridades pertinentes y establecer cláusulas de seguridad en los contratos con terceros se vuelve una estrategia con la cual se anticipan posibles incidentes externos y se genera evidencia de cumplimiento ante auditorías o revisiones regulatorias.

Controles Relacionados con el Personal y la Cultura de Seguridad

Asimismo, una buena gestión de la seguridad requiere capacidad de respuesta ante eventos inesperados, por lo que ISO (2022) indica que, “la organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes” (p. 18), lo cual permite activar protocolos formales que minimicen los daños operativos y reputacionales. Todo este entorno de control debe enmarcarse en el cumplimiento de la normativa vigente. ISO (2022) resalta que deben “identificarse, documentarse y mantenerse actualizados” los requisitos legales y contractuales aplicables a la seguridad de la información (p. 19), en Costa Rica esto implica adecuarse a leyes como la Ley N.º 8968 de protección de datos personales, entre otras disposiciones que regulan el manejo responsable de la información.

La protección de la información depende también del comportamiento, el compromiso y las acciones del personal. Por ello, los controles orientados a las personas desempeñan un papel fundamental dentro del Sistema de Gestión de Seguridad de la Información (SGSI). En el caso de Auxadi Costa Rica, los controles del Anexo A de la norma ISO/IEC 27001:2022 que se relacionan con el recurso humano resultan esenciales para establecer una cultura organizacional consciente,

prevenir errores operativos y garantizar que cada colaborador contribuya activamente a la protección de los activos de información.

La gestión de la seguridad desde el factor humano implica capacitar al personal y también garantizar que los lineamientos de seguridad estén claramente definidos desde su incorporación. En esta línea, es fundamental establecer programas de formación continua que fortalezcan el conocimiento y la conciencia sobre amenazas actuales, ISO (2022) establece que, "el personal de la organización y las partes interesadas pertinentes recibirán concienciación, educación y capacitación apropiadas sobre seguridad de la información" (p. 20), lo que garantiza una base sólida de conocimiento en todos los niveles de la empresa, además esta medida se vuelve aún más importante en entornos de trabajo híbridos o remotos donde los riesgos se amplifican. Por eso, también se debe implementar protección adicional cuando los empleados se conectan fuera del perímetro corporativo, tal como señala ISO (2022), "las medidas de seguridad se implementarán cuando el personal trabaje de forma remota" (p. 21), lo cual obliga a establecer controles como el uso de VPN, autenticación multifactor y políticas estrictas para dispositivos personales.

Una cultura de seguridad eficaz se construye a partir del fortalecimiento constante de las buenas prácticas en el entorno laboral, incluyendo aquellos escenarios que escapan al control tradicional, el trabajo remoto ha modificado las dinámicas operativas de muchas organizaciones como Auxadi Costa Rica, por lo que se requiere mayor responsabilidad individual y supervisión tecnológica, este contexto exige que la seguridad dependa también de comportamientos informados y conscientes. Invertir en capacitación y establecer controles remotos adecuados permite disminuir la superficie de ataque y mejorar la postura defensiva general de la empresa.

Además de educar y proteger a los usuarios durante su actividad en la organización, es crucial establecer mecanismos seguros para cuando su vínculo finaliza o cambia. La norma ISO/IEC 27001:2022 indica que, "las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o cambio de empleo se definirán, harán cumplir y comunicarán" (p. 20), de manera que se asegure una salida ordenada que no comprometa la información institucional, esta gestión se complementa con la existencia de canales apropiados para que el personal reporte incidentes o comportamientos sospechosos, según ISO (2022), "la

organización debe proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados de manera oportuna" (p. 21), lo cual permite activar medidas preventivas antes de que una amenaza se materialice.

El fortalecimiento del ciclo laboral en materia de seguridad debe contemplar tanto el inicio como el cierre de la relación con el colaborador, asegurando que en cada etapa existan controles efectivos y un entorno de confianza. El hecho de contar con mecanismos de reporte transparentes permite detectar irregularidades más rápido y demuestra el compromiso organizacional con la prevención y la mejora continua. Así, la gestión del recurso humano se convierte en una herramienta clave dentro del Sistema de Gestión de Seguridad de la Información (SGSI), al integrar a las personas como un componente activo y vigilante de la protección digital.

Controles Orientados a la Protección Física de la Información

La protección física es un componente esencial dentro del SGSI, ya que muchos riesgos pueden originarse por accesos no autorizados a espacios, dispositivos o soportes que contienen información crítica. En Auxadi Costa Rica, los controles físicos definidos en el Anexo A de la norma ISO/IEC 27001:2022 permiten minimizar las vulnerabilidades relacionadas con el entorno físico de trabajo, garantizando que los equipos, documentos y medios de almacenamiento se mantengan protegidos contra pérdidas, manipulaciones indebidas o exposiciones accidentales.

La protección física de la información es un componente esencial dentro del SGSI, ya que muchas veces se pasa por alto que la exposición de datos no siempre ocurre por medios digitales, sino también a través del entorno físico de trabajo. Por lo tanto, resulta necesario aplicar normas de escritorio limpio y pantalla clara, especialmente en oficinas compartidas o abiertas, donde documentos impresos o pantallas activas pueden quedar expuestas, ISO (2022) indica que, "se definirán y aplicarán adecuadamente normas de escritorio claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas" (p. 21), lo cual reduce significativamente el riesgo de accesos no autorizados por simple observación. Estas prácticas deben complementarse con una adecuada gestión de los medios de almacenamiento, como USB,

discos duros externos o unidades ópticas, según ISO (2022), “los medios de almacenamiento se gestionarán durante todo su ciclo de vida de adquisición, uso, transporte y eliminación” (p. 22), permitiendo así mantener el control de la información desde que se graba hasta que se elimina.

Este enfoque es especialmente útil en empresas como Auxadi Costa Rica, donde el manejo de información contable, financiera y de clientes se da tanto en entornos digitales como físicos. Establecer lineamientos claros sobre qué documentos pueden permanecer en el escritorio o cómo deben almacenarse medios portátiles fuera del horario laboral contribuye a reducir puntos ciegos en la protección de datos, además reforzar la supervisión sobre dispositivos móviles y establecer procesos documentados para su seguimiento garantiza que cada herramienta tecnológica utilizada tenga un control formalizado y se reduzcan los errores humanos.

Una vez que un equipo o medio de almacenamiento ha cumplido su ciclo de vida, es crucial asegurar que su retiro no represente un riesgo de fuga de información. Por ello, la eliminación segura o la reutilización del equipo debe seguir procedimientos estrictos. ISO (2022) establece que “los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que los datos confidenciales se hayan eliminado o sobrescrito de forma segura” (p. 22), lo cual implica que la organización debe implementar mecanismos automáticos o manuales de borrado seguro, así como validar que estos procesos hayan sido ejecutados correctamente, este control cobra mayor relevancia en entornos donde se hace rotación frecuente de equipos o se entregan dispositivos compartidos entre departamentos.

Asegurar la eliminación adecuada protege la información interna y garantiza el cumplimiento de normativas sobre protección de datos, algo especialmente sensible en servicios de carácter financiero y contable como los de Auxadi. Dejar rastros de datos en dispositivos reutilizados podría representar una vulnerabilidad crítica en una auditoría o una investigación de incidentes. Por ello, los procedimientos asociados a la baja de equipos deben estar estandarizados, registrados y validados por personal técnico capacitado, alineando así los recursos físicos con la estrategia general de seguridad de la información.

Controles Tecnológicos Aplicados a Dispositivos, Comunicación y Datos

La seguridad tecnológica constituye uno de los pilares más dinámicos dentro de la gestión de la información, ya que abarca la protección directa de sistemas, redes y dispositivos frente a amenazas cada vez más sofisticadas. Para Auxadi Costa Rica, los controles tecnológicos contemplados en el Anexo A de la norma ISO/IEC 27001:2022 son fundamentales para reforzar la infraestructura digital, garantizar la continuidad operativa y prevenir accesos o acciones no autorizadas sobre los sistemas que manejan datos sensibles o financieros.

La protección tecnológica de la información inicia desde los dispositivos que acceden a los sistemas corporativos y se vuelve prioritario aplicar controles sobre los dispositivos de punto final, como laptops, teléfonos o tablets, ISO (2022) señala que, "se protegerá la información almacenada, tratada o accesible a través de dispositivos de punto final de usuario" (p. 23), lo que implica medidas como cifrado, uso exclusivo de dispositivos autorizados, políticas de bloqueo automático y restricciones de instalación, estos controles se deben complementar con mecanismos de autenticación robusta que garanticen que solo personal autorizado acceda a los sistemas, ISO (2022) indica que "se utilizará la autenticación segura para verificar la identidad de los usuarios y dispositivos" (p. 24), promoviendo el uso de contraseñas fuertes, autenticación multifactor (MFA) y herramientas de gestión de identidades para reducir el riesgo de accesos indebidos.

Para Auxadi, esto representa un marco esencial para gestionar el trabajo híbrido o remoto, donde los dispositivos móviles forman parte del acceso cotidiano a sistemas críticos. La correcta configuración de estos puntos de entrada, sumado a la implementación de autenticaciones seguras, establece una primera línea de defensa frente a ataques dirigidos o robo de información, además esta combinación de controles reduce la superficie de ataque y mejora la trazabilidad de los accesos realizados desde distintos entornos tecnológicos.

Otro elemento central en la defensa tecnológica es la protección activa contra amenazas como virus, troyanos o spyware. ISO (2022) establece que "la protección contra el malware se implementará y estará respaldada por un conocimiento adecuado del usuario" (p. 23), lo que requiere la instalación de software de seguridad actualizado y también capacitar al personal en el

reconocimiento de archivos o enlaces sospechosos, esta defensa se vuelve más efectiva cuando se complementa con políticas de respaldo que aseguren la disponibilidad de los datos, ISO (2022) indica que, “las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente” (p. 23), garantizando así que ante un incidente de malware o pérdida accidental, la empresa pueda restaurar su operación sin afectar su continuidad ni la integridad de la información.

Este conjunto de medidas técnicas busca prevenir diferentes incidentes y garantizar la capacidad de recuperación de la información. En el contexto de Auxadi, donde se manejan datos contables y financieros sensibles, el respaldo constante de los sistemas y su prueba regular son prácticas que aseguran la continuidad operativa de la empresa y protegen la confianza de los clientes.

Un componente clave en la detección temprana de amenazas es la supervisión constante de los sistemas, ISO (2022) establece que, “se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos” (p. 24), lo que permite la implementación de herramientas de monitoreo, detección de intrusos y análisis de logs que alerten sobre posibles incidentes, esta vigilancia se ve fortalecida cuando la infraestructura tecnológica está correctamente segmentada, ISO (2022) señala que “los grupos de servicios de información, usuarios y sistemas de información se separarán en las redes de la organización” (p. 25), permitiendo así reducir el impacto de un posible ataque, al aislar áreas críticas y limitar los movimientos laterales dentro de la red interna.

La segregación de redes también permite establecer políticas diferenciadas según el tipo de usuario o sistema, haciendo más granular el control y disminuyendo el riesgo de exposición global. En organizaciones como Auxadi, esto se traduce en separar las distintas redes dentro de la empresa, aplicando reglas específicas a cada segmento y evitando accesos innecesarios de personas no autorizadas.

De igual forma, el acceso a internet debe ser controlado para reducir la exposición a amenazas externas, ISO (2022) indica que “el acceso a sitios web externos se gestionará para

reducir la exposición a contenidos maliciosos" (p. 25), lo cual puede lograrse a través de filtros de navegación, listas de sitios autorizados y sistemas de reputación web, este control debe estar alineado con la política de uso aceptable de tecnología dentro de la organización, bloqueando páginas de riesgo y reduciendo la probabilidad de infección a través de navegación no supervisada.

La aplicación de filtros web refuerza el entorno de seguridad tecnológica, especialmente cuando los colaboradores tienen acceso libre a internet durante su jornada, este tipo de control contribuye a aumentar la productividad y a reforzar los protocolos definidos en otros controles, consolidando así un ecosistema tecnológico más seguro y alineado con los objetivos estratégicos del negocio.

Gestión Segura de Dispositivos, Comunicaciones y Protección de Datos

Protección de Dispositivos y Continuidad Operativa

Actualmente los dispositivos digitales son herramientas esenciales para operar y almacenar información crítica, la gestión segura de estos recursos se convierte en un componente prioritario dentro de cualquier sistema de seguridad de la información, lo mismo ocurre con la protección de los canales de comunicación y los datos que circulan por ellos. En el caso de Auxadi Costa Rica, implementar políticas y controles robustos en torno al uso, acceso y resguardo de estos elementos es vital para garantizar la integridad de la operación contable y administrativa, minimizar riesgos de pérdida de información y cumplir con estándares internacionales como la norma ISO/IEC 27001:2022.

Una de las medidas fundamentales para asegurar el uso correcto de los dispositivos tecnológicos es establecer políticas claras sobre quién puede acceder, cómo se utilizan y qué nivel de privilegio es permitido según el rol de cada colaborador. En este sentido, el principio del menor privilegio es clave, ya que promueve la asignación de permisos estrictamente necesarios para cada función operativa. Como explica Samaniego y Ponce (2017), "si el sujeto no necesita acceso a un objeto para realizar su tarea, no debería tener derecho a acceder a ese objeto" (p. 7), esta regla ayuda a reducir significativamente las posibilidades de accesos no autorizados o manipulación de

datos fuera del alcance laboral asignado, estos controles deben aplicarse a computadoras portátiles, terminales, servidores o cualquier otro dispositivo donde se almacene o procese información sensible.

Además de restringir el acceso innecesario, también es importante garantizar que los sistemas dispongan de mecanismos para auditar su funcionamiento, hacer seguimiento a cambios importantes y mantener copias de seguridad actualizadas, todo esto permite anticiparse ante posibles incidentes que afecten la integridad, como virus o alteraciones no autorizadas. Por ello, una política efectiva debe contemplar el monitoreo de cambios en archivos, revisiones periódicas de registros de actividad y la correcta protección de los medios donde se almacenan los datos, con el fin de mantener su estado íntegro y verificable.

Proteger los dispositivos y garantizar la integridad de los datos no es suficiente si no se contemplan escenarios donde dichos controles puedan verse comprometidos. En un entorno donde las amenazas evolucionan constantemente y los sistemas pueden fallar por causas internas o externas, es indispensable que las organizaciones piensen en prevenir y también en cómo responder ante una eventual interrupción operativa, es aquí donde entra en juego la necesidad de complementar las políticas de seguridad con mecanismos de respuesta ante emergencias, garantizando así la seguridad en los procesos y la capacidad de recuperación ante eventos que afecten la continuidad del negocio.

Es fundamental que toda organización cuente con un plan de continuidad de negocio, ya que esto permite anticiparse a situaciones críticas y mantener la operatividad ante cualquier contingencia, como lo señala López (2017), se trata de un “plan desarrollado por la empresa ante situaciones de riesgo, necesario en toda empresa sin importar su fin, tamaño u objetivo, ni el costo que este implique” (p. 78), su implementación permite responder eficazmente cuando el flujo de información es interrumpido y es necesario proteger los procesos esenciales. Para lograrlo, el plan debe considerar aspectos como la identificación de consecuencias, la determinación de recursos tecnológicos y humanos necesarios, el diseño de simulacros, la contratación de servicios alternos y la asignación de responsables exclusivos ante emergencias.

Estos planes deben desarrollarse con base en un análisis riguroso de los riesgos más críticos para la organización, considerando tanto causas lógicas como físicas y evaluando las consecuencias que podrían comprometer la operación. Para que la respuesta sea efectiva, es necesario definir qué procesos deben restablecerse primero y establecer procedimientos prácticos que aseguren una reactivación rápida y ordenada. En el caso de una empresa como Auxadi, esto implica tener claridad sobre qué sistemas contables, plataformas de comunicación o bases de datos deben priorizarse en un escenario de contingencia.

El éxito de cualquier estrategia de continuidad y recuperación depende del compromiso institucional con la prevención y la seguridad, como explica Baca (2016), “todos los subplanes deberán elaborarse de manera que estén alineados con la misión y la visión general de la organización” (p. 262), lo que implica que las acciones frente a una crisis deben integrarse en la cultura de la empresa y no verse como esfuerzos aislados. Desarrollar este tipo de enfoque cumple con las recomendaciones de la ISO/IEC 27001:2022 y representa una inversión estratégica para garantizar la estabilidad operativa, proteger la reputación organizacional y asegurar la confianza de los clientes ante cualquier eventualidad.

Por ello, no basta con contar con un plan estructurado en papel; es fundamental que este se complemente con medidas técnicas y operativas que aborden los canales por donde se transmiten y procesan los datos críticos. Uno de los más relevantes es el correo electrónico, herramienta ampliamente utilizada en Auxadi para la gestión administrativa y contable. Su uso constante lo convierte en un blanco habitual para los ciberdelincuentes, lo que obliga a la organización a considerar la seguridad de la comunicación digital como parte integral del sistema de continuidad del negocio.

Seguridad en Redes, Correo Electrónico y Canales de Comunicación

La seguridad lógica en las redes implica identificar y mitigar riesgos que pueden comprometer la integridad, confidencialidad y disponibilidad de la información. En el caso del correo electrónico, uno de los vectores más utilizados para atacar, destacan amenazas como el spam, la suplantación de identidad y los ataques por inyección de código. Roa (2013) advierte lo

siguiente del spam, “como mínimo, llevan publicidad, pero también son una fuente de infección de virus y troyanos que pueden venir en un fichero adjunto o que aprovechan una vulnerabilidad del programa de correo” (p. 200), situación que incrementa la vulnerabilidad ante engaños, pérdida de información y acceso no autorizado, este panorama representa un riesgo directo para organizaciones como Auxadi, donde el correo electrónico es esencial para la comunicación interna y externa.

Este tipo de amenazas afectan la recepción de mensajes no deseados y pueden ser el punto de entrada para ataques más sofisticados que se aprovechan de la confianza del sistema o del usuario. Cuando un mensaje logra evadir los controles básicos, es más probable que se generen acciones como la apertura de archivos adjuntos, el acceso a enlaces maliciosos o la entrega involuntaria de credenciales. En ese contexto, resulta importante que las organizaciones integren mecanismos de validación más estrictos, tanto a nivel de contenido como de origen, reforzando así la protección frente a intentos de manipulación más avanzados.

Además del spam, los ataques por suplantación de IP o por interceptación de datos representan serias amenazas en los entornos de red, Baca (2016) indica que la suplantación de IP “permite al atacante enviar paquetes de manera anónima” (p. 153). y esto hace que se burlen filtros como los del firewall, el mismo autor también menciona que “si la dirección IP de la computadora origen se ha suplantado, parecerá que el paquete ha sido enviado desde una computadora de la LAN y el firewall lo dejará pasar” (p. 154), es decir que esta técnica permite que un correo malicioso o un paquete contaminado llegue al usuario final sin ser detectado. Para mitigar esta situación, es fundamental implementar medidas como la segmentación de redes, listas blancas de IPs y autenticación de origen.

El avance y la sofisticación de las técnicas utilizadas por los ciberdelincuentes obliga a las organizaciones a anticiparse y fortalecer sus defensas más allá de los filtros convencionales, una sola brecha en los controles de red puede ser suficiente para comprometer toda una infraestructura conectada. Es necesario adoptar una visión integral de la seguridad que contemple también la vigilancia interna del tráfico, el control de accesos y la validación de cada componente que

participa en la transmisión de datos, especialmente en redes corporativas donde el flujo de información es constante y crítico para la operación.

Los atacantes también aprovechan herramientas como analizadores de paquetes para capturar información sensible transmitida por la red, especialmente si no está cifrada. En palabras de Vega (2021), “Un analizador de red o protocolo, también conocido como sniffer de paquetes, o simplemente sniffer, es una herramienta que puede interceptar el tráfico en una red” (p. 91), esta amenaza puede ser contenida mediante el uso de protocolos cifrados como TLS, así como con soluciones de detección de intrusos (IDS) capaces de monitorear y alertar sobre comportamientos sospechosos, todas estas herramientas deben configurarse de forma adecuada para que no solo detecten el tráfico malicioso, sino que trabajen en conjunto con firewalls y gateways seguros. En Auxadi, la aplicación de estos controles tecnológicos permitiría blindar los canales de comunicación digital frente a accesos no autorizados, cumpliendo con los principios de confidencialidad y disponibilidad definidos en la ISO 27001.

En definitiva, los riesgos asociados al correo electrónico y la transferencia de información no pueden subestimarse. La organización debe reconocer que los ataques muchas veces se aprovechan de brechas básicas o malas configuraciones, la implementación de una política de protección de datos que incluya cifrado, autenticación, filtrado y monitoreo continuo es indispensable para construir un entorno digital más confiable, seguro y alineado con las mejores prácticas internacionales en seguridad de la información.

Criptografía, Autenticación y Concienciación del Personal

Otro componente clave para lograr una gestión segura de dispositivos, comunicaciones y protección de datos es el uso adecuado de mecanismos criptográficos, controles de autenticación y esquemas de respuesta ante incidentes, estos elementos resguardan la información en tránsito y en reposo y también garantizan que únicamente los usuarios autorizados accedan a los sistemas, minimizando el riesgo de filtraciones o alteraciones no detectadas. En el contexto de Auxadi Costa Rica, donde se manejan datos financieros sensibles y se trabaja con múltiples plataformas digitales,

estas prácticas son esenciales para mantener el cumplimiento normativo y preservar la confianza de clientes y socios comerciales.

Uno de los recursos más efectivos para asegurar la confidencialidad de los datos es el cifrado, técnica que transforma la información de tal modo que solo las partes autorizadas pueden interpretarla. Tal como lo explica Roa (2013), “Nuestra esperanza es que, aunque lo tengan y lo puedan leer, no entiendan nada porque el contenido estará cifrado” (p. 28), lo que significa que incluso si se produce una filtración, el atacante no podría acceder al contenido real sin la clave correspondiente. Existen dos enfoques principales para la encriptación, el simétrico que utiliza la misma clave para cifrar y descifrar la información y el asimétrico que emplea una clave pública para cifrar y una privada para descifrar, este último resulta especialmente útil para comunicaciones seguras en redes corporativas, ya que permite validar la identidad del emisor y garantizar la integridad del mensaje.

Aunque el cifrado representa una barrera sólida para proteger la confidencialidad de la información, su efectividad depende en gran medida de que solo las personas autorizadas puedan acceder a los datos cifrados. Por esta razón también es fundamental establecer mecanismos que validen la identidad del usuario antes de conceder cualquier tipo de acceso, este enfoque integral fortalece el entorno de seguridad, ya que evita que una clave o archivo protegido caiga en manos equivocadas por fallos en la verificación de credenciales o suplantación de identidad. En este contexto, el modelo de seguridad AAA se convierte en una herramienta esencial para complementar las funciones del cifrado y reforzar el control de acceso en toda la infraestructura digital.

Para que los sistemas digitales sean verdaderamente seguros, no basta con cifrar la información, es necesario garantizar que los usuarios que intentan acceder a los recursos sean quienes dicen ser. En este punto, entra en juego el modelo de seguridad AAA, que contempla tres principios fundamentales: autenticación, autorización y auditoría. La autenticación consiste en confirmar la identidad del usuario o dispositivo, según Samaniego y Ponce (2017), “la autenticación es la encargada de comprobar que quien o quienes acceden a los sistemas es realmente quien dice ser” (p. 13), este proceso puede darse a través de algo que el usuario sabe

(como una contraseña), algo que tiene (como un token o tarjeta magnética), o algo que es (como una huella digital o reconocimiento facial). En sistemas críticos, se recomienda implementar el doble factor de autenticación combinando al menos dos de estas características, fortaleciendo así la barrera de acceso frente a intentos de intrusión.

Una vez autenticado el usuario, el sistema debe aplicar los controles adecuados de autorización, esta etapa define qué recursos puede utilizar y qué acciones puede realizar, asegurando la protección de la información contra usos indebidos o accidentales. La autorización, como lo explican Samaniego y Ponce (2017), "permite acceder a los recursos según los permisos asignados ya sea a la red o a los sistemas de información en función a su identidad" (p. 14), y dichos permisos deben alinearse con las responsabilidades de cada colaborador, aplicando el principio de mínimo privilegio. De esta forma, se impide que usuarios sin las competencias técnicas o administrativas manipulen archivos, configuraciones o bases de datos que no les corresponden.

La auditoría cierra el ciclo del modelo AAA, proporcionando trazabilidad sobre las acciones ejecutadas dentro del sistema. Los mecanismos de monitoreo y generación de alertas permiten identificar conductas anómalas, como múltiples intentos de acceso fallidos o el uso de funciones no autorizadas, estos eventos deben ser registrados y revisados como parte de un plan de respuesta ante incidentes, con el fin de tomar medidas correctivas de forma oportuna. Como lo mencionan Samaniego y Ponce (2017), "los mecanismos detectivos no evitan que algunas partes del sistema se comprometan", pero sí permiten generar alertas sobre "intentos fallidos al intentar usar funcionalidades del sistema que no le competen y otras actividades irregulares" (p. 11), integrar estos controles dentro de su infraestructura fortalecería la detección temprana de amenazas, permitiendo contener riesgos antes de que escalen y afecten los procesos del negocio.

La seguridad no puede depender únicamente de herramientas automatizadas; requiere una cultura organizacional consciente y capacitada para reaccionar ante situaciones atípicas. Es aquí donde la formación y la sensibilización del personal adquieren un valor estratégico, ya que permiten reconocer comportamientos sospechosos, actuar con criterio ante situaciones inesperadas y evitar caer en trampas diseñadas para evadir las medidas de protección implementadas.

Uno de los mayores riesgos para la seguridad de la información no siempre proviene de fallas técnicas, sino del factor humano. Los atacantes lo saben y por eso utilizan técnicas como la ingeniería social para explotar la confianza, el desconocimiento o la falta de preparación de los usuarios, esta práctica se ha perfeccionado con el tiempo y tiene como objetivo obtener datos confidenciales mediante el engaño. Como lo indica Romero, et al. (2018), “La ingeniería social es cualquier acto que induce a una persona a realizar una acción que puede, o no, ser en su mejor interés” (p. 150), en un entorno corporativo como el de Auxadi, este tipo de ataques puede tener consecuencias graves si el personal no cuenta con el entrenamiento adecuado para reconocer señales de alerta.

El phishing, una de las formas más comunes de ingeniería social, consiste en engañar al usuario para que entregue voluntariamente información sensible, el atacante se hace pasar por una institución legítima, utilizando correos electrónicos, mensajes o sitios web falsos que imitan a la perfección la identidad visual de bancos, empresas o entidades benéficas. Según Roa (2013), en este tipo de estafa, “El atacante se pone en contacto con la víctima (generalmente, un correo electrónico) haciéndose pasar por una empresa con la que tenga alguna relación (su banco, su empresa de telefonía, etc.)” (p. 19), y si el usuario cae en la trampa, puede revelar contraseñas, números de tarjeta o datos corporativos sin darse cuenta del riesgo, esta situación demuestra cómo la falta de criterios básicos de validación digital puede abrir brechas en la seguridad organizacional, incluso cuando existen herramientas tecnológicas avanzadas en funcionamiento.

En resumen, proteger los dispositivos, controlar los accesos, cifrar la información, responder ante incidentes y fortalecer el criterio del usuario son piezas complementarias de una misma estrategia. En el contexto de Auxadi Costa Rica, implementar este conjunto de medidas representa un paso firme hacia un entorno digital más seguro y alineado con la norma ISO/IEC 27001:2022. Solo mediante una gestión integral de la seguridad es posible garantizar que la información permanezca disponible, íntegra y confidencial, incluso ante escenarios adversos o amenazas emergentes.

CAPÍTULO III: MARCO METODOLÓGICO

Enfoques de Investigación

Para desarrollar una propuesta metodológicamente sólida es necesario comprender los enfoques de investigación y su función dentro del proceso de construcción del conocimiento, estos enfoques sirven como una guía para definir cómo se abordará el objeto de estudio y qué tipo de información se recopilará, además permiten seleccionar los instrumentos adecuados para su análisis y establecer el procedimiento lógico para interpretar los resultados. Escoger el enfoque correcto ayuda a que los datos tengan sentido y asegura que las conclusiones estén correctamente alineadas con el problema planteado.

Como lo señalan Hernández et al. (2017), “el término diseño se refiere al plan o estrategia concebida para obtener la información que se desea y responder al planteamiento del problema” (p. 97), lo que demuestra que todo enfoque parte de una estructura organizada y lógica con el conocimiento que se busca obtener. El diseño metodológico se convierte así en la base que da validez del estudio y permite establecer relaciones claras entre variables, identificar patrones y comprender los fenómenos con mayor profundidad.

Enfoque Cuantitativo

El enfoque cuantitativo parte de una visión objetiva y estructurada de la realidad, su propósito es medir con precisión los fenómenos utilizando instrumentos estandarizados, análisis estadísticos y recolección de datos numéricos. Esta metodología permite establecer relaciones entre variables, validar hipótesis y explicar comportamientos dentro de un contexto específico. También su aplicación genera resultados replicables, generalizables y útiles para la toma de decisiones basadas en evidencia.

Una de sus fortalezas es la posibilidad de observar los datos tal como se presentan o incluso intervenir para controlar ciertas condiciones, como lo indican Hernández et al. (2017), “en la investigación no experimental se observan o miden los fenómenos tal como se dan en su contexto

natural, para posteriormente analizarlos siguiendo siempre el planteamiento del problema" (p. 107), esto evidencia que no siempre es necesario alterar las variables para obtener resultados válidos y en muchos casos basta con analizar las situaciones tal como ocurren, especialmente cuando se busca describir o correlacionar aspectos reales del entorno. Según el objetivo del estudio, los investigadores pueden aplicar diseños experimentales, cuando se requiere manipular variables, o no experimentales, cuando se desea analizar situaciones sin intervenir.

Enfoque Cualitativo

El enfoque cualitativo se orienta a comprender los fenómenos desde la mirada de quienes los experimentan, a diferencia del enfoque cuantitativo que se apoya en datos numéricos, el cualitativo se basa en relatos, observaciones, entrevistas y análisis contextual. Su objetivo es interpretar emociones, experiencias, significados y dinámicas sociales que no pueden explicarse solo con números, este enfoque da prioridad a la riqueza del contenido antes que a la generalización estadística.

Se utiliza cuando se investigan realidades complejas, que requieren flexibilidad y una visión integral, como señalan Hernández et al. (2017), "se escogen diseños cualitativos cuando el investigador quiere explorar, describir y conocer con amplitud y profundidad percepciones, emociones, sentimientos, experiencias, enfoques y puntos de vista de personas, desde la perspectiva de los propios participantes o sujetos investigados, en su ambiente natural y de manera más abierta" (p. 114), esta cualidad lo hace ideal para estudios aplicados a entornos organizacionales, ya que permite una lectura más humana del entorno y facilita diseñar estrategias que se ajusten mejor a la realidad operativa y cultural de la empresa.

Enfoque Mixto

El enfoque mixto combina los métodos cuantitativo y cualitativo para analizar un fenómeno desde distintas perspectivas, esta integración permite una visión más completa, ya que se recopilan tanto datos numéricos como percepciones o experiencias de los involucrados. Este

tipo de enfoque es ideal cuando no solo se quiere medir un problema, sino también interpretarlo en su contexto.

Como lo explican Hernández et al. (2017), “representan procesos sistemáticos, empíricos y críticos de investigación que implican la recolección y el análisis integrado de datos cuantitativos y cualitativos, para realizar inferencias y entender mejor el fenómeno que se estudia” (p. 22). este enfoque es especialmente útil en investigaciones donde se busca mayor profundidad, como en el estudio de realidades organizacionales, procesos sociales o evaluaciones integrales que requieren datos variados para su comprensión.

Enfoque de Investigación Seleccionado

El enfoque seleccionado para el desarrollo de esta investigación es el cuantitativo, debido a que el proyecto requiere trabajar con datos concretos, estructurados y medibles que permitan identificar el estado actual de cumplimiento de los controles de seguridad alineados con la norma ISO/IEC 27001:2022. La naturaleza del estudio exige aplicar instrumentos que faciliten la recopilación y análisis objetivo de información, como listas de verificación, cuestionarios cerrados y registros documentales, los cuales están diseñados para obtener evidencia clara sobre los procesos internos de la organización.

Esta metodología resulta adecuada porque la propuesta se centra en evaluar condiciones técnicas y operativas específicas dentro de Auxadi Costa Rica, tales como el control de dispositivos, la protección de datos en tránsito y en reposo, la gestión de accesos, y las comunicaciones seguras entre usuarios y plataformas. A través del enfoque cuantitativo se podrá recopilar información desde distintos departamentos y comprobar los resultados con los requisitos de la norma.

Además, este enfoque permite trabajar con variables definidas, indicadores y escalas que ayuden a identificar con precisión las brechas de seguridad y justificar con evidencia técnica la necesidad de implementar políticas correctivas. La lógica estructurada del enfoque cuantitativo también ayuda a garantizar que los datos recolectados puedan ser utilizados para análisis

comparativos, tanto internos como con respecto a lo exigido por el estándar, lo cual respalda la viabilidad técnica y metodológica del estudio, por lo tanto, esta base es clave para proponer soluciones reales, medibles y ajustadas a las necesidades operativas del entorno empresarial actual.

Tipos de Investigación

Antes de definir el diseño metodológico de una propuesta, es importante comprender los tipos de investigación, también llamados alcances. Estos permiten establecer el nivel de profundidad con el que se estudiará el fenómeno y orientan el enfoque que se aplicará para recolectar y analizar los datos. Los alcances determinan si la investigación se enfocará en describir, explorar, correlacionar o explicar un fenómeno, por eso seleccionar el tipo adecuado es muy importante porque permite estructurar correctamente los métodos, técnicas e instrumentos del estudio.

Como indican Hernández et al. (2017), “los alcances son cuatro: exploratorio, descriptivo, correlacional y explicativo, pero en la práctica, cualquier investigación puede incluir elementos de uno o varios” (p. 74), esta flexibilidad permite adaptar el enfoque según las necesidades del estudio. Conocer los tipos de investigación ayuda a alinear la estrategia metodológica con los objetivos propuestos y desarrollar un análisis más profundo que responda de forma efectiva al problema identificado.

Investigación Descriptiva

La investigación descriptiva se enfoca en detallar con claridad las características de un fenómeno, grupo, proceso u objeto de estudio. Su propósito es medir, clasificar y representar datos que permitan comprender cómo está compuesto un entorno específico, sin alterar su dinámica natural. este tipo de estudio se basa en la recolección precisa de información sobre variables concretas, como perfiles, comportamientos, condiciones o propiedades observables y a partir de estos datos se construyen representaciones claras y estructuradas del objeto de estudio.

Como lo explica Lara (2011), “La investigación descriptiva, según se mencionó, trabaja sobre realidades de hecho y su característica fundamental es la de presentar una interpretación correcta” (p. 50), esto refuerza que la investigación descriptiva no pretende establecer relaciones de causa y efecto, sino retratar fielmente una realidad tal y como se presenta en el momento del estudio. También ofrece una base sólida de información que permite comprender el estado actual de un fenómeno y sirve como punto de partida para futuros análisis más profundos o decisiones estratégicas.

Investigación Exploratoria

La investigación exploratoria se aplica cuando el objeto de estudio es reciente, poco abordado o no cuenta con suficientes antecedentes documentados. Permite al investigador adentrarse en temas nuevos, observar fenómenos emergentes y obtener un primer acercamiento a realidades poco comprendidas, además su finalidad es reconocer elementos clave que ayuden a delimitar el problema, identificar posibles variables y sentar las bases para investigaciones futuras más estructuradas y profundas. Este tipo de estudio es ideal cuando hay muchas dudas o escasa información disponible sobre el fenómeno.

Como lo indican Lara (2011), “En la investigación exploratoria los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes” (p. 50), lo que reafirma su utilidad en escenarios poco documentados, este enfoque permite identificar brechas de conocimiento, conocer el contexto real de trabajo y recopilar datos que sirvan de base para la formulación de estrategias más enfocadas.

Investigación Explicativa

La investigación explicativa busca ir más allá de la simple observación o descripción de los fenómenos, su objetivo principal es identificar las causas que los originan, comprender por qué suceden y en qué condiciones se manifiestan ciertas conductas, situaciones o relaciones entre variables, este tipo de estudio permite formular teorías, predecir comportamientos futuros y

entender los mecanismos que sustentan un determinado fenómeno dentro de un contexto específico.

Como lo aclaran Hernández et al. (2014), el estudio explicativo “Se enfoca en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables” (p. 78), esta afirmación deja en evidencia que este tipo de investigación se orienta hacia un análisis profundo en el que cada variable es examinada en función de su influencia sobre otras. Aplicar un enfoque explicativo resulta especialmente útil cuando se pretende justificar decisiones estratégicas, validar modelos teóricos o comprobar hipótesis en escenarios reales.

Tipo de Investigación Seleccionado

El tipo de investigación definido para esta propuesta es el descriptivo, ya que uno de los principales propósitos del estudio es realizar una caracterización detallada de los procesos, políticas y mecanismos de seguridad de la información actualmente implementados en Auxadi Costa Rica, la investigación busca documentar el estado actual en áreas como el control de dispositivos, la protección de datos, las comunicaciones seguras y la gestión de accesos con el fin de contar con una visión clara y ordenada sobre las prácticas existentes dentro de la organización.

Este tipo de investigación permite recopilar información relevante sobre los activos tecnológicos, las responsabilidades del personal involucrado y los niveles de cumplimiento frente a los controles definidos en la norma ISO/IEC 27001:2022. A través de técnicas estructuradas, como las listas de verificación, las entrevistas guiadas y los cuestionarios aplicados al personal, se podrá generar un diagnóstico organizacional que sirva como base para desarrollar propuestas específicas orientadas al fortalecimiento de la seguridad.

La elección de un enfoque descriptivo va acorde con los objetivos de la investigación, ya que se pretende obtener una comprensión clara del contexto institucional sin necesidad de intervenir directamente en los procesos o de establecer relaciones causales entre variables. El proyecto se enfoca en recopilar datos desde una perspectiva analítica que permita visualizar con exactitud cómo se gestionan los controles en la práctica, cuáles son las áreas más vulnerables y

qué aspectos deben ajustarse para cumplir con los estándares internacionales, toda esta información resulta fundamental para diseñar políticas y procedimientos que respondan de forma precisa a las necesidades de la empresa y contribuyan a la mejora continua de su sistema de gestión de seguridad de la información.

Fuentes de Información

En toda investigación, contar con fuentes confiables y pertinentes es un elemento clave para garantizar la solidez del análisis y la validez de las propuestas que se generen. No se trata únicamente de recopilar información, sino de seleccionar aquella que realmente aporte valor al objeto de estudio y que provenga de contenidos verificables y con fundamento técnico o académico. Como bien señala Lara (2011), "la confiabilidad se vuelve cada vez más relevante debido a que en la actualidad comunicar y publicar información está al alcance de cualquier persona" (p. 198), lo que implica una mayor responsabilidad al momento de discriminar entre fuentes útiles y aquellas que pueden comprometer la calidad del trabajo.

Este criterio toma aún mayor relevancia cuando se abordan temáticas sensibles como la seguridad de la información, donde el margen de error debe ser mínimo. En estos casos, se vuelve indispensable apoyarse en fuentes primarias y actualizadas, generadas por quienes han tenido contacto directo con el fenómeno o los datos, evitando caer en interpretaciones de segunda o tercera mano que podrían desviar la comprensión del problema y afectar las conclusiones del estudio.

Fuentes Primarias

Las fuentes primarias son aquellas que proporcionan datos directos, obtenidos por quienes presenciaron o generaron el hecho estudiado, este tipo de información resulta esencial en cualquier investigación seria, ya que permite trabajar con evidencias reales y sin intermediarios. Como se aclara Lara (2011), "proveen datos de quienes directamente presenciaron un hecho o generaron alguna idea" (p. 198), lo que refuerza su valor como base para un análisis objetivo y contextualizado.

En el caso de investigaciones aplicadas a entornos empresariales, como lo es la gestión de la seguridad de la información, estas fuentes pueden tomar la forma de registros internos, entrevistas al personal clave, bitácoras o informes originales. Utilizarlas fortalece la confiabilidad de los resultados, permite entender la dinámica real de la organización y proponer soluciones concretas, alineadas con la experiencia operativa.

Fuentes Secundarias

Las fuentes secundarias se caracterizan por ofrecer información indirecta, es decir, no provienen del autor o protagonista original del hecho, sino que recopilan, interpretan o comentan datos obtenidos de otras obras. En el contexto de una investigación, este tipo de fuente puede resultar útil para tener una visión más amplia o complementaria, especialmente cuando no se tiene acceso directo a la fuente primaria.

Tal como aclara Lara (2011), “las secundarias son aquellas que se refieren a una fuente que no se ha consultado directamente, sino a través de otras obras que las citan” (p. 198). Por eso, aunque son valiosas en muchos casos, es importante validar su objetividad y actualidad, ya que pueden contener interpretaciones parciales o distorsiones. En proyectos donde se busca precisión, como en la gestión de la seguridad de la información, el uso de fuentes secundarias debe complementarse siempre con evidencia directa para garantizar la calidad del análisis.

Fuentes Terciarias

Las fuentes terciarias funcionan como herramientas de orientación dentro del proceso investigativo. No ofrecen información nueva ni análisis directo del tema, pero permiten acceder con mayor facilidad a documentos clave al organizar y clasificar fuentes primarias y secundarias. Este tipo de material incluye catálogos, bibliografías, índices temáticos, diccionarios especializados o compilaciones digitales, y son de gran ayuda para ubicar datos relevantes cuando se está construyendo el marco teórico o realizando una revisión de antecedentes.

Un ejemplo práctico de cómo se entienden estas fuentes lo brinda Lara (2011), al indicar que: “Una fuente de primera mano: una obra de Freud; una fuente de segunda mano: un libro que cita las palabras de Freud y una tercera sería aquel que cita al que citó a Freud” (p. 198). Esto refleja cómo las fuentes terciarias se basan en referencias indirectas, por lo que deben usarse con criterio y únicamente como apoyo complementario para fortalecer la trazabilidad de los datos en investigaciones más rigurosas.

Variables

Las variables son componentes clave dentro de cualquier proceso investigativo, ya que permiten identificar, medir y analizar características que pueden cambiar entre los sujetos o situaciones que se estudian, estas características pueden ir desde datos simples como la edad o el sexo, hasta conceptos más complejos como el nivel de satisfacción, la productividad o el desempeño. Lo importante es que cada variable puede ser observada o medida, lo que permite estructurar un análisis claro y preciso del problema investigado.

Tal como explica SalusPlay (s. f.), “una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse” (párr. 1), esta definición resalta que las variables sirven para describir y son útiles para establecer relaciones, detectar tendencias y validar hipótesis. Por eso, el uso adecuado de las variables es lo que permite transformar una idea general en una investigación clara, medible y con resultados concretos.

Variables Conceptuales

Las variables conceptuales son aquellas que definen un fenómeno desde su significado teórico o abstracto, se utilizan para establecer con claridad a qué se refiere una investigación cuando habla de cierto concepto, evitando confusiones o ambigüedades. Estas definiciones suelen basarse en teorías existentes, diccionarios especializados o autores reconocidos, y sirven como base para la posterior medición u observación del fenómeno que se estudia.

Como señala Explorable.com (s. f.), “Las variables conceptuales son generalmente expresadas en términos generales, teóricos, subjetivos o cualitativos” (párr. 1), lo que confirma que este tipo de variable define el alcance del fenómeno de estudio antes de pasar a su medición. Esta definición fundamenta el desarrollo de hipótesis coherentes y alineadas con los objetivos, asegurando que el análisis posterior sea congruente con la intención investigativa y sirva como base para traducir estas ideas a indicadores medibles.

Variables Operacionales

Las variables operacionales representan la forma práctica en que se definen y miden las variables dentro de una investigación, su objetivo es traducir conceptos teóricos en indicadores claros y concretos que puedan observarse, medirse o evaluarse en la realidad. Esta definición es muy importante porque asegura que todas las personas involucradas en el estudio entiendan y midan la variable de la misma manera, lo cual es fundamental para obtener resultados consistentes y válidos.

Según lo indica SalusPlay (s. f.), “una definición operacional nos dice que hay que hacer para recoger datos respecto de una variable” (párr. 8), esto significa que la variable ya no queda en el plano abstracto, sino que se transforma en acciones concretas que permiten comprobar si el fenómeno ocurre y en qué medida. En otras palabras, la operacionalización convierte las ideas en datos medibles, y esto es esencial para cualquier estudio que busque obtener resultados aplicables a contextos reales.

Variables Instrumentales

Las variables instrumentales representan los instrumentos concretos que se emplean para recolectar información sobre las variables en estudio, permitiendo medir el fenómeno de interés de forma práctica y sistemática, estas variables se definen a partir de la operacionalización del estudio, es decir, traducen los conceptos teóricos en elementos observables mediante instrumentos como encuestas, entrevistas, observación o registros administrativos. Su propósito es garantizar

que las medidas recolectadas sean coherentes con los objetivos de la investigación y permitan obtener datos confiables.

Según Moreno Galindo (2018), la definición instrumental "implica tratar de aclarar el medio o instrumento por el cual recogerá la información a efectos de continuar con la investigación" (párr. 5), lo que deja claro que las variables instrumentales funcionan como el puente entre la teoría y la práctica, estableciendo de manera específica qué herramientas se utilizarán para recolectar los datos, esto es esencial para garantizar la coherencia metodológica y facilitar la recolección sistemática de información alineada con los objetivos y variables definidas.

Cuadro de Variables

Tabla 2

Unidades de análisis.

Objetivo Específico	Variable	Variable Conceptual	Variable Operacional	Variable Instrumental
Analizar el estado de seguridad de la información en la gestión de dispositivos, seguridad en la comunicación y protección de datos, identificando vulnerabilidades y riesgos en la empresa según la norma ISO/IEC 27001:2022.	Gestión de riesgos Seguridad de la información	Según Perallis Security (s. f.) la gestión de riesgos, "Se trata de una estrategia que incluye la implementación de procesos para identificar, evaluar y mitigar riesgos asociados a los activos de información de una organización". (párr. 4) Según Kaspersky (s. f.), "la seguridad de la información se refiere a las prácticas diseñadas para mantener seguros los datos frente a accesos no autorizados, uso indebido, alteración o destrucción". (párr. 2)	Encuestas, entrevistas y revisión documental	Matriz de riesgos, cuestionario, guía de entrevista y listas de verificación
Seleccionar los controles de seguridad aplicables a la gestión de dispositivos, seguridad en la comunicación y protección de datos, de forma que se asegure su alineación con la norma ISO/IEC	Controles de seguridad	IBM (s. f.), indica que los controles de seguridad se refieren a los "parámetros implementados para proteger diversas formas de datos e infraestructura importantes para una organización. Cualquier tipo de salvaguarda o contramedida utilizada para evitar, detectar,	Análisis de correlación riesgos-controles y entrevista	Cuadro de correspondencia riesgo-control, guía de entrevista y revisión documental

27001:2022, el análisis de riesgos realizado y las necesidades específicas de la organización.		contrarrestar o minimizar los riesgos de seguridad ". (párr. 1)		
Diseñar una propuesta estructurada de políticas y procedimientos de seguridad según el análisis y selección previos, garantizando medidas efectivas para la gestión de dispositivos, la seguridad en la comunicación y la protección de datos según la norma ISO/IEC 27001:2022.	Políticas Procedimientos	Orsys-Le Mag (s. f.) señala que las políticas de seguridad son "un documento estratégico y operativo adoptado por cualquier organización que define un conjunto de normas, directrices y procedimientos destinados a proteger los activos de información contra todas las amenazas.". (párr. 1) Según Interpolados (2020), "Los procedimientos de seguridad en la información son todos aquellos que muestran como implementar las políticas, estándares, mejores prácticas y guías enfocadas a garantizar la seguridad en la información" (párr. 1).	Redacción de propuesta de políticas y procedimientos alineados con los controles seleccionados	Revisión documental y guía estructurada para elaboración normativa
Evaluar la viabilidad económica y operativa de la propuesta basada en las buenas prácticas establecidas en la norma ISO/IEC 27001:2022, garantizando que su aplicabilidad y sostenibilidad se ajusten al contexto de la empresa.	Viabilidad de implementación	OBSBUSINESS School (s. f.) afirma que "Un estudio de viabilidad permite averiguar si la iniciativa es o no realizable. Para ello, se analizan diferentes perspectivas, como la técnica, la económica". (párr. 5)	Evaluación de los recursos actuales de la empresa y su capacidad para adoptar las medidas propuestas	Cuadro de viabilidad y guía de entrevista

Fuente: Elaboración propia

Población

La población del presente estudio está compuesta por cinco personas del equipo de tecnologías de la información de Auxadi Costa Rica, quienes desempeñan un papel clave en la gestión de dispositivos, seguridad en la comunicación y protección de datos. Esta población ha sido definida de manera intencional, considerando exclusivamente a los colaboradores con responsabilidad directa sobre los activos tecnológicos y los procesos que serán evaluados, lo cual

garantiza que los datos recopilados sean pertinentes, fiables y alineados con los objetivos del estudio. Además, se trata de una población finita, accesible y especializada, con la que es posible aplicar instrumentos de recolección de información como encuestas estructuradas, entrevistas y revisión documental de forma controlada y efectiva.

Este grupo cumple con las características fundamentales para un estudio cuantitativo, ya que está claramente delimitado, se mantiene estable durante el período de análisis y representa fielmente el entorno técnico en el cual se aplicará la propuesta. Como explican Mehdi, et al. (2023), "la población de investigación es el conjunto de individuos o elementos sobre los cuales se desea obtener información o conocimiento" (p. 70), lo cual respalda la elección de este segmento como base metodológica para obtener resultados válidos y aplicables en el marco del análisis de riesgos y controles de seguridad según la norma ISO/IEC 27001:2022.

Muestra

Para este estudio, la muestra está conformada por 5 colaboradores del área de tecnologías de la información de Auxadi Costa Rica, seleccionados mediante un muestreo no probabilístico de tipo intencional. Esta elección se justifica por la necesidad de incluir únicamente a aquellos perfiles que poseen conocimiento directo sobre la gestión de dispositivos, la seguridad en la comunicación y la protección de datos. La muestra incluye personal técnico, administradores de sistemas y responsables operativos que participan activamente en los procesos críticos que serán evaluados. Al tratarse de una población pequeña y accesible, no es necesario aplicar fórmulas estadísticas para determinar el tamaño muestral.

La finalidad de esta muestra es garantizar representatividad respecto a los dominios evaluados de la norma ISO/IEC 27001:2022, de forma que los resultados obtenidos sean relevantes para el análisis de riesgos, selección de controles y diseño de políticas de seguridad. Como explican Mehdi, et al. (2023), "la muestra representa a la población y los resultados obtenidos de la muestra se utilizan para hacer inferencias o generalizaciones sobre la población" (p. 77), lo cual respalda el uso de este grupo específico como fuente principal de información. En este caso, cada unidad

de análisis y unidad de muestreo coinciden, ya que los mismos sujetos aportarán los datos mediante encuestas, entrevistas estructuradas y revisión documental.

Instrumentos de Recolección de Datos

Para este estudio se aplicarán encuestas al personal técnico y administrativo, entrevistas a responsables de TI y revisión documental, esta combinación permite recolectar datos precisos sobre la gestión de dispositivos, seguridad en la comunicación y protección de datos, alineados con la norma ISO/IEC 27001:2022. Las encuestas aportan información cuantificable, mientras que las entrevistas y documentos refuerzan el análisis con evidencias internas.

Según Hernández, et al. (2018), "existen múltiples instrumentos para medir toda clase de variables y en algunos casos puedes combinar varias técnicas de recolección de los datos" (p. 250), lo cual respalda la elección de herramientas complementarias en esta investigación. Cada instrumento está vinculado a las variables del estudio y será aplicado a una muestra intencional bien delimitada, lo que garantiza que los resultados obtenidos sean cuantificables, confiables y útiles para la toma de decisiones dentro del contexto operativo y de seguridad de la organización.

Cuestionario

Dentro de esta investigación, el cuestionario será uno de los instrumentos fundamentales para recolectar datos del personal técnico y administrativo de Auxadi Costa Rica. Su uso responde a la necesidad de obtener información cuantitativa precisa sobre prácticas actuales en la gestión de dispositivos, seguridad en la comunicación y protección de datos, según los lineamientos de la norma ISO/IEC 27001:2022, esta herramienta se diseña con preguntas previamente estructuradas, relacionadas directamente con las variables establecidas, y permite una rápida recopilación y análisis de resultados medibles. Además, al aplicar el cuestionario a través de un formato cerrado, se asegura una mayor facilidad en la codificación de respuestas y una mejor comparación entre los participantes.

Como lo explica Hernández, et al. (2018), “las preguntas cerradas son más fáciles de codificar y preparar para su análisis. Asimismo, estas preguntas requieren un menor esfuerzo por parte de los encuestados, que no tienen que escribir o verbalizar pensamientos” (p. 254), esta característica facilita enormemente el proceso de análisis estadístico que se aplicará en esta investigación, lo que refuerza la viabilidad del enfoque cuantitativo adoptado. En este contexto, el cuestionario permitirá conocer el nivel de conocimiento y cumplimiento actual en temas de seguridad de la información y también brindará datos claros para sustentar la propuesta de políticas y procedimientos.

Entrevista

La entrevista será utilizada como instrumento complementario para obtener información precisa de los responsables de tecnologías de la información en Auxadi Costa Rica, este tipo de técnica aplicada de forma estructurada y cara a cara, permite guiar al entrevistado a través de un cuestionario estandarizado que refuerza la validez de los datos obtenidos. En el contexto de este estudio, las entrevistas permiten aclarar criterios aplicados en la gestión de dispositivos, seguridad de la comunicación y protección de datos, aportando evidencias clave sobre prácticas internas que no siempre quedan documentadas formalmente. Además, se seleccionarán participantes con amplio conocimiento técnico relacionado a seguridad informática, lo que incrementa el valor analítico de las respuestas.

En las entrevistas de tipo cuantitativo se debe mantener un formato uniforme, con preguntas cerradas, condiciones homogéneas para todos los participantes y sin intervención externa, como señalan Hernández, et al. (2018), “el mismo instrumento y procedimientos se aplican a todos los participantes, en condiciones lo más similares posible (estandarización)” (p. 269), por esta razón, la labor del estudiante será mantener la neutralidad, claridad en la formulación de preguntas y control del ambiente donde se realicen las sesiones. sí se garantiza que la información recopilada sea comparable, objetiva y alineada a las variables definidas para este estudio.

Revisión Documental

La revisión documental representa una herramienta fundamental dentro del enfoque cuantitativo, ya que permite examinar registros existentes de forma estructurada y objetiva, en esta investigación se utilizará para analizar documentos internos de Auxadi Costa Rica relacionados con la seguridad de la información, como políticas, procedimientos, informes de incidentes y controles técnicos implementados. Esto permitirá conocer el grado de alineación con la norma ISO/IEC 27001:2022, específicamente en lo que respecta a la gestión de dispositivos, comunicación segura y protección de datos. Además, al tratarse de evidencia escrita, esta técnica facilita el respaldo de los resultados obtenidos mediante otros instrumentos, como encuestas y entrevistas.

Según Concepto.de (s. f.), "una investigación documental es aquella que se caracteriza por emplear la consulta de fuentes escritas, gráficas, sonoras o fílmicas" (párr. 1), esta definición respalda el uso de documentación institucional como fuente primaria de análisis, ya que permite validar el estado real de las prácticas en la organización. Gracias a este enfoque se podrán contrastar los datos recabados y reforzar la confiabilidad del estudio, asegurando que los hallazgos no solo sean medibles, sino también verificables dentro del entorno operativo real.

Lista de Verificación

La lista de verificación se utilizará para recopilar información técnica de forma estructurada, con el fin de validar si los controles actuales implementados en Auxadi Costa Rica cumplen con los criterios definidos en la norma ISO/IEC 27001:2022, este tipo de técnica facilita una revisión clara y objetiva de los procedimientos relacionados con la gestión de dispositivos, la seguridad en la comunicación y la protección de datos. Su formato estandarizado permite identificar puntos de cumplimiento y brechas existentes en las políticas y prácticas internas, permitiendo además una comparación directa con los dominios seleccionados para este estudio.

El uso de listas de chequeo aporta valor cuantitativo al estudio, ya que cada ítem responde a una condición verificable y medible, como lo indica Unifikas (s. f.), "la lista de chequeo o

checklist es un formato creado para llevar un control en las tareas o acciones que debemos realizar en una organización" (párr. 1), lo que justifica su aplicación como método de análisis estructurado. En el caso de este proyecto, será aplicada mediante revisión documental y sesiones controladas con los responsables de TI, asegurando así que los resultados puedan ser integrados con los demás instrumentos para fortalecer el diagnóstico.

Matriz de Riegos

La matriz de riesgos es una herramienta fundamental dentro del enfoque cuantitativo, ya que permite evaluar de manera visual y estructurada los riesgos asociados a los activos tecnológicos. En el contexto de Auxadi Costa Rica, se utilizará para cruzar la probabilidad de ocurrencia y el impacto de amenazas sobre dispositivos, servicios de comunicación y protección de datos, esto facilitará la priorización de acciones correctivas y presupuestarias alineadas con la norma ISO/IEC 27001:2022, aportando claridad y objetividad al análisis. Según Pirani (s. f.), "la matriz de riesgos es una herramienta permite visualizar, cuantificar, controlar, transferir o mitigar los riesgos y, lo más importante, tomar decisiones estratégicas" (párr. 1), lo que destaca su papel esencial para orientar decisiones estratégicas sobre seguridad de la Información.

Además, al aplicar la matriz de riesgos se pueden definir criterios cuantitativos como niveles de riesgo y categorizarlos por rangos de probabilidad e impacto previamente establecidos, lo cual facilita su incorporación a indicadores estadísticos, reportes visuales y cuadros de seguimiento. Esta herramienta permite ordenar la información de forma clara, comparar resultados entre activos o áreas específicas y priorizar acciones correctivas con base en datos reales. Esto fortalece el enfoque cuantitativo del estudio, ya que se obtienen resultados numéricos útiles para identificar vulnerabilidades críticas, justificar decisiones técnicas y medir la efectividad de los controles existentes de forma objetiva.

Proceso para la Recolección y Análisis de Datos

El proceso de recolección de datos en esta investigación se ha diseñado cuidadosamente para obtener información precisa, medible y confiable sobre la gestión de dispositivos, seguridad

en la comunicación y protección de datos, todos alineados con los requisitos de la norma ISO/IEC 27001:2022. Se empleará un enfoque cuantitativo, por lo que se prioriza la obtención de datos numéricos que permitan realizar análisis estadísticos y tomar decisiones objetivas en función de los hallazgos. Para ello, se aplicarán encuestas estructuradas al personal técnico y administrativo, entrevistas dirigidas a los responsables de TI y una revisión documental sobre políticas, registros y reportes de seguridad existentes.

La encuesta será aplicada a una muestra intencional compuesta por el personal de Auxadi Costa Rica que interactúa directamente con sistemas de información, dispositivos tecnológicos y gestión de datos, estas encuestas permitirán medir el nivel de cumplimiento, percepción de riesgos y efectividad de los controles actuales. Cada ítem de la encuesta estará vinculado a las variables establecidas en el cuadro de unidades de análisis y será diseñado en función de los apartados descritos en el alcance funcional. Los resultados obtenidos serán tabulados y procesados estadísticamente para identificar patrones, niveles de riesgo y oportunidades de mejora dentro de la empresa.

Complementariamente, las entrevistas se aplicarán a los responsables de TI y encargados de seguridad informática. Aunque el enfoque principal del estudio es cuantitativo, estas entrevistas servirán para reforzar el análisis al validar la aplicabilidad y viabilidad de los controles seleccionados. También se utilizarán como respaldo para el diseño de las políticas propuestas y para entender posibles limitaciones operativas o técnicas.

La revisión documental será clave para analizar registros internos, normativas actuales, informes de auditorías y políticas ya existentes, esta técnica permitirá contrastar los resultados de encuestas y entrevistas con evidencia tangible, fortaleciendo la validez del estudio. Toda esta información será analizada en conjunto mediante herramientas como matrices de riesgo, cuadros de correlación riesgo-control, tablas de cumplimiento y análisis de viabilidad. Este proceso garantizará una visión completa, estructurada y cuantificable de la situación actual y de las recomendaciones finales que se emitirán en la propuesta.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Inventario Clasificado de Activos con Criterios de Criticidad

Objetivo del Inventario

El presente inventario se formula a partir de la revisión documental y de las entrevistas aplicadas al personal técnico de Auxadi Costa Rica, con el objetivo de identificar los activos de información de mayor relevancia para la organización. Dichos activos fueron clasificados considerando su función, el nivel de criticidad, el impacto potencial ante una falla y la disponibilidad requerida, este registro servirá como base para establecer controles alineados a la norma ISO/IEC 27001:2022 y fortalecer la gestión de dispositivos, comunicación y protección de datos.

Alcance de la Revisión

La identificación y clasificación incluyó activos de carácter físico, lógico y en la nube, tales como servidores, estaciones de trabajo, aplicaciones corporativas, sistemas de respaldo, plataformas de comunicación y dispositivos de red. El análisis abarcó tanto los activos identificados durante las entrevistas como los documentados en políticas, procedimientos y planes oficiales, considerando su relevancia para la operación diaria, su contribución a la continuidad del negocio y el grado de protección actual.

Entrevista Técnica para Clasificación de Activos de Información

La siguiente entrevista fue aplicada al equipo técnico de Auxadi Costa Rica, compuesto por cinco colaboradores clave del área de TI. El propósito principal de esta entrevista es identificar y clasificar los activos tecnológicos de la organización con base en su nivel de criticidad para las operaciones diarias y continuidad del negocio, esta información servirá como complemento para desarrollar un inventario clasificado y posteriormente aplicar controles alineados con la norma

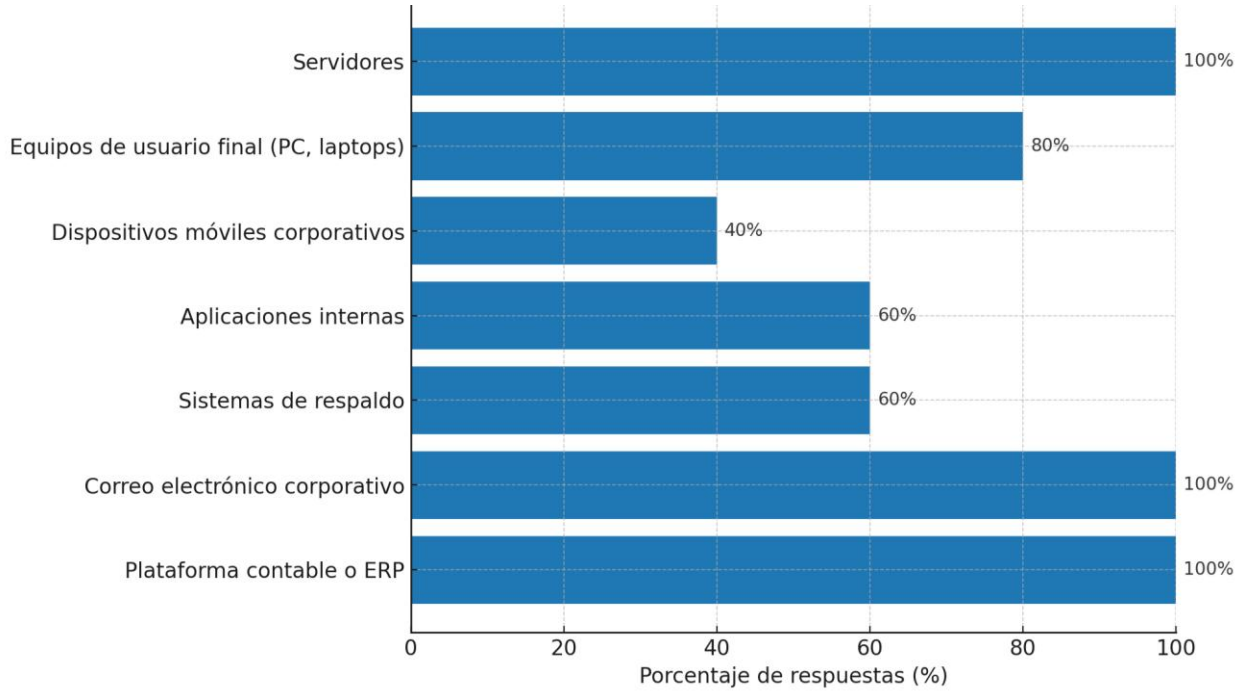
ISO/IEC 27001:2022, específicamente en el contexto de gestión de dispositivos, comunicación y protección de datos. Se utilizo el Apéndice A. Guía de Entrevista 1.

Resultados de la entrevista técnica.

- Pregunta 1: ¿Cuál de los siguientes activos considera crítico para las operaciones diarias? (Marque todos los que apliquen)

Ilustración 1

Resultados de entrevista técnica para clasificación de activos – pregunta 1.



Fuente: Elaboración propia

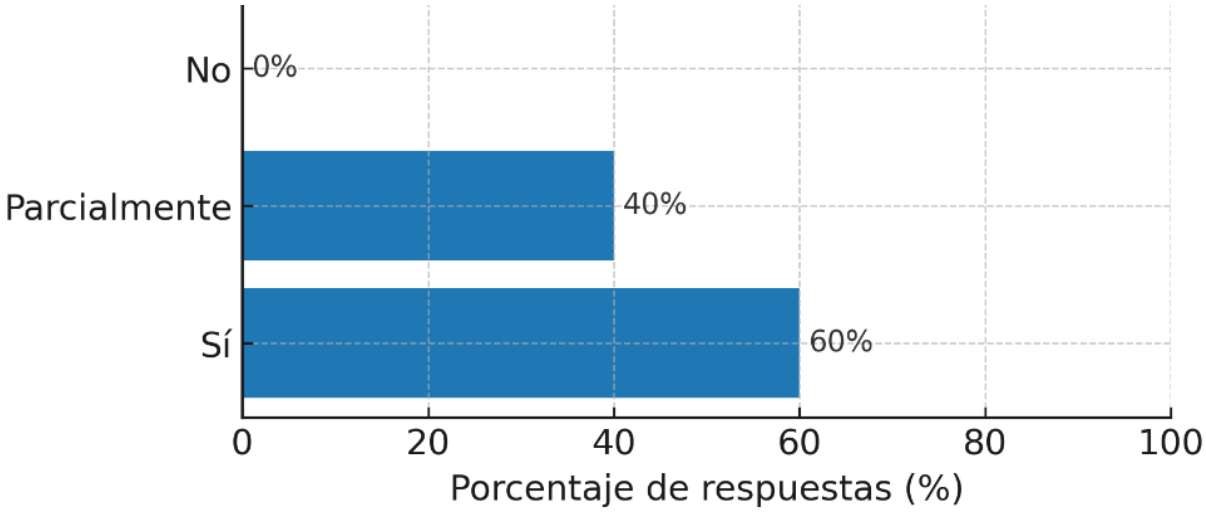
Los activos identificados como de mayor criticidad fueron los servidores, el correo electrónico corporativo y la plataforma contable o ERP, con un 100 % de coincidencia. Este hallazgo confirma que dichos elementos representan la base sobre la cual se sostiene la operación tecnológica de la empresa, al concentrar información sensible y procesos esenciales para la continuidad del negocio. En un segundo nivel se ubicaron los equipos de usuario final (80 %), cuya importancia radica en su papel directo en la productividad del personal. En menor medida,

se mencionaron las aplicaciones internas y los sistemas de respaldo (60 %), que, aunque no son utilizados de manera generalizada, cumplen funciones estratégicas para áreas específicas y para la recuperación de datos en caso de incidentes. Finalmente, los dispositivos móviles alcanzaron el menor porcentaje (40 %), lo que refleja que, aunque facilitan la movilidad y el teletrabajo, su impacto en la operación resulta más limitado frente a los activos centrales.

- Pregunta 2: ¿Existe un inventario formal de activos tecnológicos?

Ilustración 2

Resultados de entrevista técnica para clasificación de activos – pregunta 2.



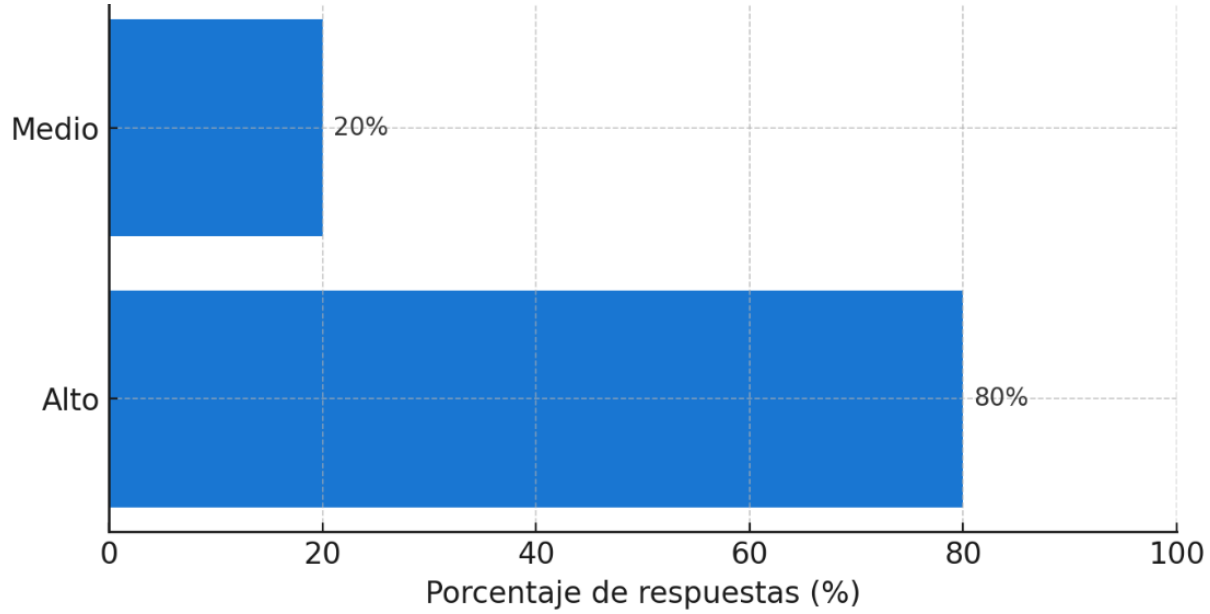
Fuente: Elaboración propia

El 60 % del personal de TI indicó que sí existe un inventario formal de activos tecnológicos, mientras que un 40 % señaló que este solo se encuentra parcialmente documentado. Ninguno de los participantes afirmó la inexistencia del registro, lo que permite concluir que la organización ya ha dado pasos importantes en esta materia. Este hallazgo refleja que el proceso de inventariado se encuentra en ejecución y que existe conciencia institucional sobre su importancia, aunque aún requiere fortalecerse en cuanto a su formalización, actualización periódica y cobertura total de los activos críticos.

- Pregunta 3: ¿Cuál es el nivel de impacto para la empresa si el activo deja de funcionar?

Ilustración 3

Resultados de entrevista técnica para clasificación de activos – pregunta 3.



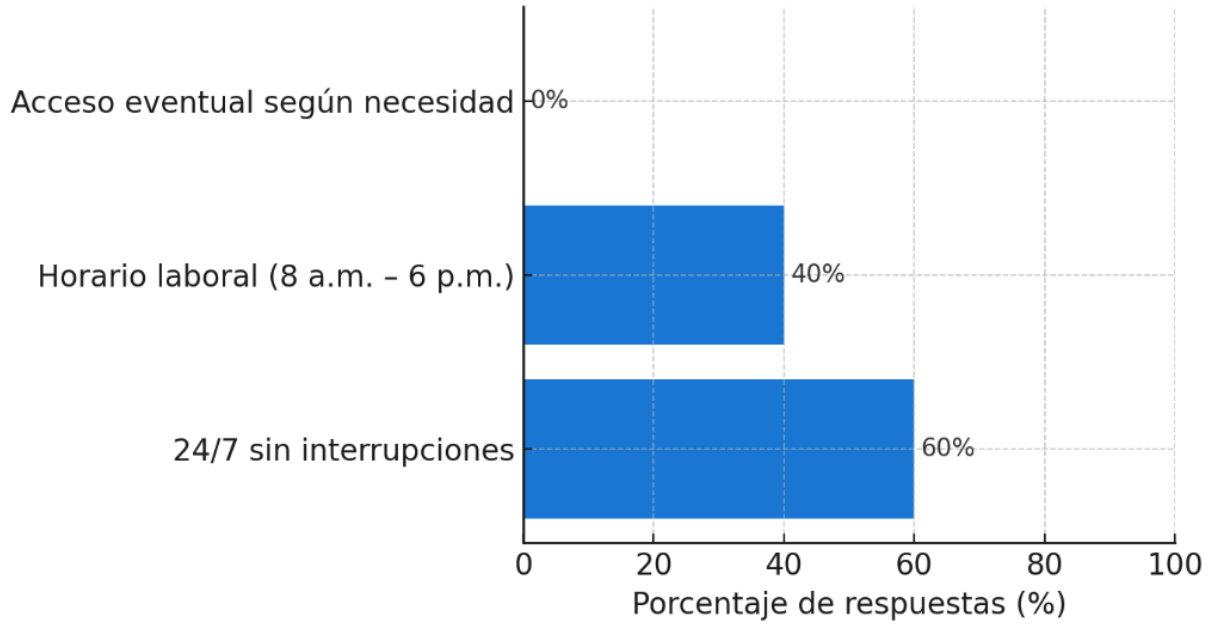
Fuente: Elaboración propia

El 80 % de los participantes consideró que la falla de un activo crítico tendría un impacto alto, mientras que el 20 % lo clasificó como impacto medio. Ninguno de los entrevistados seleccionó la opción de “impacto bajo”, lo cual resulta coherente si se toma en cuenta que se trata de activos esenciales para la operación, tales como los servidores, el correo corporativo y la plataforma ERP, esto refleja que el personal técnico reconoce la dependencia directa que tiene la organización de estos recursos y la vulnerabilidad que implicaría su interrupción.

- Pregunta 4: ¿Cuál es la disponibilidad deseada para los activos críticos?

Ilustración 4

Resultados de entrevista técnica para clasificación de activos – pregunta 4.



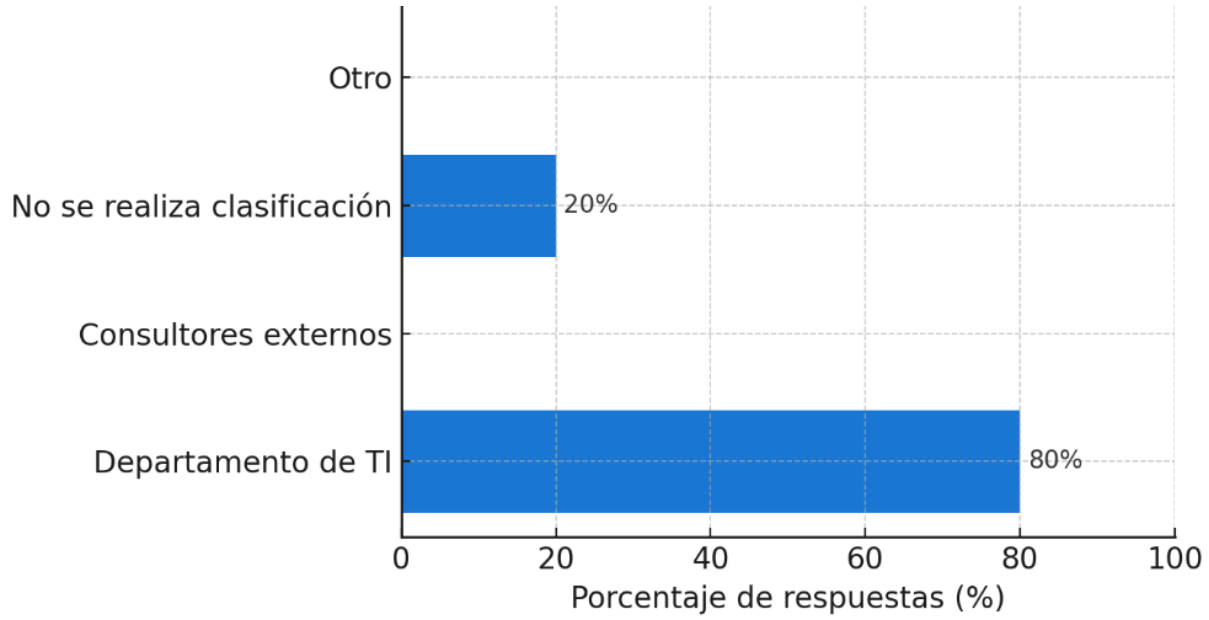
Fuente: Elaboración propia

El 60 % de los entrevistados indicó que los activos críticos deben estar disponibles 24/7 sin interrupciones, mientras que el 40 % señaló que basta con garantizar su funcionamiento en horario laboral. Ninguno seleccionó la opción de acceso eventual, lo que refleja que independientemente del nivel de exigencia planteado, todos los participantes consideran que estos activos requieren una disponibilidad constante y confiable. Este hallazgo evidencia que la continuidad operativa es una prioridad para la empresa, dado que la interrupción de servicios como servidores, correo corporativo o plataformas de gestión tendría un efecto inmediato en la productividad y en la capacidad de respuesta frente a clientes y procesos internos.

- Pregunta 5: ¿Quién clasifica actualmente los activos según criticidad?

Ilustración 5

Resultados entrevista técnica – pregunta 5.



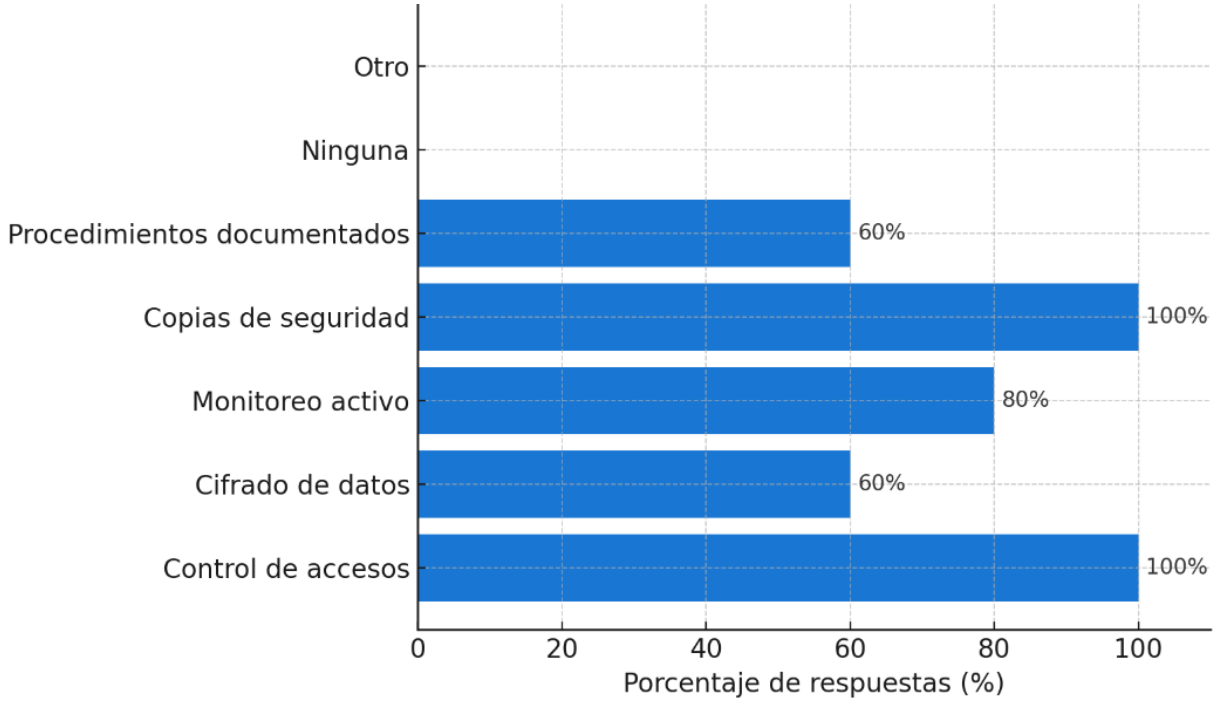
Fuente: Elaboración propia

El 80 % de los participantes indicó que la clasificación de activos según su criticidad está a cargo del Departamento de TI, mientras que un 20 % afirmó que este proceso no se realiza de manera formal. No se reportó participación de consultores externos ni de otras áreas, lo que evidencia que la responsabilidad recae principalmente en el equipo técnico interno. Esto refleja un liderazgo claro del área de TI, aunque también señala la necesidad de estandarizar y documentar este proceso, de forma que se garantice una mayor consistencia organizacional y se refuerce la trazabilidad en la toma de decisiones.

- Pregunta 6: ¿Cuál de las siguientes medidas de protección aplica a los activos identificados como críticos? (Marque todas las que correspondan)

Ilustración 6

Resultados de entrevista técnica para clasificación de activos – pregunta 6.



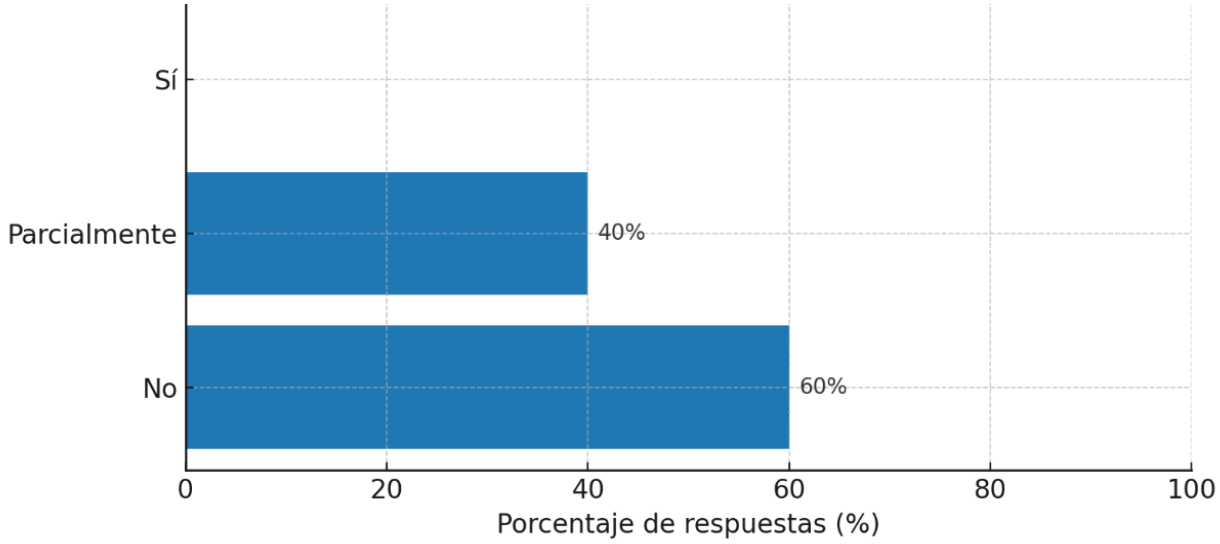
Fuente: Elaboración propia

El 100 % de los entrevistados afirmó que actualmente se aplican controles de acceso y se realizan copias de seguridad de manera sistemática. Además, un 80 % indicó que existe monitoreo activo de los sistemas, mientras que un 60 % señaló la implementación de mecanismos de cifrado de datos y la existencia de procedimientos documentados. Ninguno de los participantes seleccionó las opciones de “ninguna” ni “otro”, lo que demuestra que la organización ha desarrollado un esfuerzo integral para resguardar sus activos tecnológicos y de información.

- Pregunta 7: ¿Existe una matriz de riesgos que relacione los activos con su nivel de criticidad y protección?

Ilustración 7

Resultados de entrevista técnica para clasificación de activos – pregunta 7.



Fuente: Elaboración propia

El 60 % del personal indicó que no existe una matriz de riesgos que relacione de forma estructurada los activos con su nivel de criticidad y el grado de protección aplicado, mientras que un 40 % señaló que esta práctica se realiza de manera parcial o informal. Ninguno de los entrevistados confirmó la existencia de una matriz formal y documentada, lo que evidencia una brecha significativa en la gestión de riesgos de la organización, esta ausencia limita la capacidad de priorizar de manera objetiva las medidas de seguridad y dificulta la trazabilidad entre los activos más sensibles y los controles implementados.

Revisión Documental para Clasificación de Activos de Información

La presente revisión documental tuvo como objetivo identificar y clasificar los activos de información de Auxadi Costa Rica a partir de las políticas, procedimientos y registros internos disponibles. Este análisis permitió reconocer los elementos más relevantes para la operación diaria y evaluar el nivel de protección con que actualmente cuentan. La información obtenida servirá

como base para la elaboración de un inventario clasificado por nivel de criticidad, complementando los hallazgos de la entrevista técnica y asegurando su coherencia con los controles establecidos en la norma ISO/IEC 27001:2022, en el marco de la gestión de dispositivos, la seguridad en la comunicación y la protección de datos sensibles.

Documentos revisados para el análisis documental:

- Política de Seguridad de la Información.docx
- Política de Protección de Datos.docx
- Código Ético y de Conducta.pdf
- Gestión de Incidentes – Incident Management V2.docx
- Política de Gestión de Contraseñas.docx
- Procedimiento de Altas, Bajas y Modificaciones de Usuarios.docx
- Plan de Recuperación ante Desastres (DRP) V08.docx
- Plan de Continuidad de Negocio (BCP) V07.docx
- Procedimiento de Respaldo y Restauración de Datos.docx

Resultados de la revisión documental.

A partir de la revisión de estos documentos, se identificó que la organización cuenta con una base normativa y procedimental sólida que regula aspectos clave como el control de accesos, la administración segura de contraseñas, la gestión de incidentes, la continuidad del negocio y la protección de datos personales. Este conjunto de lineamientos refleja un esfuerzo constante por salvaguardar los recursos tecnológicos, garantizar la confidencialidad, integridad y disponibilidad de la información, y asegurar la continuidad de los servicios críticos frente a posibles contingencias. Además, la existencia de estos documentos fortalece la trazabilidad de las prácticas internas y brinda respaldo ante auditorías o evaluaciones externas, complementando y ampliando de manera significativa la información obtenida previamente durante la entrevista técnica.

El análisis documental permitió identificar detalles que no habían surgido en la entrevista, como la existencia de procedimientos específicos para respaldo y restauración de datos, referencias a la ubicación física y custodia de servidores, así como menciones concretas sobre plataformas

corporativas que soportan procesos financieros, administrativos y de comunicación. También se detectaron menciones indirectas a activos de soporte, como estaciones de trabajo especializadas y dispositivos de red, que no habían sido priorizados por el personal entrevistado, pero que desempeñan un papel fundamental para la operatividad diaria.

No obstante, pese a estos aportes, no se encontraron evidencias de una clasificación estructurada de los activos ni de un esquema formal que defina su criticidad, el impacto potencial ante una falla o la disponibilidad requerida. Tampoco se halló una matriz de riesgos que relacione de manera clara los activos con sus amenazas, vulnerabilidades y controles aplicados. Esta ausencia limita la capacidad de priorizar recursos de forma objetiva y de establecer medidas de protección diferenciadas según la relevancia estratégica de cada activo. Además, dificulta la trazabilidad de los riesgos en auditorías internas y reduce la posibilidad de anticipar escenarios críticos, lo que resalta la necesidad de formalizar un modelo que consolide estos elementos y fortalezca la gestión de seguridad de la información en la organización.

Los resultados de esta revisión confirman la necesidad de desarrollar un inventario clasificado que reúna toda la información disponible, tanto la obtenida en las entrevistas como la identificada en la documentación institucional. Dicho inventario deberá considerar criterios como función, criticidad, impacto, disponibilidad y dependencias, asegurando su alineación con los principios y buenas prácticas establecidos en la norma ISO/IEC 27001:2022, con el fin de fortalecer la gestión de activos de Auxadi Costa Rica y garantizar la continuidad de sus operaciones.

Resultados Inventario

La elaboración del inventario clasificado permitió consolidar en un solo registro la información obtenida mediante entrevistas técnicas y revisión documental, identificando los activos de información más relevantes para las operaciones de Auxadi Costa Rica. Este inventario refleja una visión integral que incluye activos físicos, lógicos y en la nube, clasificados según su función, nivel de criticidad, impacto ante una falla y disponibilidad requerida. Los resultados muestran que la organización cuenta con activos altamente críticos como servidores de

autenticación, ERP, plataformas de almacenamiento y sistemas de respaldo, los cuales requieren medidas de protección robustas y alta disponibilidad. Asimismo, se evidenció la existencia de activos de criticidad media o baja, cuya correcta gestión contribuye a la continuidad operativa y la reducción de riesgos. La formalización de este inventario representa un paso clave para priorizar recursos, definir controles alineados a la norma ISO/IEC 27001:2022 y fortalecer la trazabilidad en la gestión de activos.

Tabla 3

Inventario clasificado de activos con criterios de criticidad.

Activo de Información	**Tipo de Activo**	**Función Principal**	**Criticidad**	**Impacto ante Falla**	**Disponibilidad Requerida**
Servidor AD / Autenticación	Hardware / Software	Gestión de identidades, control de acceso y autenticación	Alta	Alto	24/7
Servidor de Archivos	Hardware / Software	Almacenamiento centralizado y compartición de documentos	Alta	Alto	24/7
Servidor ERP / Contabilidad	Hardware / Plataforma	Ejecución de sistema ERP y procesos contables/financieros	Alta	Alto	24/7
Servidor de Respaldo Local	Hardware / Software	Copias de seguridad para recuperación inmediata	Alta	Alto	24/7
Servidor de Desarrollo/Pruebas	Hardware / Software	Entorno de test para cambios y validaciones	Media	Media	Horario laboral
Servidor de Monitoreo/Logs	Hardware / Software	Registro y análisis de eventos para auditoría	Media-Alta	Media	24/7
Laptops – Dirección/Gerencia	Hardware	Equipos de trabajo con acceso a datos estratégicos y confidenciales	Alta	Alto	Horario laboral
Laptops – Personal Administrativo	Hardware	Ejecución de tareas administrativas y operativas	Media-Alta	Media	Horario laboral
Laptops – Personal de Soporte/Operativo	Hardware	Ejecución de tareas técnicas y soporte	Media	Media	Horario laboral
Sistemas de Respaldo en la Nube	Servicio / Software	Copias de seguridad remotas y redundancia	Alta	Alto	24/7

Correo Electrónico Corporativo	Servicio / Software	Comunicación interna y externa	Alta	Alto	24/7
Plataforma de Colaboración (Teams, SharePoint)	Servicio / Software	Comunicación y gestión documental	Media-Alta	Media	Horario laboral
Almacenamiento en la Nube (OneDrive, SharePoint)	Servicio / Software	Archivos compartidos y sincronización	Alta	Alto	24/7
Firewalls y Dispositivos de Red	Hardware	Seguridad perimetral y gestión de tráfico	Alta	Alto	24/7
Conexión VPN Corporativa	Servicio / Software	Acceso remoto seguro a la red corporativa	Alta	Alto	24/7
Aplicaciones Internas de Gestión	Software	Soporte a procesos internos específicos	Media	Media	Horario laboral
Dispositivos Móviles Corporativos	Hardware	Comunicación y acceso remoto ocasional	Baja	Baja	Acceso eventual

Fuente: Elaboración propia

Informe de Cumplimiento y Desviaciones

Objetivo del Informe

El presente informe se elabora como resultado de la auditoría documental realizada mediante listas de verificación y la comparación con los requisitos establecidos en la norma ISO/IEC 27001:2022. Su propósito es identificar el grado de cumplimiento actual en materia de seguridad de la información, así como detectar posibles desviaciones que puedan comprometer la eficacia del sistema de gestión. A partir de este análisis se busca proponer áreas de mejora que permitan fortalecer las políticas, procedimientos y controles internos, garantizando con ello una mayor alineación con las mejores prácticas internacionales y una base más sólida para la protección de los activos críticos en Auxadi Costa Rica.

Alcance de la Revisión

Se revisaron políticas, procedimientos, planes y registros oficiales relacionados con la gestión de la seguridad de la información, abarcando aspectos como el control de accesos, la protección de datos, la gestión de incidentes, la administración de contraseñas, la continuidad del negocio y el respaldo de información. Este proceso no se limitó únicamente al análisis documental, sino que se complementó con la aplicación de listas de verificación diseñadas con base en los controles de la norma ISO/IEC 27001:2022, lo que permitió reforzar la validez de los hallazgos y asegurar un contraste objetivo entre lo establecido formalmente y lo que realmente se aplica en la operación diaria. Gracias a la combinación de ambos instrumentos, se logró obtener una visión integral y precisa del nivel de formalización documental y su correspondencia con la ejecución práctica de los procesos críticos en Auxadi Costa Rica.

Revisión Documental de Cumplimiento de Políticas y Procedimientos de Seguridad

La revisión documental se llevó a cabo con el propósito de evaluar el nivel de cumplimiento de las políticas, procedimientos y registros de Auxadi Costa Rica frente a los requisitos establecidos en la norma ISO/IEC 27001:2022. Este análisis se basó en la verificación detallada de documentos clave, con el fin de identificar tanto las fortalezas consolidadas como las áreas de mejora que requieren atención prioritaria. Los resultados obtenidos constituyen la base para la elaboración del informe de cumplimiento y desviaciones, el cual orienta las acciones correctivas y el desarrollo de la propuesta técnica final.

Documentos revisados para el análisis documental:

- Política de Seguridad de la Información.docx
- Política de Protección de Datos.docx
- Código Ético y de Conducta.pdf
- Gestión de Incidentes – Incident Management V2.docx
- Política de Gestión de Contraseñas.docx
- Procedimiento de Altas, Bajas y Modificaciones de Usuarios.docx
- Plan de Recuperación ante Desastres (DRP) V08.docx

- Plan de Continuidad de Negocio (BCP) V07.docx
- Procedimiento de Respaldo y Restauración de Datos.docx

Resultados de la revisión documental.

El análisis permite confirmar que la organización dispone de un marco normativo y procedimental robusto que abarca aspectos fundamentales como el control de accesos, la gestión de contraseñas, el tratamiento de datos personales, la gestión de incidentes, la continuidad de negocio y el respaldo de información. Este conjunto de directrices evidencia un compromiso formal con la protección de los activos y también refleja un esfuerzo constante por adoptar prácticas alineadas a estándares internacionales, fortaleciendo la confianza en la capacidad de la empresa para garantizar la seguridad y la resiliencia de su entorno tecnológico.

Sin embargo, el estudio también revela brechas relevantes que impactan el nivel de cumplimiento esperado. Entre ellas, la ausencia de plazos formales para la baja de usuarios inactivos, la falta de aplicación homogénea de políticas de cambio periódico de contraseñas en todos los sistemas, y la carencia de un inventario clasificado y actualizado de activos de información que permita una trazabilidad completa.

En materia de protección de datos personales, se confirma que la organización cuenta con políticas formales y responsabilidades claramente definidas para el manejo de esta información. Sin embargo, la identificación exhaustiva de todos los sistemas que almacenan y procesan datos sensibles aún se encuentra incompleta, lo que genera vacíos en la trazabilidad y limita la capacidad de control integral. Esta situación podría afectar la rapidez y efectividad de la respuesta ante incidentes de seguridad, así como el nivel de preparación frente a auditorías regulatorias o requerimientos externos, evidenciando la necesidad de fortalecer los mecanismos de inventariado y clasificación de sistemas que gestionan información personal.

Respecto a la continuidad operativa, aunque los planes DRP y BCP contienen escenarios definidos, tiempos de recuperación establecidos y responsables claramente designados, no se encontró evidencia reciente de pruebas documentadas que validen de manera práctica su

efectividad real. Esta falta de validación limita la capacidad de garantizar que los procedimientos funcionen de forma adecuada en una situación crítica. Asimismo, se detecta que algunas políticas no han sido actualizadas en el último año, lo que reduce su vigencia frente a cambios tecnológicos y regulatorios, y que no existe un lineamiento formal de sanciones aplicables en caso de incumplimientos, lo que debilita la capacidad de control y la cultura de cumplimiento dentro de la organización.

El análisis también evidencia oportunidades de mejora en áreas complementarias como la ausencia de programas de capacitación formal y periódica en seguridad de la información, la falta de registros actualizados de auditorías internas específicas al SGSI, y la carencia de cláusulas contractuales estandarizadas que obliguen a proveedores externos a cumplir con requisitos de seguridad alineados a la ISO/IEC 27001:2022.

En conjunto, estos hallazgos permiten que, mediante el uso de listas de verificación, se establezca un informe de cumplimiento y desviaciones más completo, que no solo evidencie con claridad el estado actual de la seguridad de la información en Auxadi Costa Rica, sino que también proporcione insumos estratégicos para orientar las decisiones de mejora. Dicho informe facilitará la priorización de acciones correctivas, cerrará las brechas identificadas y reforzará la alineación con los controles exigidos por la norma ISO/IEC 27001:2022, contribuyendo a consolidar una gestión más robusta, confiable y adaptable a los retos tecnológicos y regulatorios actuales.

Listas de Verificación de Cumplimiento de Políticas y Procedimientos de Seguridad

Las listas de verificación se aplicaron en conjunto con la revisión documental y con el propósito de contrastar las políticas y procedimientos de Auxadi Costa Rica frente a los requisitos establecidos en la norma ISO/IEC 27001:2022. Este instrumento permite identificar de forma estructurada los controles que cumplen con la normativa y aquellos que presentan desviaciones, ofreciendo una visión clara del grado de madurez en la gestión de seguridad. A su vez, los resultados obtenidos proporcionan insumos objetivos y medibles que servirán para orientar de manera más precisa las acciones de mejora, así como para respaldar la construcción de la propuesta

final del proyecto, garantizando que esta se base en evidencias reales y necesidades detectadas dentro del contexto organizacional. Se utilizó el Apéndice B. Listas de Verificación 1.

Resultados de las listas de verificación.

Ilustración 8

Resultados de cumplimiento de políticas y procedimientos – lista de verificación 1.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
1.1	¿El procedimiento de altas y bajas documenta quién autoriza el acceso?	✓		El procedimiento documenta claramente la autoridad responsable de autorizar el acceso
1.2	¿Se establecen plazos para la baja de usuarios inactivos o desvinculados?		✗	No se especifican plazos concretos, lo que podría generar riesgos de acceso no autorizado
1.3	¿Se aplican contraseñas con longitud y complejidad adecuadas?	✓		Se exige un mínimo de 12 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales
1.4	¿Se exige el cambio periódico de contraseñas?		✗	No existe una política formal que establezca la frecuencia del cambio de contraseñas

Fuente: Elaboración propia

El análisis muestra que la organización tiene documentado el proceso de altas y bajas, especificando quién autoriza el acceso, y cumple con las prácticas recomendadas en cuanto a longitud y complejidad de contraseñas. Sin embargo, se detectaron dos áreas de mejora: no se definen plazos claros para la baja de usuarios inactivos y la política de cambio periódico de

contraseñas no se aplica de forma uniforme en todos los sistemas. Estas brechas, aunque no críticas, representan oportunidades para reforzar el cumplimiento de los controles de seguridad y alinear las prácticas a los requisitos de la norma ISO/IEC 27001:2022.

Ilustración 9

Resultados de cumplimiento de políticas y procedimientos – lista de verificación 2.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
2.1	¿Existe una política de protección de datos personales?	✓		La política de protección de datos establece lineamientos claros sobre el tratamiento y resguardo de información personal
2.2	¿Se definen responsabilidades en el tratamiento de datos sensibles?	✓		Se designan responsables específicos para la gestión de datos sensibles, con funciones documentadas
2.3	¿Se identifican los sistemas donde se almacena información personal?		✗	No existe un inventario completo y actualizado de los sistemas que almacenan datos personales, lo que limita la trazabilidad y control

Fuente: Elaboración propia

El análisis evidencia que la organización dispone de una base normativa sólida en materia de protección de datos personales, con políticas y responsabilidades definidas que cumplen con los lineamientos de la ISO/IEC 27001:2022. Sin embargo, se identificó como área de mejora la falta de un inventario exhaustivo y actualizado de los sistemas que contienen información personal, lo que representa una oportunidad para optimizar el control y la trazabilidad, así como para fortalecer la capacidad de respuesta ante incidentes y auditorías regulatorias.

Ilustración 10

Resultados de cumplimiento de políticas y procedimientos – lista de verificación 3.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
3.1	¿Existe un plan de continuidad documentado y vigente?	✓		El Plan de Continuidad de Negocio (BCP) se encuentra documentado y vigente, contemplando escenarios y procedimientos para mantener operaciones críticas
3.2	¿El plan contempla responsables, tiempos de recuperación y escenarios críticos?	✓		El BCP y el DRP establecen responsables claros, tiempos de recuperación y escenarios críticos, alineados a los riesgos identificados
3.3	¿Se realizan pruebas del plan de continuidad o recuperación?		✗	No se cuenta con evidencia reciente de pruebas documentadas que validen la efectividad y aplicabilidad real de los planes

Fuente: Elaboración propia

El análisis confirma que la organización dispone de planes de continuidad del negocio y recuperación ante desastres bien estructurados, que incluyen responsables, tiempos de recuperación y escenarios críticos definidos. Esto refleja un compromiso con la resiliencia operativa y la protección de los procesos esenciales. No obstante, se identificó que no se han realizado pruebas documentadas recientes, lo cual limita la capacidad de validar la efectividad práctica de dichos planes. Abordar esta brecha permitirá garantizar que los procedimientos establecidos funcionen de manera óptima en una situación real, asegurando la alineación con los requisitos de la norma ISO/IEC 27001:2022.

Ilustración 11

Resultados de cumplimiento de políticas y procedimientos – lista de verificación 4.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
4.1	¿Las políticas están aprobadas y firmadas por la alta dirección?	✓		La mayoría de las políticas cuentan con aprobación y firma formal de la alta dirección
4.2	¿Se incluye una política de sanciones ante incumplimientos de seguridad?		✗	No se identificó un lineamiento formal que defina sanciones específicas ante incumplimientos de seguridad.
4.3	¿Se establece un procedimiento para gestión de incidentes?	✓		Existe un procedimiento documentado y vigente para la gestión de incidentes de seguridad
4.4	¿Se han actualizado las políticas en el último año?		✗	Algunas políticas no han sido actualizadas en el último año, lo que podría afectar su vigencia frente a nuevos riesgos o cambios normativos

Fuente: Elaboración propia

El análisis muestra que la organización cuenta con un respaldo formal de la alta dirección en la aprobación de sus políticas de seguridad, así como con un procedimiento definido para la gestión de incidentes. Sin embargo, se evidenció la ausencia de una política de sanciones ante incumplimientos, lo que podría debilitar la aplicación de medidas disciplinarias y la cultura de cumplimiento. Además, se detectó que ciertas políticas no han sido actualizadas en el último año, lo que representa una oportunidad para reforzar su vigencia y asegurar que respondan a los riesgos actuales y a los requisitos de la norma ISO/IEC 27001:2022.

Resultados Informe

Auxadi Costa Rica presenta una base normativa y procedimental sólida en aspectos esenciales de la seguridad de la información, lo cual refleja un compromiso formal con la protección de los activos y el cumplimiento de buenas prácticas internacionales. No obstante, las desviaciones detectadas evidencian la necesidad de fortalecer la trazabilidad, asegurar una aplicación homogénea de los controles y garantizar la actualización periódica de las políticas. Asimismo, se requiere formalizar actividades críticas como los inventarios, las auditorías y los programas de capacitación, de manera que se consolide una gestión más integral y sostenible. Atender estas áreas permitirá incrementar el nivel de cumplimiento con la norma ISO/IEC 27001:2022, reducir riesgos, reforzar la resiliencia operativa de la organización y mejorar la capacidad de respuesta ante incidentes o auditorías externas.

Fortalezas detectadas.

- Control de accesos: Existe un procedimiento documentado para la gestión de altas y bajas de usuarios, en el cual se identifica claramente la autoridad responsable de aprobar cada acceso. Este mecanismo constituye una base sólida para asegurar la trazabilidad de privilegios y reducir la posibilidad de accesos indebidos, aunque aún puede complementarse con controles automatizados que refuercen su efectividad.
- Gestión de contraseñas: Se exige un mínimo de 12 caracteres con combinación de mayúsculas, minúsculas, números y caracteres especiales, cumpliendo con las mejores prácticas de seguridad. Esta medida asegura un nivel adecuado de protección, aunque podría fortalecerse con políticas de caducidad periódica y la integración de autenticación multifactor en todos los sistemas críticos.
- Protección de datos: Se cuenta con políticas específicas para el tratamiento de datos personales y confidenciales, donde se definen roles y responsabilidades en el manejo de esta información. Esto constituye una fortaleza en términos de cumplimiento legal, aunque su alcance requiere consolidarse con mecanismos más formales de seguimiento y socialización entre todo el personal.

- Continuidad y recuperación: La organización dispone de planes formales de recuperación ante desastres (DRP) y continuidad de negocio (BCP), con responsables asignados y tiempos de recuperación establecidos. Este marco representa un avance en resiliencia operativa, aunque aún se requiere mayor frecuencia en las pruebas y la documentación de sus resultados.
- Gestión de incidentes: Existe un procedimiento vigente para la notificación, registro y tratamiento de incidentes de seguridad, lo que refleja una estructura organizada para responder a eventos críticos. Sin embargo, debe reforzarse la estandarización del registro y la trazabilidad del cierre de cada caso.
- Respaldo de información: Se documenta una política y procedimiento para la realización de copias de seguridad, con frecuencia semanal y almacenamiento seguro fuera de sitio. Esto garantiza un nivel mínimo de protección frente a pérdidas de información, aunque sería conveniente ampliar la cobertura a respaldos diarios para los sistemas de mayor criticidad.

Desviaciones y oportunidades de mejora.

- Plazos para baja de usuarios inactivos: No se especifican plazos formales para la desactivación de cuentas inactivas, lo que podría generar riesgos de accesos no autorizados. Formalizar este proceso es esencial para garantizar mayor control y reducir brechas de seguridad.
- Cambio periódico de contraseñas: Aunque existe una recomendación general, no se aplica de manera uniforme en todos los sistemas, especialmente en plataformas heredadas. Esta inconsistencia debilita el nivel de seguridad y debe ser atendida con políticas homogéneas en toda la infraestructura.
- Inventario de activos: No se dispone de un inventario clasificado y actualizado de todos los activos de información, lo que dificulta la trazabilidad, la priorización de medidas de protección y la correcta asignación de recursos de seguridad. La creación de este inventario es una necesidad inmediata.
- Sistemas con datos personales: La identificación de todos los sistemas que almacenan datos personales sigue siendo incompleta, lo que limita la capacidad de control,

seguimiento y respuesta ante auditorías o incidentes regulatorios. Completar este mapeo fortalecerá la gestión de riesgos.

- Pruebas de continuidad y recuperación: No se encontró evidencia reciente de pruebas documentadas que validen la efectividad real de los planes DRP y BCP. La ausencia de estos ejercicios reduce la confianza en su aplicabilidad y efectividad ante contingencias reales.
- Actualización de políticas: Algunas políticas de seguridad y protección de datos no han sido revisadas ni actualizadas en el último año, lo que limita su vigencia frente a cambios tecnológicos y regulatorios. Establecer un calendario de revisiones periódicas resolvería esta limitación.
- Sanciones por incumplimiento: No existe un lineamiento formal que establezca sanciones específicas en caso de incumplimiento de las políticas y procedimientos. Esta carencia debilita el marco normativo interno y resta fuerza a la aplicación de controles.
- Concientización y formación: No se evidencian programas formales ni periódicos de capacitación en seguridad de la información para todo el personal. Esta situación incrementa el riesgo de errores humanos y requiere acciones inmediatas para elevar el nivel de madurez organizacional.
- Gestión de proveedores: No hay evidencia de cláusulas contractuales estandarizadas que obliguen a los proveedores externos a cumplir con requisitos de seguridad alineados a la ISO/IEC 27001:2022. Esta omisión representa un riesgo que debe atenderse para garantizar una cadena de valor segura.
- Auditorías internas: No se encontraron registros recientes de auditorías internas específicas al sistema de gestión de seguridad de la información, lo que limita la capacidad de supervisión continua. Implementar auditorías periódicas reforzará la gobernanza y el cumplimiento normativo.

Informe de Clasificación de Riesgos

Objetivo del Informe

El presente informe tiene como propósito identificar, analizar y clasificar los principales riesgos que afectan la seguridad de la información en Auxadi Costa Rica, considerando tanto la percepción del personal técnico como la documentación institucional vigente. Esta evaluación tiene como fin priorizar los riesgos según su nivel de criticidad, entendida como la combinación entre el impacto potencial de una amenaza y la probabilidad de que esta ocurra, sirviendo como base técnica para el diseño de políticas, controles y procedimientos alineados con los requisitos de la norma ISO/IEC 27001:2022.

Alcance de la Revisión

El análisis incluyó la aplicación de encuestas estructuradas al equipo técnico de la organización, así como una revisión documental de las políticas, procedimientos y registros relacionados con la seguridad de la información. La evaluación abarcó aspectos clave como el uso y protección de dispositivos, control de accesos, comportamiento del usuario, transmisión de datos y gestión operativa de incidentes. Los resultados obtenidos se analizaron mediante categorización de riesgos según impacto y probabilidad, representándose gráficamente para facilitar su interpretación y posterior tratamiento.

Encuesta de Percepción Sobre Riesgos de Seguridad de la Información

Resultados de la encuesta de percepción.

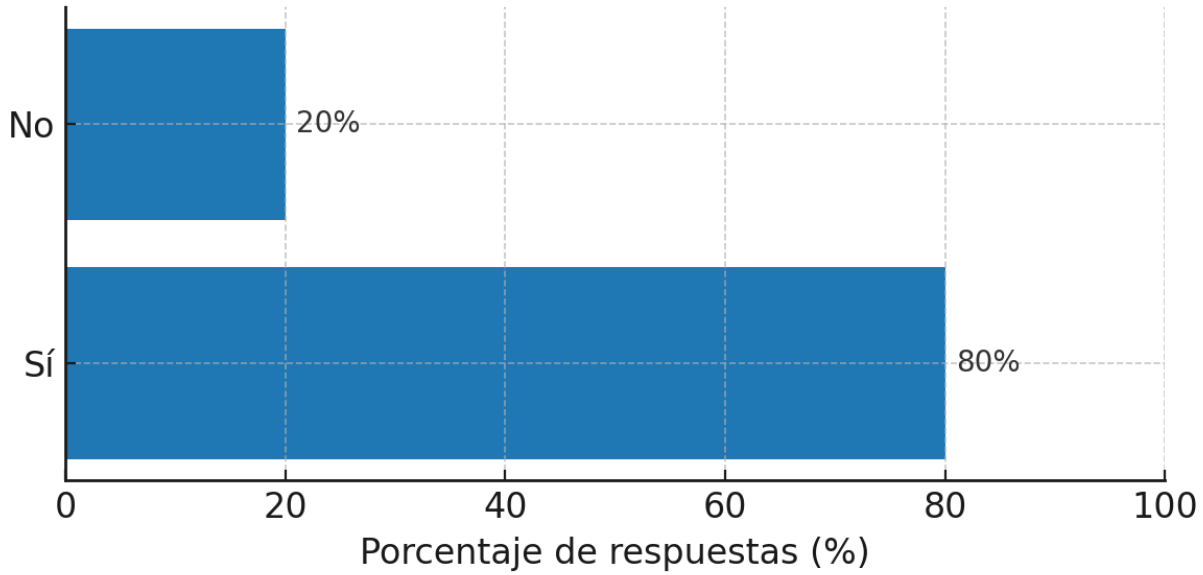
La siguiente encuesta fue aplicada a cinco colaboradores del equipo técnico de Auxadi Costa Rica con el fin de identificar la percepción del personal sobre los riesgos más frecuentes que afectan la seguridad de la información en el entorno digital de la empresa. A través de esta herramienta se busca comprender el nivel de cumplimiento de buenas prácticas, detectar posibles brechas y evaluar el impacto potencial de situaciones como el uso inadecuado de dispositivos, la

exposición de datos sensibles o la falta de medidas de protección. Los resultados obtenidos se representarán mediante gráficos estadísticos y permitirán clasificar los riesgos según su impacto y probabilidad, sentando las bases para desarrollar una propuesta de políticas y procedimientos alineados con la norma ISO/IEC 27001:2022. Se utilizó el Apéndice C. Encuesta 1.

- Pregunta 1: ¿Ha detectado prácticas inseguras en el uso de dispositivos corporativos?

Ilustración 12

Resultados de encuesta de percepción sobre riesgos – pregunta 1.



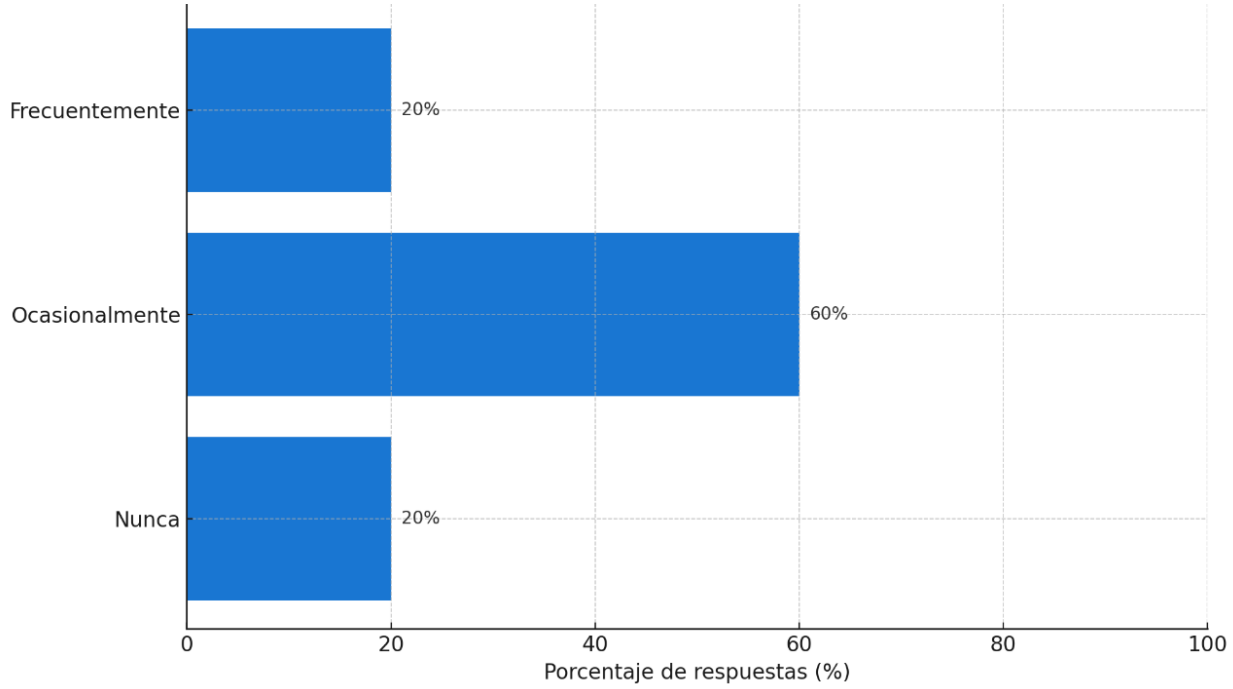
Fuente: Elaboración propia

Los resultados evidencian que el 80 % del personal de TI ha identificado prácticas inseguras en el manejo de dispositivos corporativos, lo que pone de manifiesto la existencia de conductas que podrían comprometer la seguridad de la información y la integridad de los activos tecnológicos. Solo un 20 % afirmó no haber observado este tipo de situaciones, lo que confirma que la mayoría de los encuestados reconoce áreas de mejora en la aplicación de controles y en la concientización del personal, esto resalta la necesidad de fortalecer las políticas de uso seguro, así como de reforzar los programas de capacitación que promuevan buenas prácticas en el manejo cotidiano de los dispositivos.

- Pregunta 2: ¿Con qué frecuencia comparte información sensible por correo o WhatsApp?

Ilustración 13

Resultados de encuesta de percepción sobre riesgos – pregunta 2.



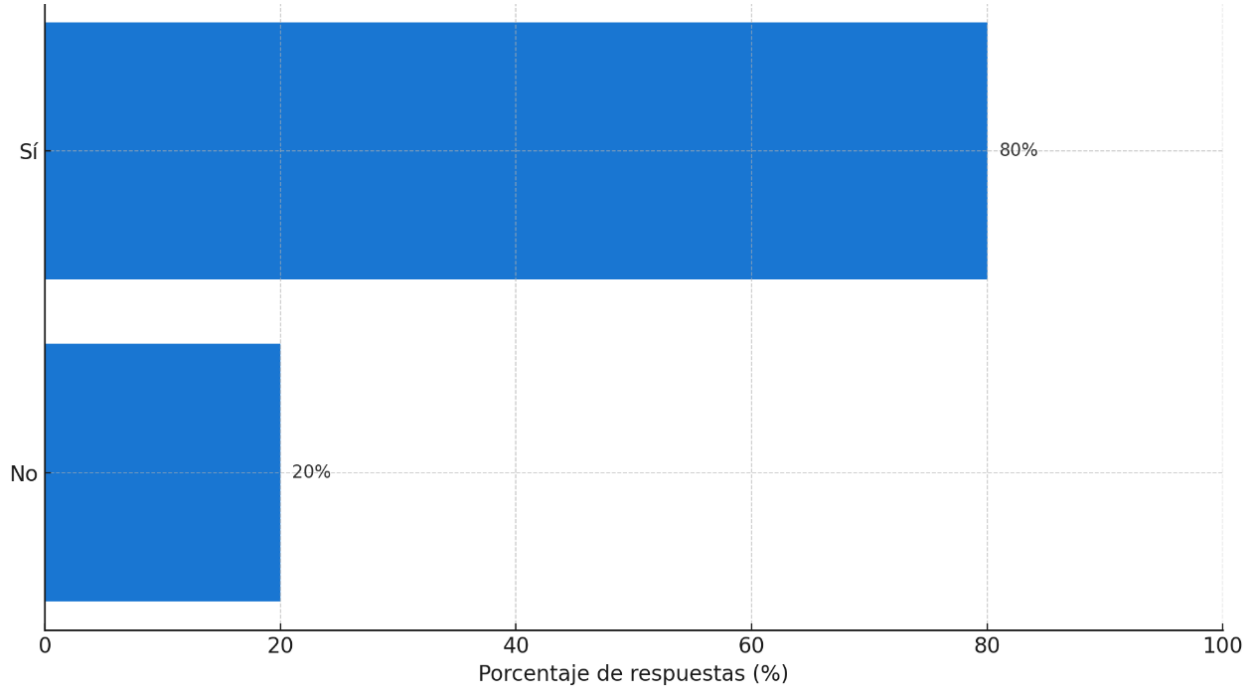
Fuente: Elaboración propia

Los resultados indican que un 60% del personal de TI comparte información sensible de manera ocasional, generalmente en casos de coordinación interna o soporte técnico. Un 20% manifestó hacerlo frecuentemente, lo que podría incrementar el riesgo si no se utilizan medios seguros de transmisión. Otro 20% señaló que nunca realiza este tipo de prácticas, evidenciando apego estricto a las políticas de seguridad establecidas. Este hallazgo sugiere la necesidad de reforzar la capacitación y el uso de canales cifrados para la comunicación de datos críticos.

- Pregunta 3: ¿Ha recibido capacitación reciente sobre seguridad de la información?

Ilustración 14

Resultados de encuesta de percepción sobre riesgos – pregunta 3.



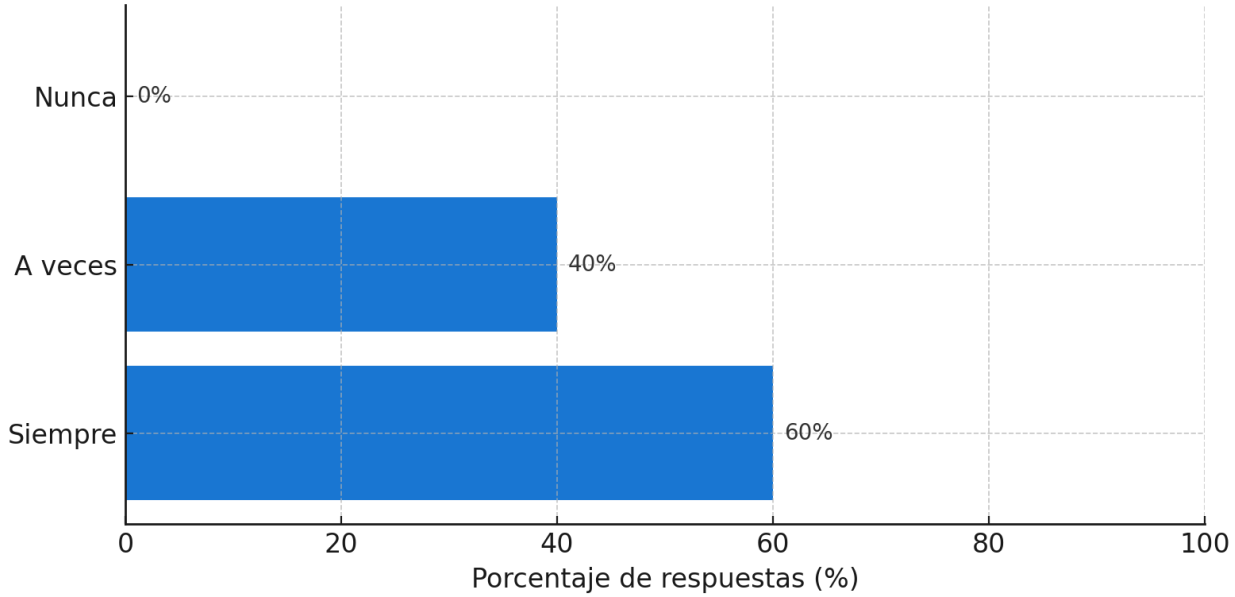
Fuente: Elaboración propia

El 80 % de los colaboradores encuestados indicó haber recibido capacitación reciente en seguridad de la información, lo que evidencia un nivel positivo de actualización en prácticas seguras y un esfuerzo institucional por fortalecer la cultura de protección de datos. No obstante, el 20 % restante no ha tenido formación en el mismo periodo, lo que representa una brecha que debe atenderse para asegurar una cobertura total. Esta situación constituye una oportunidad para ampliar y sistematizar los programas de capacitación, garantizando que todo el personal clave se mantenga alineado con las políticas y procedimientos de seguridad vigentes y que la concientización en buenas prácticas sea homogénea en toda la organización.

- Pregunta 4: ¿Utiliza contraseñas seguras (largas, combinadas, únicas)?

Ilustración 15

Resultados de encuesta de percepción sobre riesgos – pregunta 4.



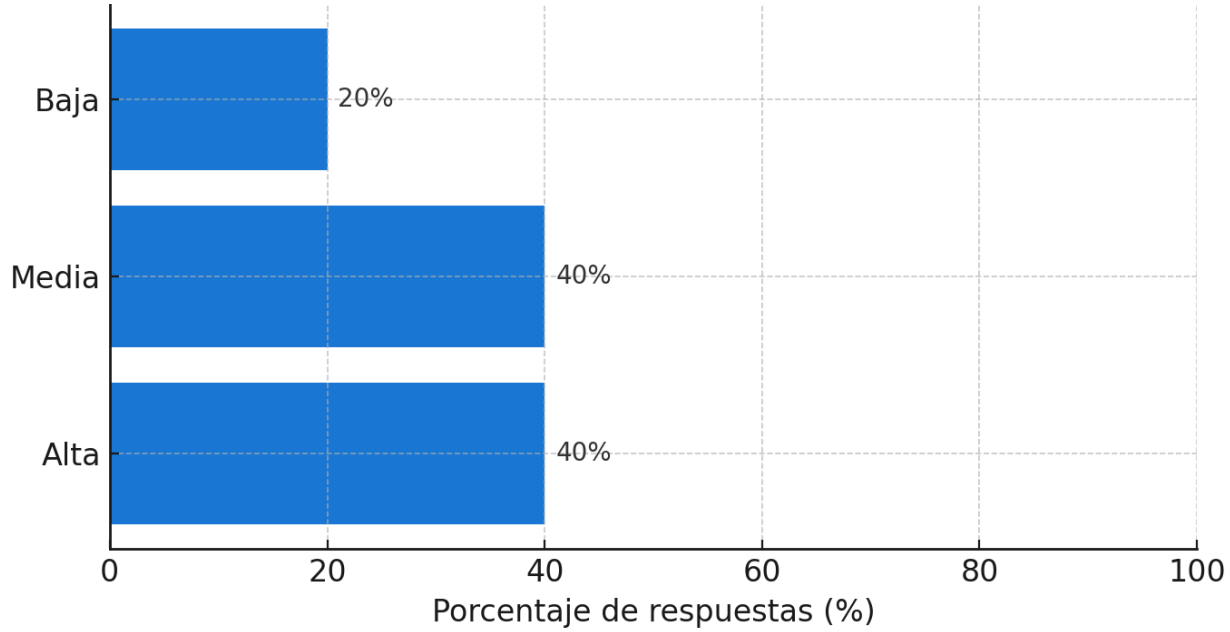
Fuente: Elaboración propia

El 60% del personal de TI indicó que utiliza siempre contraseñas seguras, combinando longitud, complejidad y unicidad, lo que demuestra una práctica sólida alineada con las políticas de seguridad. Un 40% reconoció aplicarlas solo a veces, lo que sugiere posibles brechas en cuentas secundarias o servicios menos críticos. No se registraron casos de uso de contraseñas inseguras, lo que refleja un nivel de madurez alto, aunque aún existe oportunidad de reforzar la cultura de seguridad para asegurar una adopción uniforme.

- Pregunta 5: ¿Cuál es la probabilidad de que ocurra una filtración de datos por error humano?

Ilustración 16

Resultados de encuesta de percepción sobre riesgos – pregunta 5.



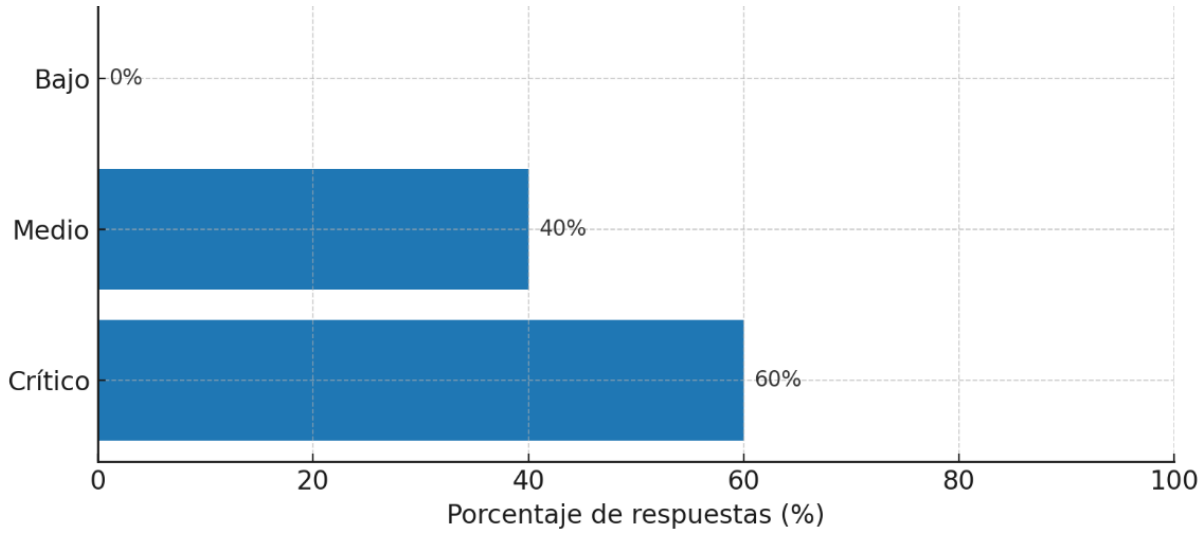
Fuente: Elaboración propia

El 40 % del personal de TI considera alta la probabilidad de una filtración de datos por error humano, mientras que otro 40 % la percibe como media. Solo un 20 % la califica como baja, lo que confirma que la mayoría reconoce este factor como un riesgo latente dentro de las operaciones diarias. Estos resultados reflejan una preocupación significativa en torno al impacto que pueden tener los errores operativos en la seguridad de la información, evidenciando que la vulnerabilidad humana sigue siendo uno de los puntos más críticos en la gestión de riesgos, todo esto sugiere la necesidad de reforzar de manera constante los programas de capacitación y establecer controles preventivos más rigurosos que ayuden a minimizar la ocurrencia de incidentes por descuido o falta de concientización.

- Pregunta 6: ¿Cuál sería el impacto si se pierde el acceso a un dispositivo que no cuenta con respaldo ni cifrado?

Ilustración 17

Resultados de encuesta de percepción sobre riesgos – pregunta 6.



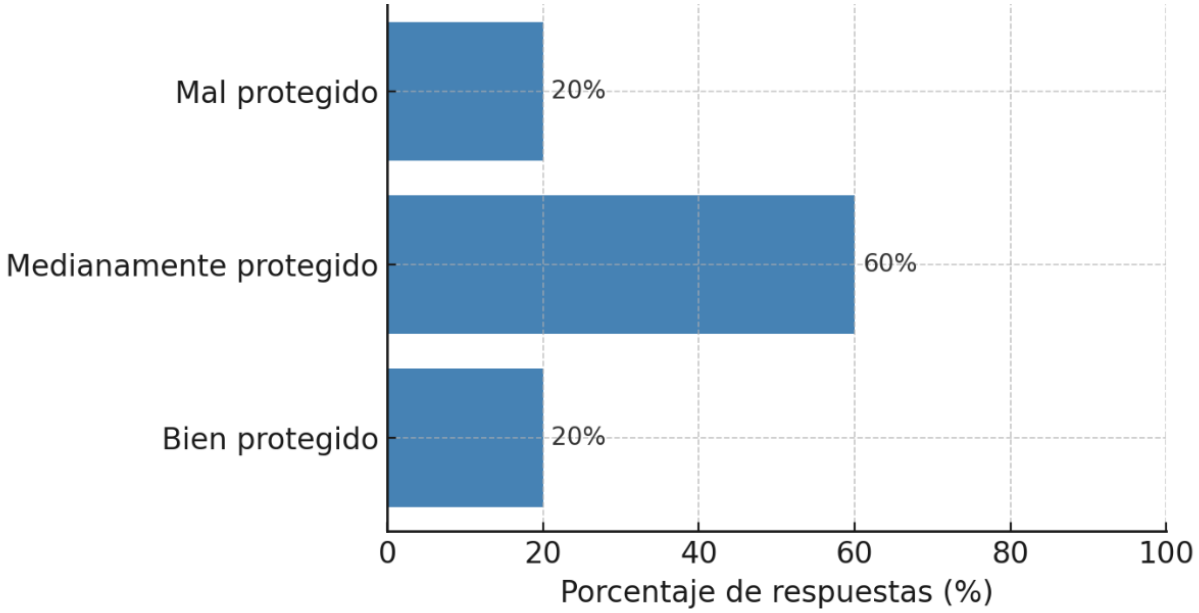
Fuente: Elaboración propia

El 60 % del personal de TI considera que la pérdida de acceso a un dispositivo sin respaldo ni cifrado tendría un impacto crítico, reflejando un alto nivel de conciencia sobre la importancia de la continuidad operativa y la protección de datos sensibles. El 40 % indicó que el impacto sería medio, probablemente contemplando escenarios donde algunos datos pueden ser recuperados por otros medios o sistemas redundantes. Ningún encuestado seleccionó la opción de impacto bajo, lo cual es coherente con el entorno técnico de la empresa, donde los dispositivos gestionan información esencial para la operación diaria.

- Pregunta 7: ¿Qué tan protegido cree que está el entorno digital de la empresa actualmente?

Ilustración 18

Resultados de encuesta de percepción sobre riesgos – pregunta 7.



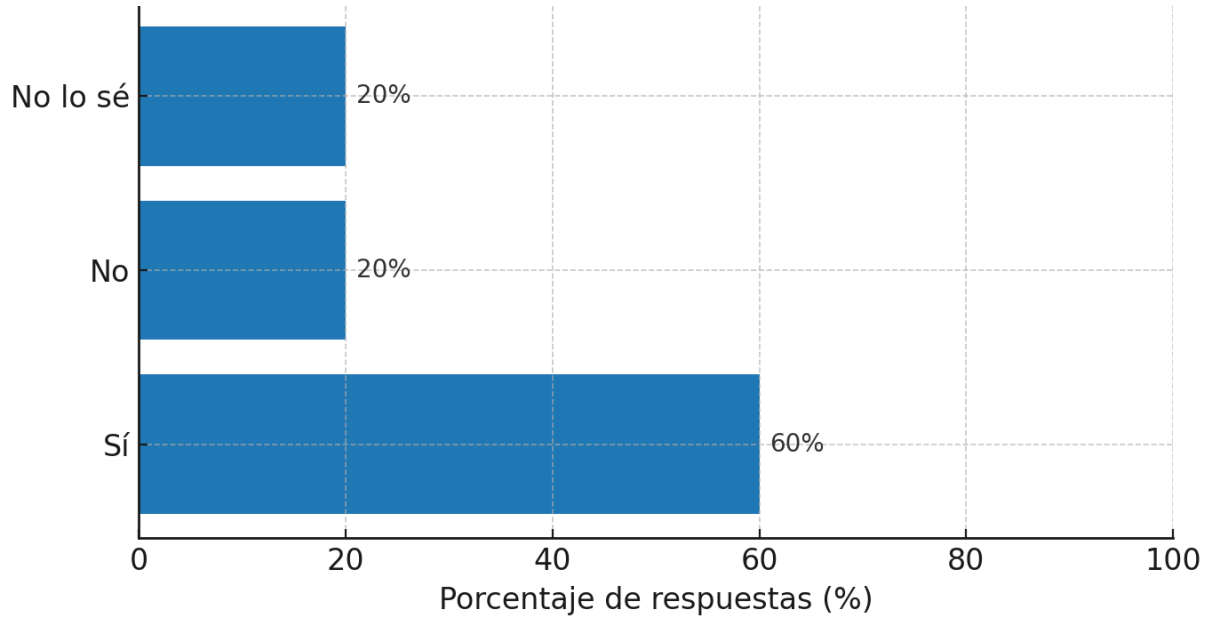
Fuente: Elaboración propia

Según los datos recolectados, el 60 % del personal técnico considera que el entorno digital de la empresa está medianamente protegido, lo que sugiere que, si bien existen medidas básicas de seguridad implementadas, aún persisten áreas que requieren fortalecimiento. Por otro lado, un 20 % lo califica como bien protegido, mientras que otro 20 % lo percibe como mal protegido, lo que pone en evidencia percepciones dispares entre los colaboradores respecto al nivel de madurez alcanzado. Esta diferencia de criterios refleja que la seguridad, aunque presente, no se percibe de forma uniforme dentro de la organización y señala la necesidad de consolidar controles más consistentes y de reforzar la comunicación sobre las medidas aplicadas.

- Pregunta 8: ¿Ha visto casos donde varios usuarios comparten una misma cuenta o acceso?

Ilustración 19

Resultados de encuesta de percepción sobre riesgos – pregunta 8.



Fuente: Elaboración propia

El 60 % del personal técnico indicó haber observado casos en los que varios usuarios comparten una misma cuenta o acceso dentro de la infraestructura digital de la empresa. Un 20 % afirmó que no ha sido testigo de esta práctica, mientras que otro 20 % expresó no tener certeza sobre ello. Estos resultados reflejan una situación de riesgo latente en la gestión de accesos, ya que el uso compartido de credenciales debilita los mecanismos de trazabilidad, control y responsabilidad individual.

Revisión Documental para Informe de Clasificación de Riesgos

La revisión documental efectuada en esta sección tuvo como objetivo respaldar de forma objetiva el análisis de riesgos detectados en las áreas de gestión de dispositivos, control de accesos, comunicación de información y comportamiento del usuario. Para ello, se examinó un conjunto de

políticas, procedimientos internos y registros operativos vinculados a la seguridad de la información, con el fin de identificar fortalezas, vacíos y oportunidades de mejora que pudieran influir directamente en la probabilidad e impacto de ocurrencia de los eventos considerados más críticos.

Documentos revisados para el análisis documental:

- Política de Seguridad de la Información.docx
- Política de Protección de Datos.docx
- Código Ético y de Conducta.pdf
- Gestión de Incidentes – Incident Management V2.docx
- Política de Gestión de Contraseñas.docx
- Procedimiento de Altas, Bajas y Modificaciones de Usuarios.docx
- Plan de Recuperación ante Desastres (DRP) V08.docx
- Plan de Continuidad de Negocio (BCP) V07.docx
- Procedimiento de Respaldo y Restauración de Datos.docx

Resultados de la revisión documental.

En este proceso se evidencia que, aunque Auxadi Costa Rica dispone de un marco documental que aborda elementos clave como la protección de datos, la recuperación ante desastres, la gestión de usuarios y la seguridad en las comunicaciones, varios de estos lineamientos presentan limitaciones técnicas o carecen de un desarrollo operativo que garantice su cumplimiento efectivo. Por ejemplo, se detectaron debilidades en el nivel de detalle de los procedimientos de respaldo y restauración, donde no se encontraron evidencias de pruebas de recuperación o de validaciones periódicas que aseguren la disponibilidad real de los datos ante una eventual pérdida. Esto representa un factor de riesgo relevante, considerando la criticidad de los activos de información.

Asimismo, se observa que las políticas de acceso y gestión de cuentas no contemplan mecanismos automatizados de control ni una trazabilidad suficientemente robusta sobre los privilegios asignados. Esta ausencia de controles técnicos incrementa la posibilidad de accesos

indebidos, especialmente si se toma en cuenta que los registros operativos no evidencian auditorías frecuentes sobre el uso compartido de credenciales ni revisiones sistemáticas de cuentas inactivas. En paralelo, se identifica que los documentos relacionados con la concientización del personal carecen de un enfoque estructurado de sensibilización continua, limitándose en su alcance y periodicidad, esta situación podría incidir de manera directa en el nivel de exposición frente a errores humanos y malas prácticas en el uso de los canales de comunicación, lo que resalta la necesidad de fortalecer tanto el control técnico como la formación permanente de los colaboradores.

Por otro lado, los planes de continuidad y recuperación de negocio revisados presentaron escenarios genéricos que no contemplan situaciones específicas como la pérdida o robo de dispositivos portátiles, ni procedimientos detallados para contener incidentes vinculados al uso de redes no seguras fuera de la oficina. Esta omisión representa una limitación importante, ya que dichos escenarios son cada vez más comunes en entornos de teletrabajo y movilidad. La ausencia de protocolos claros que orienten una respuesta rápida y coordinada ante estos eventos podría derivar en un impacto operativo considerable, afectando tanto la disponibilidad de los servicios como la confidencialidad de la información crítica.

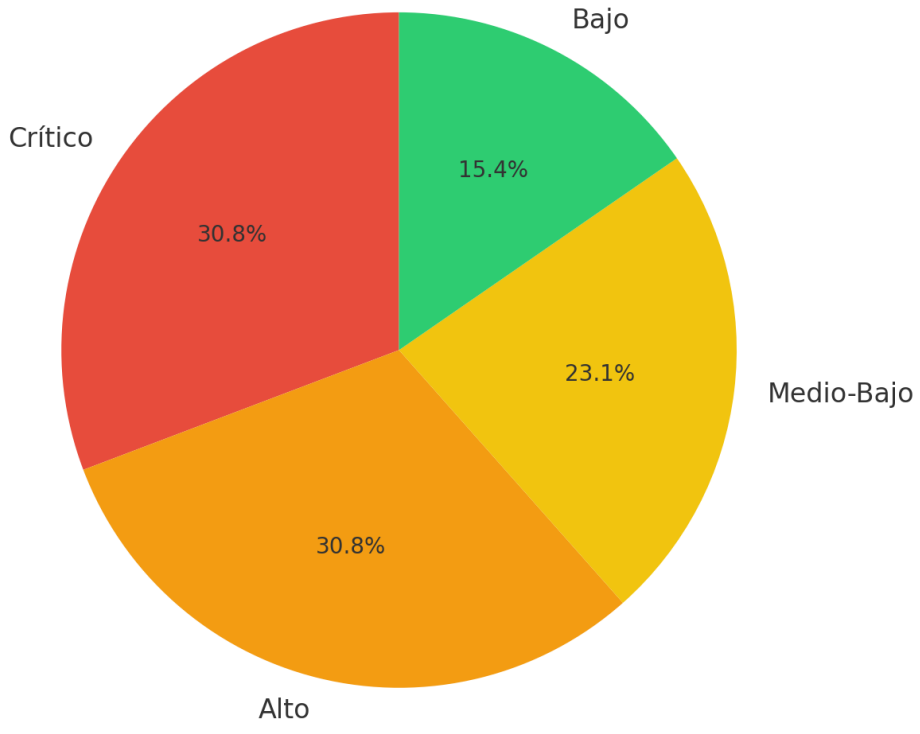
A partir del análisis anterior, fue posible clasificar de manera más precisa los riesgos identificados, considerando no solo las percepciones del personal técnico, sino también el grado de madurez de los controles actuales. Esta combinación de elementos documentales y observaciones operativas permitió asignar niveles objetivos de probabilidad e impacto a cada riesgo, facilitando su jerarquización y posterior tratamiento en la propuesta técnica del proyecto. En consecuencia, la revisión documental se consolida como un insumo clave para validar la necesidad de fortalecer el sistema de gestión de seguridad de la información, mediante la implementación de controles específicos, campañas de sensibilización efectivas y actualizaciones periódicas de los procedimientos existentes, todo esto en conformidad con la norma ISO/IEC 27001:2022.

Resultados Informe

El análisis integral realizado permite confirmar que Auxadi Costa Rica enfrenta riesgos de seguridad significativos relacionados con la gestión de dispositivos, control de accesos y factores humanos. La combinación entre la percepción técnica, los hallazgos documentales y el análisis lógico revela que varios escenarios críticos tienen una alta probabilidad de ocurrencia y podrían generar un impacto directo en la disponibilidad, integridad y confidencialidad de la información. Estos resultados refuerzan la urgencia de implementar políticas y procedimientos actualizados, priorizando aquellas áreas donde los controles existentes son insuficientes o inexistentes. Esta clasificación estructurada de los riesgos representa un insumo fundamental para definir medidas concretas alineadas con la norma ISO/IEC 27001:2022, enfocadas en garantizar la continuidad operativa y la protección efectiva de los activos de información de la organización.

Ilustración 20

Distribución de riesgos por clasificación.



Fuente: Elaboración propia

El gráfico muestra que la mayoría de los riesgos identificados se concentran en las categorías Crítico y Alto, representando cada una un 30.8 % del total. Este resultado evidencia una alta exposición a escenarios que podrían comprometer de forma directa la confidencialidad, integridad o disponibilidad de la información en Auxadi Costa Rica. Por otro lado, un 23.1 % corresponde a riesgos Moderados o parcialmente controlados, y solo un 15.4 % a riesgos Menores, lo que indica que, si bien existen controles básicos implementados, todavía se requiere un mayor grado de formalización y seguimiento continuo. Esta distribución resalta la urgencia de priorizar acciones correctivas en los niveles más críticos, con el objetivo de mejorar la gestión de la seguridad y alcanzar una alineación más sólida con los lineamientos de la norma ISO/IEC 27001:2022.

Riesgos críticos (alta probabilidad + alto impacto).

Pérdida de dispositivos sin respaldo ni cifrado.

- Impacto: Alto
- Probabilidad: Alta
- Clasificación: Crítico
- Observación: La falta de cifrado y respaldo automatizado en laptops o dispositivos móviles puede provocar pérdida total de datos confidenciales ante robos, daños o extravíos. Este riesgo compromete tanto la disponibilidad como la integridad de la información, y actualmente no existe evidencia de políticas técnicas que aseguren su mitigación efectiva.

Uso compartido de cuentas.

- Impacto: Alto
- Probabilidad: Alta
- Clasificación: Crítico
- Observación: Se identificó que no existen controles formales para evitar esta práctica, lo que dificulta la trazabilidad de accesos y eleva el riesgo de ingresos no autorizados

o de errores humanos sin responsables claramente definidos. Esta carencia limita la capacidad de control y seguimiento, generando un punto débil en la gestión de seguridad.

Filtraciones por error humano.

- Impacto: Alto
- Probabilidad: Media
- Clasificación: Crítico
- Observación: Estas filtraciones incluyen correos mal enviados, archivos adjuntos incorrectos o información compartida por canales no seguros. Aunque se reconocen buenas prácticas en algunos documentos, no hay programas de sensibilización vigentes que reduzcan su ocurrencia.

Accesos sin control a información sensible.

- Impacto: Alto
- Probabilidad: Media
- Clasificación: Crítico
- Observación: La documentación muestra una falta de segmentación clara en carpetas compartidas y en los accesos a diferentes plataformas, lo que facilita que usuarios sin la debida autorización puedan visualizar o incluso manipular información crítica. Esta debilidad incrementa el riesgo de exposición de datos sensibles y refleja la necesidad de aplicar controles más estrictos en la asignación y gestión de privilegios.

Riesgos altos (uno de los dos criterios en nivel alto).

Transmisión de datos sensibles por canales no cifrados.

- Impacto: Medio
- Probabilidad: Media

- Clasificación: Alto
- Observación: En ausencia de políticas que regulen el uso de herramientas de mensajería instantánea o de correos electrónicos sin cifrado, se genera un riesgo de exposición de información confidencial, particularmente en contextos de soporte técnico o de coordinación remota. Esta carencia incrementa la posibilidad de que datos sensibles sean transmitidos por canales no seguros.

Uso inconsistente de contraseñas robustas.

- Impacto: Medio
- Probabilidad: Alta
- Clasificación: Alto
- Observación: La política de contraseñas no ha sido actualizada recientemente y aún se detectan prácticas como la reutilización de claves o el uso de combinaciones demasiado simples. Esta situación incrementa el riesgo frente a ataques por fuerza bruta o accesos indebidos, al no garantizar un nivel de robustez suficiente en la protección de credenciales.

Dispositivos personales en redes corporativas (BYOD).

- Impacto: Medio
- Probabilidad: Media
- Clasificación: Alto
- Observación: No se identificaron medidas de control específicas ni esquemas de segmentación de red que permitan aislar estos dispositivos, lo que representa una vía de entrada potencial para malware o una posible pérdida de información sensible. Esta ausencia de controles técnicos aumenta la exposición a riesgos que podrían comprometer la continuidad operativa y la seguridad de los datos.

Falta de doble autenticación en accesos remotos.

- Impacto: Alto
- Probabilidad: Baja
- Clasificación: Alto
- Observación: Aunque existen mecanismos de MFA, estos no se encuentran aplicados a todos los accesos críticos. Esta omisión deja expuestas ciertas plataformas sensibles frente a posibles intentos de acceso remoto no autorizado, incrementando la vulnerabilidad de los sistemas más relevantes para la operación. Esta situación refleja una cobertura parcial que podría afectar directamente la capacidad de prevención y respuesta ante amenazas externas.

Riesgos moderados o parcialmente controlados.

Capacitación poco frecuente en seguridad.

- Impacto: Medio
- Probabilidad: Baja
- Clasificación: Medio-Bajo
- Observación: Aunque se han desarrollado sesiones informativas, estas no siguen una periodicidad definida ni incluyen contenidos sobre las amenazas más actuales. Esta limitación reduce la efectividad del conocimiento práctico del personal y dificulta que se mantenga una preparación constante frente a riesgos emergentes.

Ausencia de monitoreo sobre prácticas inseguras.

- Impacto: Bajo
- Probabilidad: Media
- Clasificación: Medio-Bajo
- Observación: No se evidenció un sistema proactivo de auditoría que permita detectar acciones como el uso de dispositivos USB sin control, conexiones inseguras o comportamientos fuera de norma. Esta ausencia limita la capacidad de anticiparse a

incidentes y reduce la efectividad del monitoreo sobre prácticas que pueden comprometer la seguridad de la información.

Uso de software sin verificar actualizaciones.

- Impacto: Bajo
- Probabilidad: Media
- Clasificación: Medio-Bajo
- Observación: Algunas estaciones aún dependen de actualizaciones manuales o parciales, lo que puede dejar vulnerabilidades sin resolver durante lapsos extensos. Esta situación incrementa el riesgo de explotación por amenazas conocidas y refleja la necesidad de consolidar un proceso automatizado y uniforme de gestión de parches.

Riesgos menores.

Nivel general de protección percibido como adecuado.

- Impacto: Bajo
- Probabilidad: Baja
- Clasificación: Bajo
- Observación: La mayoría del personal mantiene una percepción positiva del entorno de seguridad; sin embargo, esta valoración no necesariamente refleja la implementación completa de los controles exigidos por la norma. Esta diferencia entre percepción y práctica evidencia la necesidad de reforzar la verificación objetiva del cumplimiento y no depender únicamente de la opinión del personal.

Registros de incidentes menores no documentados.

- Impacto: Bajo
- Probabilidad: Baja
- Clasificación: Bajo

- Observación: Aunque existe una política formal de gestión de incidentes, los eventos menores no se documentan de manera sistemática, lo que limita el aprendizaje preventivo y reduce la efectividad de la mejora continua. Esta falta de registro detallado impide generar estadísticas completas y restringe la posibilidad de anticiparse a patrones recurrentes que podrían derivar en incidentes de mayor impacto.

Matriz de Control de Accesos y Permisos

Objetivo de la Matriz

El presente apartado se desarrolla con el fin de evaluar cómo se gestionan actualmente los accesos y privilegios de los usuarios en Auxadi Costa Rica, identificando los controles existentes, su nivel de formalización y los criterios utilizados para la asignación de permisos en los sistemas críticos. A partir de este análisis se construye una matriz estructurada que permita registrar de forma clara los niveles de acceso, los responsables de autorización, los medios de autenticación y la periodicidad de revisión, con el objetivo de alinear la gestión de accesos a los principios establecidos por la norma ISO/IEC 27001:2022 y reforzar la trazabilidad, seguridad y eficiencia en la administración de privilegios.

Alcance de la Revisión

El análisis desarrollado en este apartado se basa en la entrevista técnica aplicada al equipo de TI y en la revisión documental de las políticas, procedimientos y registros vinculados a la gestión de accesos en Auxadi Costa Rica. Esta combinación permite identificar el nivel de control existente sobre la asignación de privilegios a usuarios, la validación de permisos en sistemas críticos y la existencia de medidas de trazabilidad o auditoría. A partir de esta información, se establece una matriz de control de accesos y permisos como insumo clave para fortalecer la seguridad lógica, mitigar el riesgo de accesos inadecuados y cumplir con los principios definidos en la norma ISO/IEC 27001:2022.

Entrevista para Evaluación de Accesos y Privilegios de Usuarios

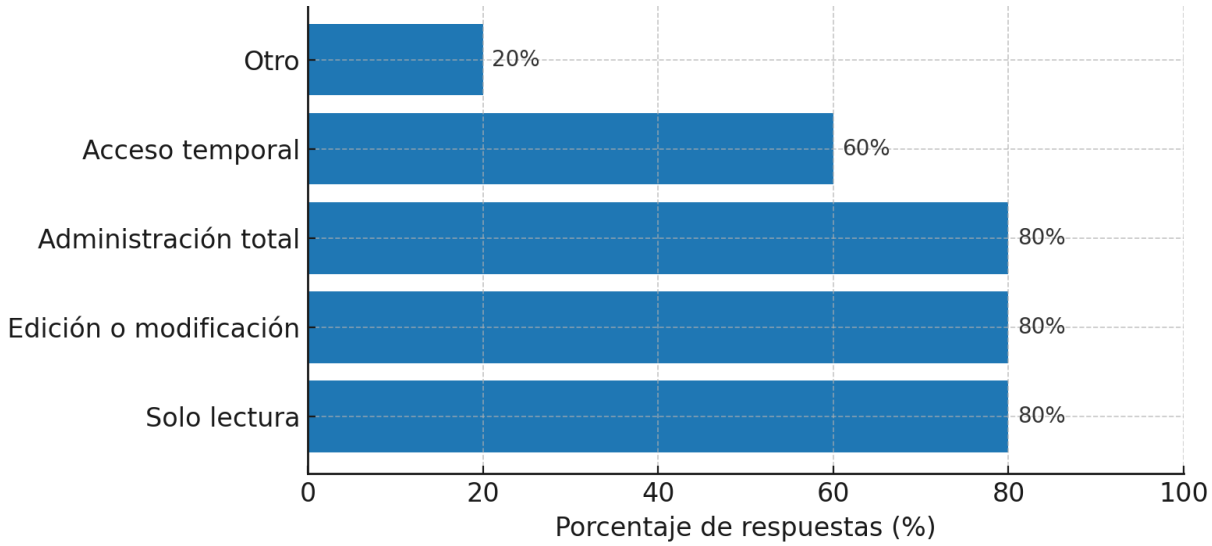
Como parte del proceso de diagnóstico para proponer políticas y procedimientos de seguridad de la información, se aplica una entrevista estructurada al personal técnico de Auxadi Costa Rica, con el fin de comprender cómo se gestionan actualmente los accesos y privilegios de usuarios en los distintos sistemas de la empresa. Esta entrevista permite recabar información sobre los niveles de acceso, criterios de asignación, control de credenciales, procedimientos de baja y auditoría de accesos. La información obtenida es clave para construir una matriz de control de accesos y permisos, la cual facilita la identificación de brechas en la administración de privilegios, y permite diseñar propuestas alineadas con la norma ISO/IEC 27001:2022, especialmente en los controles relacionados con la asignación, revisión y revocación de derechos de acceso. Se utilizó el Apéndice D. Guía de Entrevista 2.

Resultados de la entrevista.

- Pregunta 1: ¿Cuántos niveles de acceso están definidos actualmente en los sistemas?

Ilustración 21

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 1.



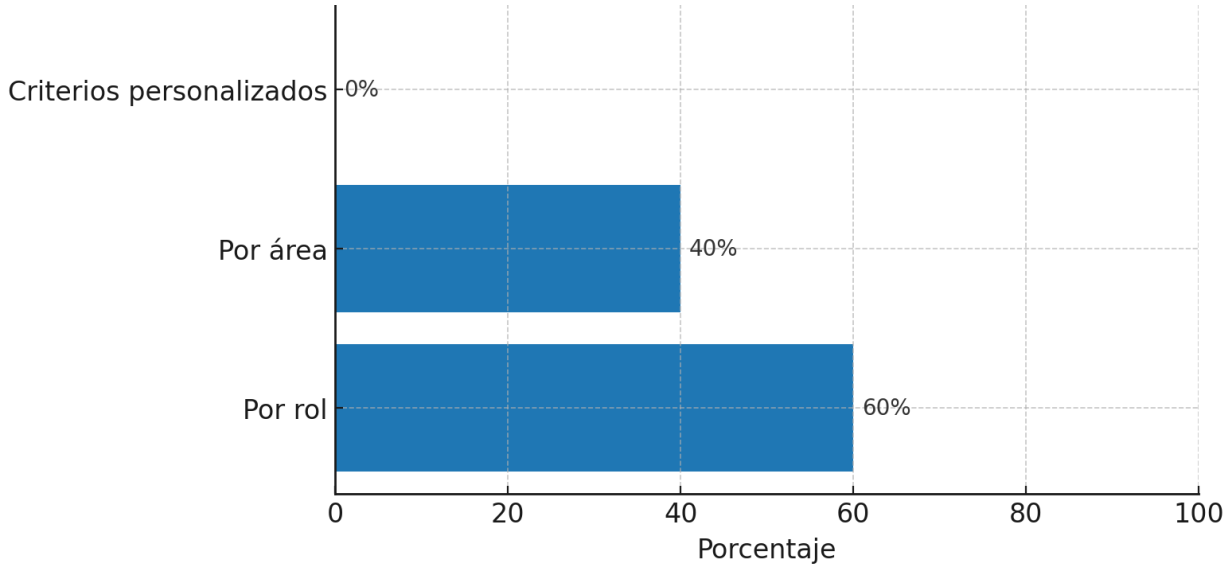
Fuente: Elaboración propia

Los resultados reflejan que la administración de accesos en los sistemas de Auxadi Costa Rica contempla distintos niveles con un enfoque jerárquico. El 100 % de los entrevistados coincidió en que existen niveles diferenciados de acceso, aunque la distribución muestra ciertas áreas de mejora. Un 80 % de los encuestados indicó que están definidos los niveles de solo lectura, edición y administración total, mientras que un 60 % señaló la existencia de accesos temporales para tareas o proyectos específicos. Además, un 20 % mencionó otro tipo de acceso particular vinculado a herramientas externas o plataformas de clientes, lo que indica que, aunque hay una estructura general, existen casos fuera del control centralizado.

- Pregunta 2: ¿Los accesos se asignan con base en el rol, el área o criterios personalizados?

Ilustración 22

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 2.



Fuente: Elaboración propia

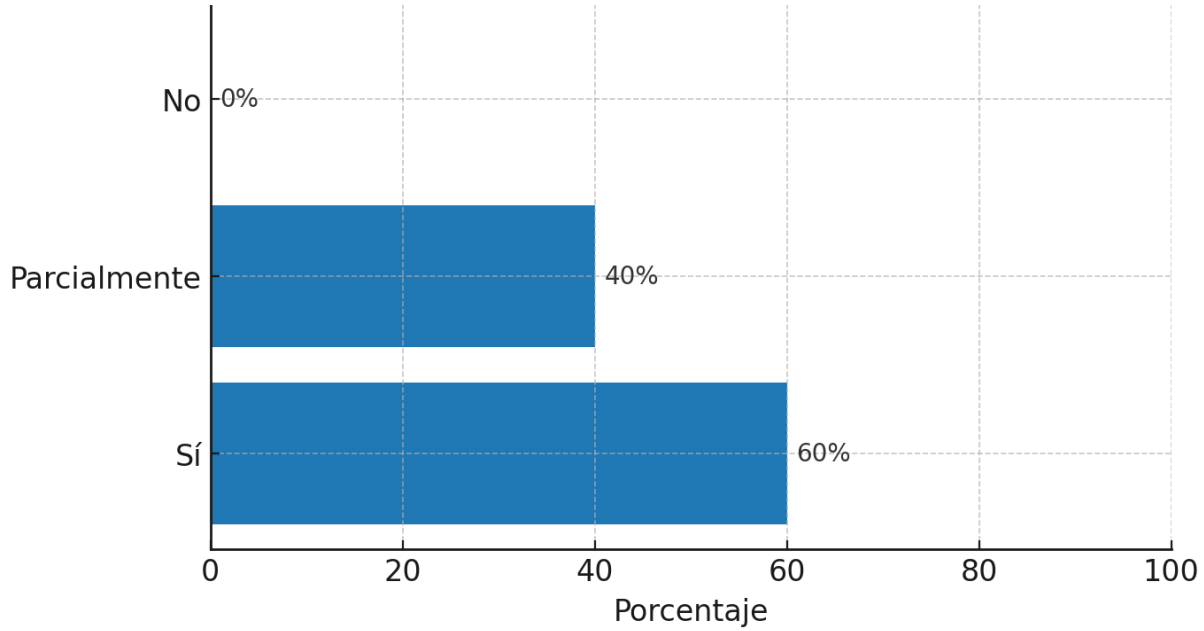
El 60 % del personal de TI entrevistado afirma que los accesos a los sistemas se asignan principalmente por rol, lo cual sugiere que existe cierta estandarización en la forma de otorgar

permisos según funciones específicas dentro de la organización. Por otro lado, un 40 % indicó que los accesos se definen según el área funcional, lo cual puede dar lugar a diferencias entre departamentos, dependiendo de cómo cada uno gestiona sus necesidades de acceso. Este resultado evidencia que, aunque se aplican criterios lógicos para otorgar permisos, todavía hay margen para fortalecer la homogeneidad y trazabilidad en la administración de privilegios.

- Pregunta 3: ¿Existe un registro formal y actualizado de los accesos por usuario?

Ilustración 23

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 3.



Fuente: Elaboración propia

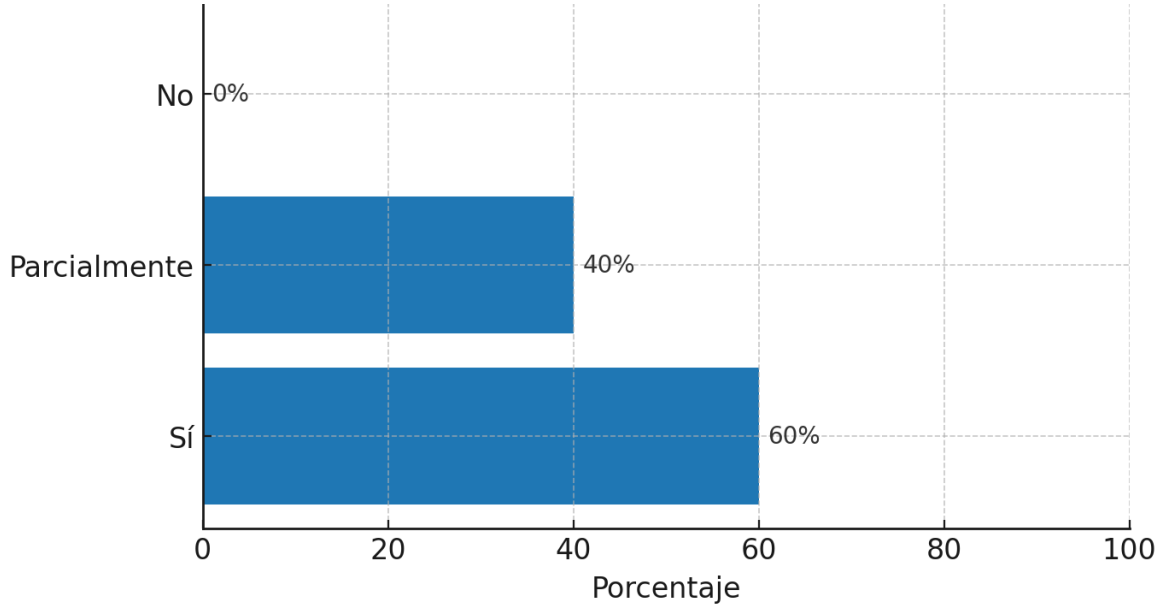
El 60 % de los entrevistados indica que sí existe un registro formal y actualizado sobre los accesos de cada usuario a los sistemas. Un 40 % adicional afirmó que este control existe solo parcialmente, lo que sugiere que, aunque se han tomado medidas en esta área, aún hay procesos que no se aplican de forma uniforme en todos los sistemas o usuarios. Este resultado refleja un esfuerzo activo por parte del equipo de TI para gestionar los accesos de manera organizada, pero

también revela áreas de mejora, especialmente en lo que respecta a la actualización constante y a la consolidación de registros en un sistema centralizado.

- Pregunta 4: ¿Todos los usuarios utilizan credenciales únicas?

Ilustración 24

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 4.



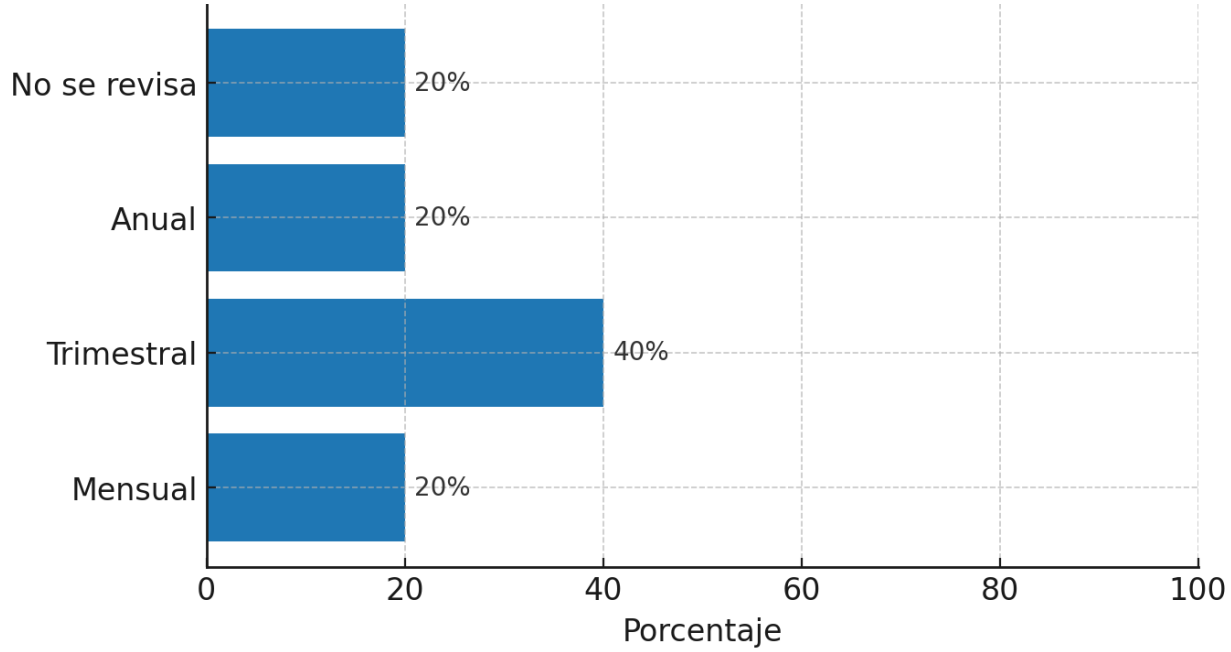
Fuente: Elaboración propia

Según la entrevista, un 60 % de los participantes indica que todos los usuarios utilizan credenciales únicas para acceder a los sistemas, lo cual es un indicador positivo en términos de control de accesos. Sin embargo, un 40 % señaló que solo algunos usuarios cuentan con credenciales personales, lo que sugiere que aún persisten prácticas como el uso compartido de cuentas en ciertos entornos o equipos específicos, todo esto revela una oportunidad importante para reforzar las medidas de autenticación individual, ya que el uso exclusivo de credenciales únicas es esencial para garantizar la trazabilidad, aplicar principios de responsabilidad individual y cumplir con los controles de seguridad.

- Pregunta 5: ¿Con qué frecuencia se revisan los permisos de acceso en los sistemas críticos?

Ilustración 25

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 5.



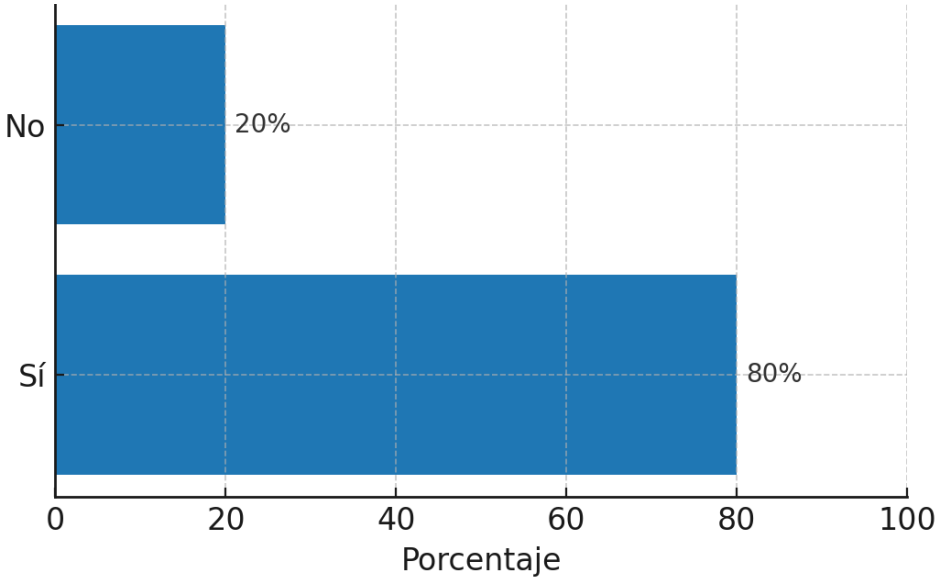
Fuente: Elaboración propia

Un 40 % de los entrevistados indica que la revisión de permisos se realiza de manera trimestral, mientras que un 20 % mencionó que este proceso se hace mensualmente. Otro 20 % señaló que la revisión es anual, y el 20 % restante afirmó que no se realiza ningún tipo de verificación periódica. Aunque se evidencian prácticas positivas en cuanto a revisiones regulares, la falta de uniformidad y la ausencia de controles en ciertos casos representan un riesgo de accesos no justificados o desactualizados, lo que resalta la necesidad de mayor consistencia en este proceso.

- Pregunta 6: ¿Existe un procedimiento documentado para dar de baja accesos cuando alguien deja la empresa?

Ilustración 26

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 6.



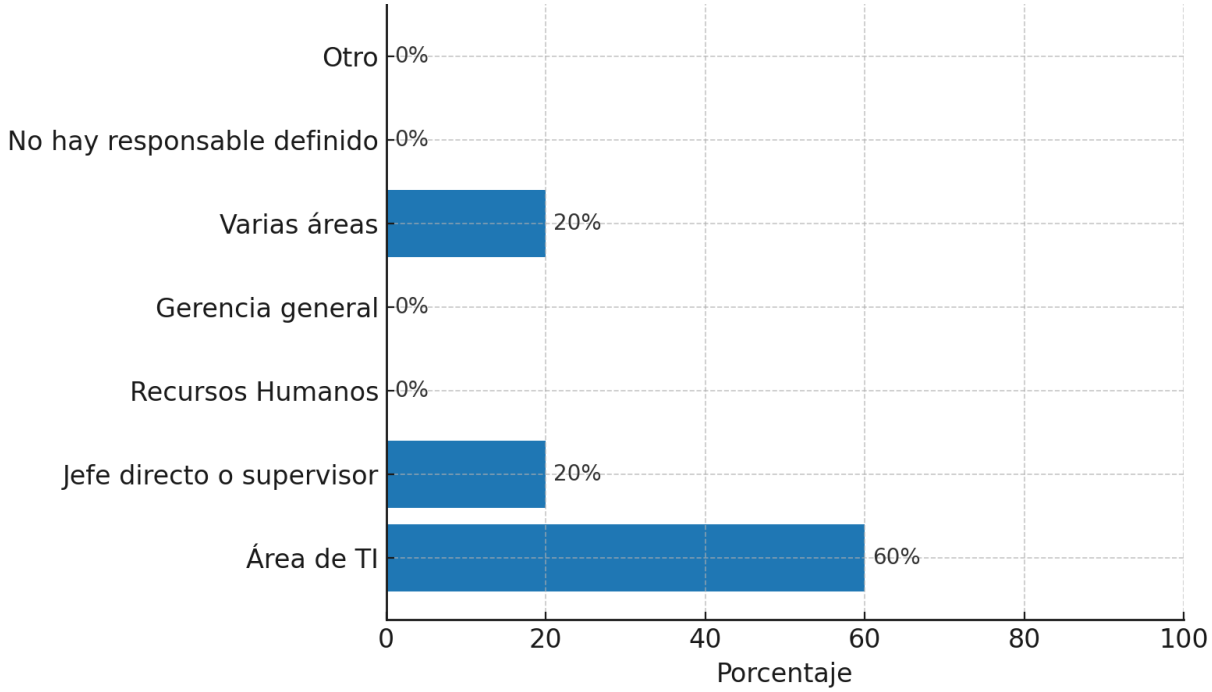
Fuente: Elaboración propia

El 80 % de los entrevistados confirma que sí existe un procedimiento formal para dar de baja los accesos de usuarios que finalizan su relación laboral con la empresa. Solo un 20 % indicó que no hay un proceso definido o este no se encuentra debidamente documentado. Este resultado refleja una buena práctica en la gestión de accesos; no obstante, la falta de formalización en ciertos casos puede generar vacíos de control y aumentar el riesgo de mantener credenciales activas sin justificación.

- Pregunta 7: ¿Quién autoriza los accesos y controla los cambios de permisos?

Ilustración 27

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 7.



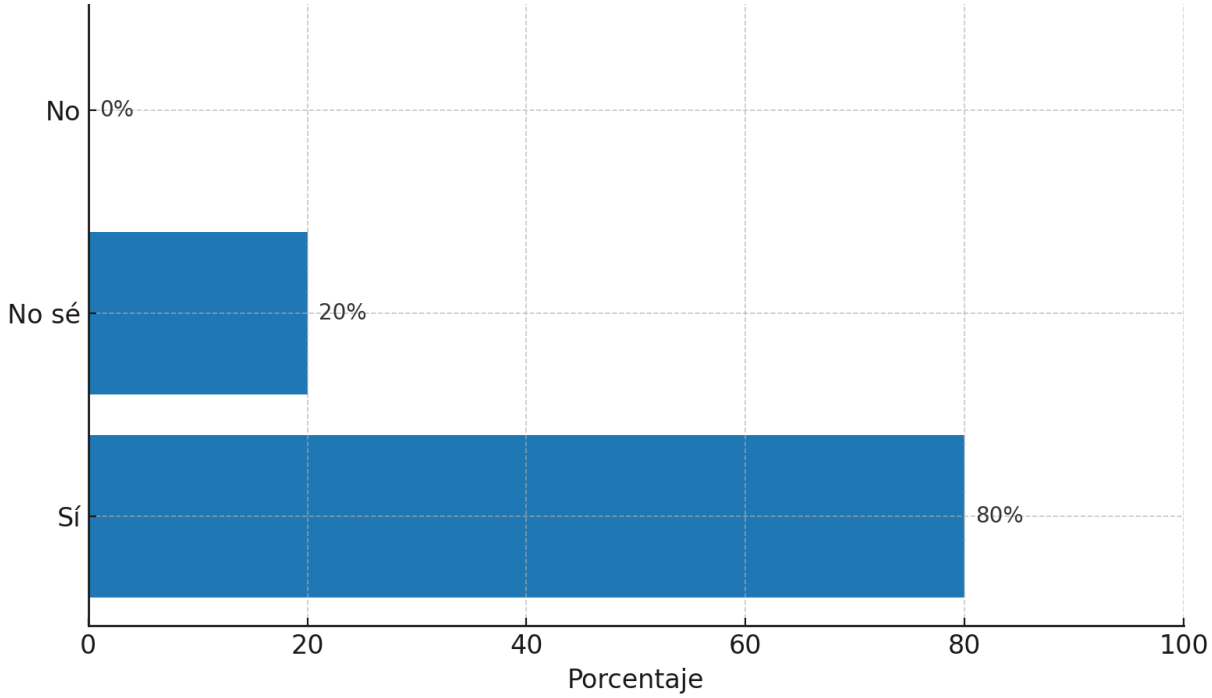
Fuente: Elaboración propia

La mayoría de los encuestados, el 60 % indica que el área de TI es la principal responsable de autorizar accesos y controlar cambios de permisos, mientras que un 20 % mencionó que este proceso es compartido entre varias áreas y otro 20 % señaló que los jefes directos también tienen participación. Esta diversidad en los criterios de autorización refleja una estructura funcional flexible, aunque también podría generar ambigüedades en la gestión de privilegios si no se cuenta con una política unificada que delimite claramente los responsables y garantice trazabilidad.

- Pregunta 8: ¿Se auditan los accesos mediante bitácoras o registros de eventos?

Ilustración 28

Resultados de entrevista para evaluación de accesos y privilegios de usuarios – pregunta 8.



Fuente: Elaboración propia

El 80 % de los participantes indica que sí se auditan los accesos mediante bitácoras o registros de eventos, mientras que un 20 % menciona no saber si este control se aplica. Este resultado refleja que, aunque existen mecanismos de monitoreo en los sistemas críticos, es necesario reforzar la comunicación y documentación del proceso para asegurar que todos los miembros del equipo de TI conozcan cómo se realiza la auditoría, aumentando la transparencia y efectividad en la detección de accesos no autorizados.

Revisión Documental de Accesos y Privilegios de Usuarios

Como parte del análisis integral de la gestión de seguridad de la información en Auxadi Costa Rica, se realizó una revisión documental específica sobre los lineamientos y registros relacionados con la asignación de accesos y privilegios a los usuarios. Esta revisión tuvo como finalidad identificar el grado de formalización, control y trazabilidad existente en los procedimientos que regulan el uso de credenciales, la segmentación de accesos y la baja o modificación de permisos en los sistemas críticos. A partir de este análisis, se busca sustentar la necesidad de establecer una matriz estructurada de control de accesos y privilegios, alineada con los principios de la norma ISO/IEC 27001:2022 y adaptada al contexto operativo de la organización.

Documentos revisados para el análisis documental:

- Política de Seguridad de la Información.docx
- Política de Protección de Datos.docx
- Código Ético y de Conducta.pdf
- Gestión de Incidentes – Incident Management V2.docx
- Política de Gestión de Contraseñas.docx
- Procedimiento de Altas, Bajas y Modificaciones de Usuarios.docx
- Plan de Recuperación ante Desastres (DRP) V08.docx
- Plan de Continuidad de Negocio (BCP) V07.docx
- Procedimiento de Respaldo y Restauración de Datos.docx

Resultados de la revisión documental.

Del análisis se identifica que, si bien la empresa ha definido lineamientos generales sobre el manejo de accesos, todavía persisten vacíos que limitan su aplicación práctica y dificultan el control efectivo sobre los privilegios asignados. Se identificó que los procedimientos actuales abarcan aspectos como la protección de credenciales, el alta y baja de usuarios y la gestión ante incidentes de acceso, pero no se cuenta con una herramienta consolidada que integre toda esta

información en un formato único, consultable y auditable. Esta carencia reduce la trazabilidad de los procesos y limita la capacidad de supervisión continua.

Uno de los hallazgos más relevantes es la ausencia de un registro centralizado que permita identificar en tiempo real qué usuarios tienen acceso a cada sistema, con qué nivel de privilegio y bajo qué criterios fueron autorizados. Si bien la documentación sugiere que estos procesos existen, se ejecutan de forma aislada por áreas funcionales o responsables técnicos, sin una coordinación uniforme ni validaciones cruzadas. Esta dispersión limita la eficiencia en la supervisión y aumenta el riesgo de mantener privilegios innecesarios, conservar accesos después de cambios de puesto o desvinculaciones, y exponer recursos críticos sin un control adecuado. La falta de un repositorio único de accesos también dificulta la preparación ante auditorías y reduce la capacidad de respuesta frente a incidentes de seguridad.

Además, se evidencia la ausencia de mecanismos definidos para la revisión periódica de accesos, lo cual limita la capacidad de la organización para detectar credenciales obsoletas, inconsistencias en los permisos o desviaciones respecto a lo aprobado inicialmente, esta situación se vuelve aún más crítica en sistemas que gestionan información contable, financiera, de clientes o respaldos de datos, donde el principio de necesidad justificada de acceso debe aplicarse con rigor. La falta de este control formal incrementa la posibilidad de accesos indebidos y reduce la trazabilidad necesaria para garantizar un cumplimiento adecuado con los estándares de seguridad.

Tampoco se establece de forma consistente un proceso de autorización formal respaldado por documentación verificable. En ciertos casos, los permisos se otorgan por solicitud directa sin contar con evidencia clara o sin la validación del área de TI, lo que reduce la trazabilidad del proceso. Esta práctica debilita los controles internos y expone a la organización a la posibilidad de accesos no alineados con las funciones asignadas, dificultando además la rendición de cuentas en caso de auditorías o incidentes.

En este contexto, resulta fundamental implementar una matriz de control de accesos y privilegios que consolide la información actualmente dispersa, estandarice los criterios de autorización, delimite claramente a los responsables y establezca frecuencias de revisión

específicas para cada sistema. Este instrumento no solo facilitaría el cumplimiento con los controles definidos en la norma ISO/IEC 27001:2022, sino que también reforzaría la capacidad de respuesta ante incidentes, adaptaciones derivadas de cambios organizacionales y requerimientos de auditorías internas o externas. De esta forma, la empresa contaría con una herramienta estructurada que fortalecería la trazabilidad y la transparencia en la gestión de accesos.

Resultados Matriz

La elaboración de la matriz de control de accesos y permisos permitió consolidar información clave sobre la manera en que Auxadi Costa Rica gestiona los privilegios asignados en sus sistemas críticos. A través de este recurso se identificaron aspectos como el tipo de acceso por rol, los medios de autenticación utilizados, la existencia o no de registros formales, los responsables de autorización y la frecuencia con que se revisan dichos accesos. Los resultados muestran que, si bien existen prácticas definidas en algunas áreas como controles en Active Directory, el ERP financiero o la VPN empresarial, también se evidencian vacíos relevantes en otros entornos como el CRM o las carpetas compartidas, donde los registros son parciales o inexistentes. Además, la aplicación de autenticación robusta como el 2FA no es uniforme, y el control sobre accesos temporales varía considerablemente según el sistema. Esta matriz permitió visualizar de forma integral el panorama actual de los privilegios otorgados y resalta la necesidad de establecer controles más estrictos, revisiones periódicas formales y validaciones cruzadas, asegurando así una gestión alineada con los principios de minimización de privilegios, trazabilidad y segregación de funciones que establece la norma ISO/IEC 27001:2022.

Tabla 4

Matriz de control de accesos y permisos.

Sistema / Recurso	Rol del Usuario	Nivel de Acceso	Medio de Autenticación	Responsable de Autorización	Revisión Periódica	Registro Formal	Accesos Temporales Permitidos	Auditoría de Accesos / Bitácoras
Active Directory	Técnico de soporte	Edición parcial	Usuario + Contraseña única	Área de TI	Trimestral	Sí	Sí (máx. 30 días)	Sí (registro de eventos)
	Administrador de TI	Control total	2FA + Credencial única	Gerencia + TI	Trimestral	Sí	No	Sí
Carpetas compartidas (LAN)	Todo el personal	Lectura / Edición por carpeta	Usuario + Contraseña	Jefatura directa	Trimestral	Parcial	Sí (proyectos específicos)	Parcial (solo cambios críticos)
Sistema de Tickets	Técnico nivel 1	Edición de casos asignados	Usuario + Contraseña	Coordinador de soporte	Trimestral	Sí	Sí (externos temporales)	Sí
	Coordinador	Administración total	2FA + Usuario único	Coordinador + TI	Trimestral	Sí	No	Sí
ERP Financiero	Analista contable	Lectura / Edición limitada	Credencial única	Jefe de Finanzas + TI	Trimestral	Parcial	No	Bitácora de cambios
	Contador / Auditor	Acceso total	2FA + Credencial única	Dirección General + TI	Trimestral	Sí	No	Sí
CRM / Herramienta de clientes	Ejecutivo comercial	Lectura	Usuario + Contraseña	Supervisor comercial	Semestral	No	Sí (validado por jefatura)	No (registro básico)
	Supervisor comercial	Edición	Usuario único	Jefatura + TI	Trimestral	Parcial	No	Parcial

Respaldo en la nube	Administrador	Control total	2FA + Credencial única	Coordinador de Infraestructura	Trimestral	Sí	No	Sí (auditoría automática)
Correo corporativo (M365)	Todo el personal	Envío / Lectura	Credencial única	RH + TI	Anual	Parcial	No	Parcial (registro central)
Red VPN empresarial	Personal autorizado	Acceso a red interna	Usuario + 2FA	Seguridad TI + RH	Trimestral	Sí	Sí (previa justificación)	Sí

Fuente: Elaboración propia

Informe de Cumplimiento Regulatorio

Objetivo del Informe

El presente informe tiene como propósito evaluar el grado de cumplimiento normativo y regulatorio de Auxadi Costa Rica en materia de seguridad de la información y protección de datos, considerando tanto la normativa nacional (Ley 8968) como los lineamientos de la norma ISO/IEC 27001:2022. Su objetivo es identificar fortalezas y brechas dentro del marco documental y procedimental de la organización, de manera que los hallazgos sirvan como base para la mejora continua, el fortalecimiento del sistema de gestión y la construcción de un entorno más seguro y confiable para el manejo de la información crítica.

Alcance de la Revisión

La revisión contempló el análisis documental de políticas, procedimientos y lineamientos internos relacionados con la seguridad de la información, la gestión de accesos, la protección de datos, la continuidad del negocio, la recuperación ante desastres y la gestión de incidentes. Este proceso se complementó con la aplicación de listas de verificación estructuradas, lo que permitió contrastar de manera más rigurosa los hallazgos frente a las exigencias legales y normativas vigentes. La utilización combinada de ambos instrumentos fortaleció la objetividad del análisis y facilitó la identificación de brechas entre lo documentado y lo implementado en la práctica. El

alcance incluyó la valoración del respaldo institucional de la alta dirección, la definición de responsabilidades, la aplicación de controles organizativos y tecnológicos, así como la efectividad de los mecanismos de seguimiento y auditoría, generando así un panorama integral y confiable sobre el nivel de cumplimiento regulatorio en Auxadi Costa Rica.

Revisión Documental de Cumplimiento Normativo y Regulatorio

Como parte del análisis de la seguridad de la información en Auxadi Costa Rica, se llevó a cabo una revisión documental enfocada en el cumplimiento normativo y regulatorio, con el fin de contrastar el marco interno de políticas y procedimientos frente a lo dispuesto en la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales y la norma ISO/IEC 27001:2022. Este proceso permitió constatar que la organización cuenta con lineamientos formales que abarcan aspectos clave como la protección de datos, la seguridad de la información, la gestión de accesos, la continuidad del negocio y la recuperación ante desastres, evidenciando el compromiso de la alta dirección al contar con políticas firmadas y respaldadas en el nivel gerencial.

Documentos revisados para el análisis documental:

- Política de Seguridad de la Información.docx
- Política de Protección de Datos.docx
- Código Ético y de Conducta.pdf
- Gestión de Incidentes – Incident Management V2.docx
- Política de Gestión de Contraseñas.docx
- Procedimiento de Altas, Bajas y Modificaciones de Usuarios.docx
- Plan de Recuperación ante Desastres (DRP) V08.docx
- Plan de Continuidad de Negocio (BCP) V07.docx
- Procedimiento de Respaldo y Restauración de Datos.docx

Resultados de la revisión documental.

En los hallazgos se identifica que la existencia de documentos oficiales brinda una base normativa sólida, al definir roles y responsabilidades para los puestos con acceso a información

crítica, así como al establecer medidas organizativas y tecnológicas que fortalecen la trazabilidad en los procesos de aprobación de accesos y en la gestión de incidentes. A su vez, se verifica que los planes de continuidad de negocio y de recuperación ante desastres se encuentran diseñados y aplicados de manera parcial, lo que refleja una intención de garantizar la resiliencia organizacional frente a eventuales contingencias. También se observa que la seguridad ha sido incluida dentro de las auditorías internas, lo cual constituye un avance en la integración de los aspectos legales y normativos dentro de los procesos de supervisión.

No obstante, se evidenciaron varias desviaciones que limitan el grado de cumplimiento esperado. Entre ellas sobresale la necesidad de actualizar de manera periódica las políticas de seguridad y de protección de datos, ya que algunas presentan rezagos frente a los cambios regulatorios y tecnológicos recientes. De igual forma, la capacitación y socialización de estas políticas con el personal no ha sido uniforme ni se encuentra debidamente documentada, lo que genera brechas en la concientización y en la aplicación práctica de los lineamientos. También se detectó una gestión documental dispersa, ya que registros de incidentes, bajas de usuarios y acciones correctivas no siempre están centralizados, lo que dificulta el control, la trazabilidad y el seguimiento oportuno. Adicionalmente, se observó que en algunos incidentes el cierre de acciones correctivas no queda registrado con el detalle requerido, lo que reduce la capacidad de aprendizaje organizacional y limita la efectividad del ciclo de mejora continua.

La revisión también mostró que las auditorías internas no abarcan en su totalidad todas las áreas críticas relacionadas con la seguridad de la información, lo que deja espacios sin evaluar en términos de cumplimiento. Otro aspecto pendiente es la formalización de mecanismos que aseguren la obtención y resguardo del consentimiento informado de los titulares de los datos personales, requisito indispensable en la aplicación de la Ley 8968. Asimismo, los planes de continuidad no han sido probados de manera integral en todas las áreas operativas, lo que reduce su efectividad real. Finalmente, se evidenció la ausencia de métricas e indicadores que permitan medir y dar seguimiento al nivel de cumplimiento normativo, además de una cobertura limitada frente a riesgos emergentes vinculados a entornos de teletrabajo, movilidad y servicios en la nube.

En resumen, la revisión documental permitió identificar fortalezas relevantes que reflejan el interés de la empresa en consolidar un marco formal de cumplimiento, al tiempo que dejó en evidencia brechas que requieren atención para lograr una plena alineación con la legislación nacional y los estándares internacionales. Estos hallazgos constituyen la base para el informe de cumplimiento regulatorio y aportan insumos claros para orientar acciones de mejora que fortalezcan la gestión de la seguridad de la información en Auxadi Costa Rica. De esta manera, se sientan las bases para avanzar hacia un sistema de gestión más maduro, confiable y alineado con las mejores prácticas internacionales.

Listas de Verificación de Cumplimiento Normativo y Regulatorio

Las listas de verificación se aplicaron en conjunto con la revisión documental y con el objetivo de valorar el nivel de cumplimiento de Auxadi Costa Rica en relación con la normativa vigente y los estándares de seguridad de la información definidos en la ISO/IEC 27001:2022. A través de este proceso se logra evidenciar el estado actual de las políticas institucionales, la formalización de los procedimientos y las brechas que requieren atención, aportando elementos claros para orientar la mejora continua y reforzar la gestión de seguridad dentro de la organización. Se utilizo el Apéndice E. Listas de Verificación 2.

Resultados de las listas de verificación.

Ilustración 29

Resultados de cumplimiento normativo y regulatorio – lista de verificación 1.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
1.1	¿Existe una política formal de seguridad de la información firmada por la alta dirección?	✓		La política está firmada por la gerencia, aunque requiere una actualización en algunos apartados técnicos
1.2	¿Está vigente y actualizada la política de protección de datos personales?		✗	El documento existe, pero no se ha actualizado en los últimos dos años; necesita alineación con cambios regulatorios recientes
1.3	¿Se definen claramente los roles y responsabilidades en el tratamiento de datos sensibles?	✓		Se encuentran definidos en las políticas, aunque algunos puestos requieren mayor especificación
1.4	¿Se han socializado estas políticas entre los empleados con acceso a datos críticos?		✗	No todos los colaboradores han recibido capacitaciones formales; se han hecho comunicaciones por correo, pero sin evidencia documental suficiente

Fuente: Elaboración propia

Se evidencia que Auxadi Costa Rica dispone de políticas y lineamientos básicos en seguridad de la información, incluyendo la aprobación por parte de la gerencia y la existencia de procedimientos formales. No obstante, también se identifican debilidades relevantes que requieren atención, como la falta de actualización de la política de protección de datos, la ausencia de

procesos de capacitación formal para socializar estas políticas y la documentación incompleta de incidentes y acciones correctivas. Estos aspectos generan vacíos que podrían comprometer la trazabilidad y el cumplimiento normativo en el mediano plazo. Atender estas áreas de mejora permitirá consolidar un sistema de gestión más robusto, garantizando tanto la alineación con la Ley 8968 como con la norma ISO/IEC 27001:2022.

Ilustración 30

Resultados de cumplimiento normativo y regulatorio – lista de verificación 2.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
2.1	¿Se cumple con los principios de la Ley 8968 sobre protección de datos personales?	✓		La organización cuenta con prácticas alineadas, aunque falta reforzar el proceso de consentimiento informado
2.2	¿Se han implementado controles alineados con los dominios de la ISO/IEC 27001:2022?	✓		Los principales controles tecnológicos y organizativos están aplicados, aunque no todos se encuentran formalizados en matrices de control
2.3	¿Existen registros que evidencien acciones correctivas ante desviaciones legales o normativas?		✗	La gestión de incidentes sí se realiza, pero no siempre se documenta con detalle el cierre de las acciones correctivas
2.4	¿Se incluye el cumplimiento normativo dentro de los procesos de auditoría interna?	✓		El área de auditoría revisa aspectos legales, aunque de forma parcial; se recomienda ampliar el alcance hacia seguridad de la información

Fuente: Elaboración propia

Se observa que la organización cumple en gran medida con los requerimientos normativos y regulatorios, mostrando un nivel adecuado de alineación tanto con la Ley 8968 como con los dominios de la ISO/IEC 27001:2022. Sin embargo, aún se presentan áreas de mejora importantes, como la necesidad de fortalecer el proceso de consentimiento informado y la falta de registros detallados sobre el cierre de acciones correctivas ante desviaciones legales o normativas. Estas debilidades reducen la capacidad de demostrar cumplimiento pleno en auditorías o revisiones externas, lo cual podría derivar en riesgos de carácter legal o reputacional. Corregir dichas brechas permitirá a la organización no solo cumplir con la normativa vigente, sino también asegurar un marco de gestión más transparente y confiable.

Ilustración 31

Resultados de cumplimiento normativo y regulatorio – lista de verificación 3.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
3.1	¿Se cuenta con procedimientos documentados de alta, baja y modificación de usuarios?	✓		Existe un procedimiento formal aprobado, aunque algunos registros de bajas no se encuentran digitalizados
3.2	¿Existe trazabilidad de la aprobación de accesos por parte de responsables autorizados?	✓		La aprobación se encuentra documentada en correos y formularios, aunque no siempre centralizada en un repositorio único
3.3	¿Están documentados y vigentes los planes de continuidad y recuperación ante desastres?	✓		Los planes están vigentes, revisados en 2022, con pruebas realizadas parcialmente en áreas críticas
3.4	¿Los incidentes de seguridad se registran y gestionan conforme al procedimiento formal?		✗	Si bien existe registro, no siempre se hace seguimiento completo a la resolución final de cada incidente

Fuente: Elaboración propia

Se evidencia que la organización cuenta con procedimientos documentados y vigentes en aspectos clave como la gestión de usuarios, trazabilidad de accesos y planes de continuidad, lo que refleja un nivel de madurez adecuado en la gestión de seguridad de la información. No obstante, se identifican limitaciones en el seguimiento de incidentes de seguridad y en la digitalización

completa de ciertos registros, lo que genera riesgos de pérdida de información o falta de trazabilidad en auditorías. Aunque las bases del control interno son sólidas, se requiere fortalecer la sistematización y la disciplina en la gestión de evidencias, asegurando que cada incidente tenga un ciclo de vida documentado y que todos los registros se centralicen en un repositorio único. Estas acciones permitirán aumentar la efectividad de la respuesta a incidentes y mejorar la capacidad de recuperación ante eventualidades críticas.

Resultados Informe

El informe de cumplimiento regulatorio muestra que Auxadi Costa Rica cuenta con una base normativa y procedimental sólida, respaldada por la alta dirección y reflejada en políticas formales de seguridad y protección de datos, definición de roles, controles tecnológicos, gestión de incidentes y auditorías internas. Estos elementos evidencian un compromiso con la gobernanza y la mejora continua en la protección de la información. No obstante, se identifican brechas como la falta de actualización de políticas, capacitación insuficiente, gestión documental dispersa, trazabilidad limitada en acciones correctivas, auditorías con cobertura parcial y debilidades en el consentimiento informado. También se observa la ausencia de métricas de cumplimiento y de lineamientos frente a riesgos emergentes en teletrabajo y nube, así como pruebas limitadas de continuidad, lo que representa una oportunidad de mejora para robustecer la alineación con la normativa vigente y la norma ISO/IEC 27001:2022.

Fortalezas detectadas.

- Respaldo de la alta dirección: La política de seguridad de la información cuenta con la firma de la gerencia, lo que refleja un compromiso formal con la gobernanza, la supervisión estratégica y el cumplimiento normativo, asegurando que las directrices de seguridad cuenten con respaldo institucional al más alto nivel.
- Políticas vigentes de seguridad y protección de datos: Aunque algunas requieren actualización, la organización dispone de documentos oficiales que establecen lineamientos claros para la protección de información sensible y la gestión adecuada

de datos personales, sirviendo como marco de referencia en auditorías y procesos de control.

- Definición de roles y responsabilidades: Los puestos con acceso a datos críticos cuentan con responsabilidades formalmente definidas, lo que brinda una base sólida para la rendición de cuentas y garantiza una adecuada segregación de funciones entre colaboradores.
- Cumplimiento parcial con la Ley 8968: La organización aplica prácticas alineadas con los principios de protección de datos, incluyendo procesos de confidencialidad y resguardo de información personal, lo que evidencia avances en la adaptación al marco legal nacional.
- Controles tecnológicos y organizativos aplicados: Se han implementado medidas de seguridad como la trazabilidad en la aprobación de accesos, los procedimientos de altas y bajas de usuarios, y planes de continuidad con pruebas parciales que fortalecen la resiliencia y la respuesta ante eventualidades.
- Inclusión de seguridad en auditorías internas: El área de auditoría revisa aspectos legales y normativos, lo cual refleja un esfuerzo por integrar la seguridad en los procesos de supervisión, aunque aún de forma parcial.
- Gestión activa de incidentes: Existen registros de incidentes de seguridad y acciones de mitigación documentadas, lo que evidencia un enfoque de mejora continua en la gestión de riesgos y en la capacidad de respuesta de la organización.

Desviaciones y oportunidades de mejora.

- Políticas desactualizadas: La política de protección de datos personales no se ha actualizado en los últimos dos años, lo que limita su alineación con cambios regulatorios recientes y nuevas amenazas tecnológicas.
- Capacitación insuficiente: La socialización de políticas no ha sido formal ni documentada en toda la organización, generando brechas en la concientización del personal y debilitando la adopción uniforme de las medidas de seguridad.

- Gestión documental dispersa: Registros de bajas de usuarios, incidentes y acciones correctivas no siempre están centralizados, lo que dificulta la trazabilidad, limita el control efectivo y retrasa la capacidad de respuesta.
- Documentación incompleta en acciones correctivas: Aunque los incidentes son gestionados, no siempre se documenta con el detalle necesario el cierre de las acciones, lo que reduce la trazabilidad y limita el aprendizaje institucional.
- Cobertura parcial de auditorías internas: La verificación de cumplimiento normativo en auditorías no es integral, dejando fuera áreas críticas relacionadas con la seguridad de la información y debilitando la visión completa del sistema de gestión.
- Consentimiento informado débil: No se evidencia un mecanismo estandarizado que asegure la recolección y resguardo del consentimiento de los titulares de datos personales, lo que representa una brecha frente a la Ley 8968 y podría derivar en riesgos legales.
- Pruebas limitadas de continuidad: Los planes de recuperación ante desastres no han sido probados en todas las áreas críticas, reduciendo su efectividad real en un escenario de contingencia que afecte la operación.
- Ausencia de métricas e indicadores: No se han definido indicadores para medir el nivel de cumplimiento normativo y de seguridad, lo que impide dar un seguimiento cuantitativo y continuo al progreso de la organización.
- Cobertura tecnológica limitada: Los lineamientos técnicos no contemplan de manera suficiente los riesgos emergentes asociados a entornos de teletrabajo, movilidad y servicios en la nube, lo que deja un espacio de exposición que requiere atención prioritaria.

Informe de Patrones de Amenazas y Vulnerabilidades

Objetivo del Informe

El presente informe tiene como propósito analizar los registros históricos de incidentes de seguridad en Auxadi Costa Rica con el fin de identificar patrones de amenazas recurrentes, evaluar el impacto de los eventos en la confidencialidad, integridad y disponibilidad de la información, y

reconocer áreas críticas que requieren fortalecimiento. El objetivo central es generar insumos prácticos para la mejora continua del sistema de gestión de seguridad de la información, aportando recomendaciones que permitan reducir la recurrencia de incidentes y anticiparse a nuevos riesgos, en concordancia con los lineamientos de la norma ISO/IEC 27001:2022.

Alcance de la Revisión

La revisión incluye el análisis documental de los registros almacenados en el sistema de tickets corporativo, abarcando incidentes reportados en un periodo histórico de dos años, el cual se seleccionó por ser el máximo permitido por la propia plataforma como filtro de consulta. Cabe señalar que dicho sistema fue desarrollado internamente, lo que permite acceder a la información de manera estructurada y alineada a las necesidades operativas de la organización. El análisis contempla incidentes relacionados con accesos indebidos, errores humanos, fallos de disponibilidad, intentos de phishing, gestión documental incompleta y riesgos asociados al teletrabajo, la movilidad y los servicios en la nube. El alcance considera tanto la clasificación y trazabilidad de los incidentes como la efectividad de las medidas de contención y corrección aplicadas. Asimismo, se valora el nivel de documentación, la identificación de causas raíz y la incorporación de lecciones aprendidas como parte de la respuesta organizacional. Con este enfoque se busca ofrecer una visión integral sobre los patrones de amenazas y vulnerabilidades presentes en Auxadi Costa Rica, estableciendo una base sólida para la definición de estrategias de mejora.

Revisión Documental de Patrones de Amenazas y Vulnerabilidades

Resultados de la revisión documental.

Dentro del análisis integral de la gestión de la seguridad de la información en Auxadi Costa Rica, se llevó a cabo una revisión documental centrada en los registros históricos de incidentes de seguridad almacenados en el sistema de tickets corporativo. Este proceso se desarrolla con el propósito de identificar los patrones de amenazas más frecuentes, evaluar la efectividad de las acciones de respuesta aplicadas y reconocer las áreas críticas que requieren un fortalecimiento inmediato. La revisión se enfocó en reportes de los últimos dos años, lo que permitió obtener una

visión representativa de la situación actual y de la evolución en el manejo de incidentes por parte de la organización.

Los resultados evidenciaron que los incidentes registrados pueden agruparse en categorías específicas que reflejan las principales debilidades de la infraestructura de seguridad: accesos indebidos o intentos de acceso no autorizado, errores humanos en el manejo de información sensible, fallos de disponibilidad en servicios críticos, y vulnerabilidades explotadas en entornos de teletrabajo y movilidad. Esta clasificación evidencia que la organización enfrenta riesgos tanto de origen interno como externo, siendo los accesos no autorizados y las brechas por descuido humano los más recurrentes. La existencia de un sistema formal de tickets constituye una fortaleza, ya que permite conservar evidencia documental de los eventos, registrar acciones de mitigación y contar con trazabilidad en la atención. Sin embargo, también se detecta que los registros no siempre siguen una clasificación estandarizada y en algunos casos no incluyen un cierre formal de las acciones correctivas, lo que afecta la posibilidad de generar estadísticas confiables para medir tendencias y recurrencias.

En cuanto a la respuesta ante incidentes, se observa que los casos de mayor impacto fueron atendidos dentro de plazos razonables, con medidas de contención aplicadas de forma oportuna. Aun así, en múltiples registros no se documenta con detalle el análisis del impacto ni se incluyen las lecciones aprendidas, lo que limita la capacidad de prevención futura. Esta carencia de retroalimentación organizada se traduce en una pérdida de oportunidades para generar conocimiento interno y fortalecer la resiliencia organizacional. Asimismo, se evidenció que los incidentes relacionados con entornos de teletrabajo, movilidad y uso de servicios en la nube no se encuentran claramente diferenciados en los registros, lo que invisibiliza riesgos emergentes que hoy tienen un peso significativo en el ecosistema digital de la empresa.

Por otro lado, se identificaron prácticas positivas que refuerzan la cultura de seguridad en la organización. Entre ellas destacan los registros asociados a intentos de phishing y ataques de ingeniería social, donde se documentaron no solo las acciones de mitigación inmediatas, sino también campañas de concientización dirigidas al personal. Estas iniciativas reflejan un enfoque de mejora continua y evidencian la importancia que se le da a la sensibilización de los

colaboradores frente a riesgos recurrentes. No obstante, estas prácticas aún no están consolidadas en un esquema formal de métricas o indicadores que permitan medir de forma cuantitativa la reducción del riesgo posterior a la implementación de controles.

Un aspecto crítico identificado en la revisión es la dispersión de los registros asociados a bajas de usuarios, controles de acceso y acciones correctivas derivadas de incidentes. En varios casos, los reportes se encuentran fragmentados en diferentes repositorios, lo que dificulta su trazabilidad y la construcción de una visión integral de los eventos. Esta situación resalta la necesidad de centralizar la gestión documental y aplicar un modelo estandarizado de reporte que facilite tanto la clasificación como la evaluación de los incidentes.

La revisión documental de registros de incidentes demuestra que, aunque Auxadi Costa Rica cuenta con un sistema formal que permite dar seguimiento a los eventos de seguridad, persisten áreas críticas que deben ser atendidas para robustecer el sistema de gestión. La falta de estandarización en la clasificación de incidentes, la ausencia de métricas claras, la dispersión documental y la escasa documentación de lecciones aprendidas representan desviaciones que, de ser corregidas, fortalecerían la capacidad de prevención y respuesta de la organización. Estos hallazgos servirán como insumo clave para la elaboración del resumen de patrones de amenazas y riesgos, así como para la definición de recomendaciones específicas que permitan consolidar la seguridad de la información en un marco alineado a la norma ISO/IEC 27001:2022.

Resultados Informe

La revisión documental de los registros de incidentes de seguridad almacenados en el sistema de tickets de Auxadi Costa Rica permitió identificar patrones recurrentes que reflejan tanto la madurez alcanzada en la gestión de riesgos como las brechas existentes en la protección de activos críticos. El análisis de estos registros evidenció incidentes que impactan de forma directa la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones. Estos hallazgos resultan valiosos porque no solo revelan vulnerabilidades técnicas y organizativas, sino también aspectos relacionados con la cultura de seguridad y la gobernanza corporativa.

El análisis de los registros de incidentes permitió reconocer que Auxadi Costa Rica ha establecido una base sólida en la gestión de riesgos, pero aún enfrenta desafíos significativos relacionados con la estandarización de procesos, la capacitación del personal y la cobertura de nuevos escenarios tecnológicos. La adopción de las recomendaciones planteadas contribuirá no solo a disminuir la recurrencia de incidentes, sino también a consolidar una cultura de seguridad más madura y proactiva, capaz de anticipar y responder a las amenazas emergentes.

Patrones detectados.

- Accesos indebidos e intentos de intrusión: Los registros evidencian incidentes vinculados a intentos de acceso no autorizado a sistemas críticos, principalmente originados en accesos remotos fuera de la red corporativa. Aunque los controles de autenticación han mitigado parte de estos eventos, se observan casos recurrentes en usuarios con privilegios elevados, lo que sugiere la necesidad de un mayor control en la asignación y revisión de permisos.
- Errores humanos en el manejo de información sensible: Los incidentes más frecuentes en este ámbito se relacionan con el envío de información confidencial a destinatarios equivocados, uso de correos personales para transferir archivos internos y empleo de credenciales compartidas en determinados procesos. Estos errores, más allá de ser puntuales, reflejan debilidades en la concientización del personal y la ausencia de un proceso formal de capacitación en seguridad de la información.
- Fallos de disponibilidad en servicios críticos: Los tickets muestran interrupciones en servicios esenciales como el correo corporativo, aplicaciones internas y accesos a bases de datos. En algunos casos, la recuperación se ejecutó sin documentación completa, dificultando la identificación de la causa raíz y reduciendo la efectividad del plan de continuidad. Estos fallos demuestran la necesidad de fortalecer tanto las pruebas de contingencia como la documentación posterior al restablecimiento.
- Phishing e ingeniería social: El análisis refleja múltiples intentos de phishing dirigidos a colaboradores de distintas áreas. Aunque la mayoría fueron contenidos, se reportaron incidentes que derivaron en bloqueos de cuentas y retrasos operativos. Esto pone en

evidencia que, a pesar de contar con filtros técnicos, la ingeniería social sigue siendo un riesgo activo y depende en gran medida de la preparación de los usuarios.

- Gestión documental dispersa y acciones incompletas: Varios tickets carecen de información suficiente sobre las acciones correctivas aplicadas o el estado de cierre del incidente. Esta falta de estandarización en los registros limita la trazabilidad, impide identificar tendencias con precisión y afecta la capacidad de aprendizaje organizacional frente a los incidentes.
- Cobertura insuficiente en entornos emergentes: No se encontró un registro diferenciado para incidentes relacionados con entornos de teletrabajo, movilidad y servicios en la nube, lo que sugiere que estas modalidades no han sido integradas de manera formal al marco de gestión de incidentes. Este vacío limita la capacidad de la organización para responder a riesgos asociados a nuevas formas de trabajo y plataformas tecnológicas en expansión.

Elementos de mejora.

- Estandarizar la gestión de incidentes: Se recomienda establecer un procedimiento único y estandarizado para la gestión de incidentes de seguridad, que abarque desde el registro inicial hasta el cierre final. Este documento debe definir responsables, tiempos de respuesta según la criticidad y la obligatoriedad de documentar las acciones correctivas. Con ello se logrará una mayor trazabilidad y un control más eficiente en el ciclo de vida de cada incidente.
- Reforzar la seguridad en accesos remotos y teletrabajo: Es necesario reforzar la seguridad en los accesos remotos mediante la aplicación obligatoria de autenticación multifactor, la revisión periódica de privilegios y el principio de mínimo acceso. Estas medidas permitirán reducir la exposición frente a intentos de intrusión, en especial en escenarios de teletrabajo o movilidad, donde los riesgos tienden a incrementarse.
- Fortalecer la capacitación y concientización del personal: Dado que los errores humanos continúan siendo una causa frecuente de incidentes, se recomienda implementar un programa anual de formación en seguridad de la información. Este debe contemplar módulos prácticos sobre el manejo responsable de datos, la

identificación de amenazas y la prevención frente a ataques de ingeniería social, con el fin de elevar el nivel de madurez en el personal.

- Mejorar la documentación y trazabilidad de los incidentes: Se sugiere que cada incidente registrado incluya un análisis de causa raíz, las acciones correctivas aplicadas y las lecciones aprendidas. Además, deben definirse indicadores cuantitativos como tiempos de resolución, reincidencias y frecuencia por categoría, de manera que la organización pueda medir de forma objetiva la efectividad de sus controles.
- Ampliar el alcance de los planes de continuidad y recuperación: Los planes de continuidad del negocio y recuperación ante desastres deben ampliarse para incluir escenarios relacionados con servicios en la nube, entornos de teletrabajo y aplicaciones móviles. A su vez, se recomienda realizar pruebas periódicas en todas las áreas críticas, documentando resultados y aplicando mejoras que refuercen la resiliencia de la organización.
- Monitoreo proactivo de amenazas emergentes: La organización debe adoptar un esquema de monitoreo que contemple riesgos propios de la movilidad, el teletrabajo y el uso de servicios en la nube. Integrar estas verificaciones dentro de las auditorías internas permitirá anticiparse a nuevas amenazas y mantener actualizado el sistema de seguridad frente a un entorno tecnológico en constante evolución.

CAPÍTULO V: PROPUESTA

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

PROPUESTA DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE DISPOSITIVOS, COMUNICACIÓN Y PROTECCIÓN DE DATOS BASADA EN LA NORMA ISO/IEC 27001:2022 PARA AUXADI COSTA RICA, UBICADA EN SAN JOSÉ

MODALIDAD PROYECTO PARA OPTAR POR EL GRADO DE LICENCIATURA EN INGENIERÍA EN INFORMÁTICA CON ÉNFASIS EN GERENCIA

Allan Enrique Barquero Gómez

Noviembre, 2025

CONTENIDO DE LA PROPUESTA

Introducción

La propuesta de políticas y procedimientos para Auxadi Costa Rica se formula como resultado directo del proceso de análisis, diagnóstico y validación de riesgos desarrollado en etapas previas. Este trabajo no surge de manera aislada, sino que responde a una secuencia metodológica que inició con la identificación y clasificación de los activos de información más críticos, continuó con la evaluación de políticas y controles existentes, la aplicación de encuestas estructuradas y entrevistas a personal clave, la revisión de accesos y autorizaciones, así como el análisis de cumplimiento normativo y de incidentes de seguridad históricos. Todo este recorrido permitió obtener una visión integral y realista del estado actual de la organización en cuanto a la gestión de dispositivos, la seguridad en la comunicación y la protección de datos.

A partir de este diagnóstico, los riesgos identificados fueron clasificados mediante la matriz de impacto y probabilidad, lo cual posibilitó su priorización y el diseño de estrategias enfocadas en mitigar aquellos de mayor criticidad. Seguidamente, se llevó a cabo un ejercicio de correlación entre vulnerabilidades y controles establecidos en la norma ISO/IEC 27001:2022, cuyo resultado fue validado con el personal de TI y Cumplimiento. Este proceso permitió ajustar y contextualizar las recomendaciones, garantizando que las medidas propuestas no permanecieran en un plano teórico, sino que respondieran a las condiciones tecnológicas, operativas y normativas específicas de la empresa.

En este sentido, la propuesta que aquí se presenta busca consolidar un marco documental integral que convierta la gestión de la seguridad de la información en un proceso preventivo, estandarizado y medible. Con ello se asegura la trazabilidad de las acciones, se fortalece la resiliencia de la organización frente a amenazas tecnológicas y se garantiza el cumplimiento de disposiciones legales como la Ley N.° 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales. A su vez, se promueve una cultura organizacional orientada hacia la responsabilidad, la mejora continua y la sostenibilidad en la protección de la información, lo cual constituye un valor estratégico para el desarrollo de Auxadi Costa Rica.

Objetivos

Objetivo general

Desarrollar una propuesta integral de políticas y procedimientos de seguridad de la información para la gestión de dispositivos, comunicación y protección de datos para Auxadi Costa Rica, basada en la norma ISO/IEC 27001:2022.

Objetivos específicos

Analizar el estado de seguridad de la información en la gestión de dispositivos, seguridad en la comunicación y protección de datos, identificando vulnerabilidades y riesgos en la empresa según la norma ISO/IEC 27001:2022.

Seleccionar los controles de seguridad aplicables a la gestión de dispositivos, seguridad en la comunicación y protección de datos, de forma que se asegure su alineación con la norma ISO/IEC 27001:2022, el análisis de riesgos realizado y las necesidades específicas de la organización.

Diseñar una propuesta estructurada de políticas y procedimientos de seguridad según el análisis y selección previos, garantizando medidas efectivas para la gestión de dispositivos, la seguridad en la comunicación y la protección de datos según la norma ISO/IEC 27001:2022.

Evaluar la viabilidad económica y operativa de la propuesta basada en las buenas prácticas establecidas en la norma ISO/IEC 27001:2022, garantizando que su aplicabilidad y sostenibilidad se ajusten al contexto de la empresa.

Alcance

El alcance de la presente propuesta comprende el diseño de políticas y procedimientos orientados a tres áreas prioritarias dentro de Auxadi Costa Rica: la gestión de dispositivos, la

seguridad en la comunicación y la protección de datos sensibles. Estas políticas no se conciben de manera independiente, sino como una extensión y complemento de los lineamientos ya existentes en la organización. En ningún caso sustituyen o contradicen las políticas vigentes, sino que las fortalecen mediante un marco más estructurado, actualizado y alineado con los riesgos identificados y con los controles establecidos en la norma ISO/IEC 27001:2022.

La propuesta se fundamenta en un proceso metodológico riguroso que incluyó la identificación y clasificación de activos críticos, la evaluación de políticas y controles actuales, la aplicación de encuestas y entrevistas al personal responsable, así como la correlación de vulnerabilidades con controles específicos de la norma. De esta manera, el alcance responde a hallazgos reales obtenidos en el diagnóstico, asegurando que cada medida planteada tenga un sustento práctico, verificable y coherente con la realidad tecnológica y organizativa de la empresa.

En cuanto a su aplicación, este alcance abarca a todos los colaboradores, contratistas y terceros autorizados que gestionen o accedan a la información corporativa de Auxadi Costa Rica, sin importar si lo hacen desde ambientes locales, remotos o a través de plataformas en la nube. Se contemplan aspectos relacionados con el uso de dispositivos, la transmisión segura de datos mediante herramientas colaborativas como Microsoft 365, la administración de credenciales y accesos, y la protección de datos personales y sensibles que forman parte de la operación diaria.

El alcance de la propuesta comprende la estandarización de los procesos vinculados con la administración de accesos y credenciales, asegurando que existan reglas claras y consistentes para su gestión. También incorpora la implementación de procedimientos definidos para la clasificación, resguardo y control del ciclo de vida de la información, con el fin de garantizar que cada documento o dato sea protegido de acuerdo con su nivel de sensibilidad. Asimismo, se establecen lineamientos para promover el uso responsable tanto de los dispositivos corporativos como de aquellos personales previamente autorizados, reforzando la seguridad en su manejo. Del mismo modo, se incluyen medidas concretas para proteger la comunicación y el intercambio de información sensible, minimizando riesgos de fuga o manipulación indebida. Finalmente, se integra un marco que abarca los procesos de respaldo, la continuidad del negocio y la gestión

formal de incidentes, asegurando la resiliencia operativa de la organización ante posibles contingencias.

Además, este alcance incorpora el análisis detallado de costos y recursos, junto con la evaluación de impacto y beneficios esperados derivados de la implementación de las políticas propuestas. Dicho análisis permitió determinar la viabilidad técnica, operativa y financiera del proyecto, identificando oportunidades de optimización mediante el aprovechamiento de licencias ya disponibles, la capacitación interna del personal y la reducción de dependencias externas. De igual forma, se estimaron los beneficios esperados en términos de eficiencia, reducción de incidentes, cumplimiento normativo y sostenibilidad del sistema de gestión, lo que asegura una visión integral de la propuesta tanto desde la perspectiva económica como estratégica.

En resumen, este alcance no solo delimita el campo de acción de la propuesta, sino que asegura que las políticas y procedimientos recomendados respondan directamente a los riesgos diagnosticados, refuercen las políticas ya vigentes y generen un marco integral de gestión alineado con las mejores prácticas internacionales. Con ello, Auxadi Costa Rica contará con un esquema sólido, verificable y adaptable a sus necesidades actuales y futuras, consolidando una postura de seguridad más preventiva, resiliente y sostenible.

Matriz de Riesgos

Objetivo de la Matriz

El objetivo de la matriz de riesgos es identificar, clasificar y priorizar los principales escenarios que pueden afectar la seguridad de la información en Auxadi Costa Rica, considerando los aspectos de gestión de dispositivos, seguridad en la comunicación y protección de datos. A través de este instrumento se busca disponer de una visión clara y estructurada de los riesgos que enfrentan los activos críticos de la organización, con el fin de facilitar la toma de decisiones estratégicas y orientar la selección de controles de acuerdo con los lineamientos de la norma ISO/IEC 27001:2022.

Alcance de la Matriz

El alcance de la matriz comprende el análisis integral de los riesgos detectados durante la fase de diagnóstico, los cuales fueron valorados según su probabilidad de ocurrencia y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información. La matriz considera tanto factores tecnológicos como organizativos y humanos, abarcando desde vulnerabilidades en la gestión de accesos y contraseñas hasta deficiencias en la capacitación, monitoreo y documentación. Con ello se establece un marco de referencia que permite evaluar los riesgos en una escala uniforme y definir prioridades de mitigación que fortalezcan el sistema de gestión de seguridad de la información de Auxadi Costa Rica.

Resultados Matriz

La matriz de riesgos constituye un instrumento esencial dentro de la fase de análisis, al permitir representar de manera estructurada las amenazas detectadas y relacionarlas con su nivel de probabilidad e impacto sobre la confidencialidad, integridad y disponibilidad de la información. Su construcción posibilita identificar con mayor claridad los escenarios que requieren atención prioritaria y establecer un orden lógico de tratamiento, diferenciando los riesgos críticos, medios y bajos en función de su efecto potencial sobre la operación y la seguridad de los activos de Auxadi Costa Rica.

Probabilidad

- 1 = Improbable
- 2 = Posible
- 3 = Ocasional
- 4 = Moderado
- 5 = Constante

Impacto

- 1 = Insignificante
- 2 = Menor

- 3 = Crítica
- 4 = Mayor
- 5 = Catastrófico

Nivel de riesgo = Probabilidad × Impacto

Clasificación

- Bajo: 1–6
- Medio: 7–14
- Crítico: 15–25

Tabla 5

Matriz de riesgos.

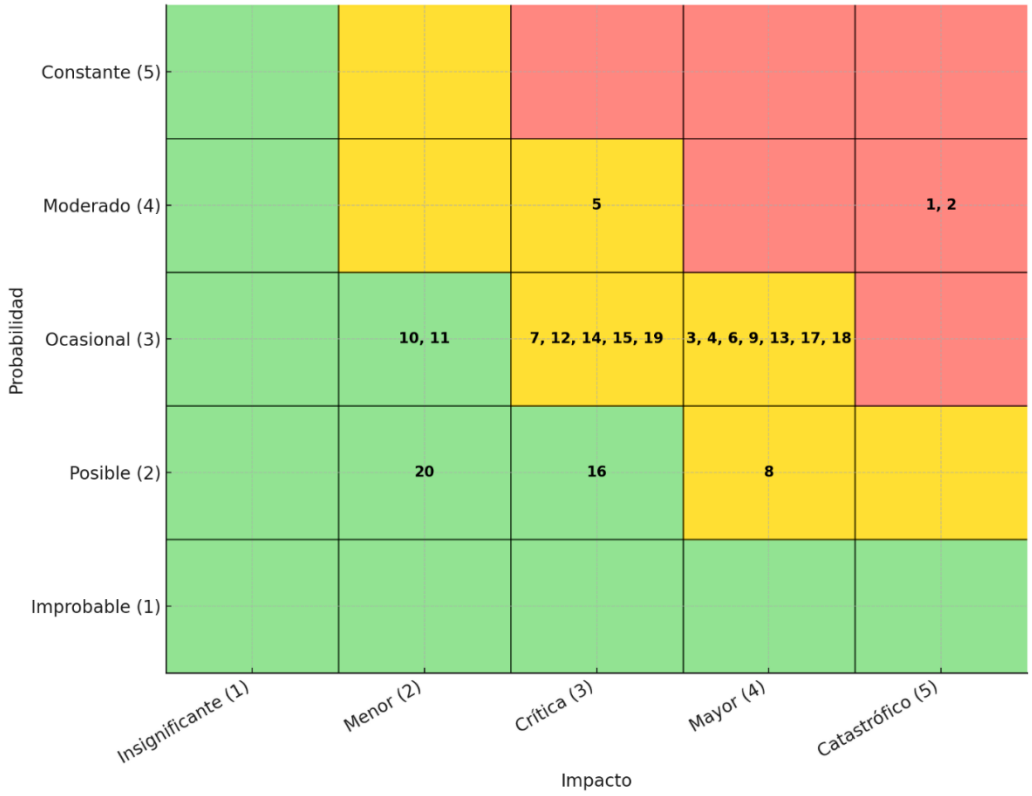
Nº	Riesgo identificado	Prob. (1–5)	Impacto (1–5)	Nivel	Clasificación	Observación
1	Pérdida de dispositivos sin respaldo ni cifrado	4	5	20	Crítico	Pérdida total de datos ante robo/extravío; falta de cifrado y evidencias de recuperación.
2	Uso compartido de credenciales o cuentas	4	5	20	Crítico	Sin controles formales; nula trazabilidad y alto riesgo de accesos indebidos.
3	Filtración de datos por error humano	3	4	12	Medio	Envíos erróneos y uso de canales inseguros; dependencia del factor humano.
4	Accesos sin control en carpetas/sistemas críticos	3	4	12	Medio	Segmentación y revisiones insuficientes de permisos.
5	Uso inconsistente de contraseñas robustas	4	3	12	Medio	Reutilización/fragilidad de claves en algunos entornos.
6	Falta de MFA en accesos críticos	3	4	12	Medio	Cobertura parcial de MFA expone accesos remotos sensibles.
7	Transmisión de información sin cifrado	3	3	9	Medio	Correo/mensajería sin cifrado en coordinaciones y soporte.
8	DRP/BCP sin pruebas integrales	2	4	8	Medio	Planes existentes, pero con validación insuficiente.
9	Protección insuficiente de datos personales	3	4	12	Medio	Falta inventario completo/consentimiento estandarizado y actualización.
10	Gestión documental dispersa	3	2	6	Bajo	Registros fragmentados dificultan trazabilidad y control.
11	Capacitación insuficiente en seguridad	3	2	6	Bajo	Formación no uniforme ni periódica.

12	BYOD sin controles específicos	3	3	9	Medio	Exposición a malware/fuga por dispositivos personales.
13	Phishing e ingeniería social	3	4	12	Medio	Intentos recurrentes; campañas aún insuficientes.
14	Políticas/procedimientos desactualizados	3	3	9	Medio	Rezago frente a cambios regulatorios y tecnológicos.
15	Monitoreo y registro de accesos/cambios insuficiente	3	3	9	Medio	Bitácoras sin revisión consolidada oportuna.
16	Ausencia de sanciones formales	2	3	6	Bajo	Falta proceso disciplinario documentado.
17	Fallas de disponibilidad en servicios críticos	3	4	12	Medio	Interrupciones sin causa raíz/acciones de mejora documentadas.
18	Cobertura limitada de riesgos en nube/teletrabajo	3	4	12	Medio	Políticas e incidentes sin enfoque formal a estos escenarios.
19	Software sin actualizaciones verificadas	3	3	9	Medio	Parches manuales dejan ventanas de vulnerabilidad.
20	Incidentes menores sin registro sistemático	2	2	4	Bajo	Falta de registro limita aprendizaje y métricas.

Fuente: Elaboración propia

Ilustración 32

Mapa de calor de matriz de riesgos.



Fuente: Elaboración propia

El resultado obtenido refleja un panorama en el cual los riesgos clasificados como críticos, en particular el riesgo uno vinculado a la pérdida de dispositivos sin medidas de protección adecuadas y el riesgo dos relacionado con el uso compartido de credenciales, concentran un nivel elevado de exposición para la organización. Ambos escenarios comprometen directamente la confidencialidad de la información sensible y debilitan la trazabilidad de accesos, lo que genera una vulnerabilidad significativa frente a posibles incidentes. Ante esta condición, se requiere la aplicación inmediata de controles robustos que incluyan cifrado de datos, políticas claras de respaldo seguro y mecanismos de autenticación individual. Estas medidas no solo mitigan el impacto potencial, sino que también fortalecen la capacidad de respuesta frente a eventos no deseados, asegurando una gestión más resiliente de los activos críticos dentro del entorno operativo de Auxadi Costa Rica.

Dentro de la categoría de riesgos clasificados como medios se concentra la mayor parte de los hallazgos identificados, entre los cuales se incluyen situaciones como filtraciones de datos ocasionadas por errores humanos, ausencia de políticas actualizadas, deficiencias en los mecanismos de monitoreo, pruebas incompletas de los planes de continuidad del negocio y limitaciones en la protección de datos personales. Este grupo abarca los riesgos numerados como tres, cuatro, cinco, seis, siete, ocho, nueve, doce, trece, catorce, quince, diecisiete, dieciocho y diecinueve, lo cual evidencia una diversidad de amenazas que, aunque no se consideran críticas de forma individual, representan un conjunto de vulnerabilidades relevantes cuando se observan de manera acumulada. Su tratamiento requiere un enfoque integral que combine tanto controles tecnológicos, como la implementación de autenticación multifactor, cifrado de la información y sistemas de monitoreo continuo, así como también acciones de carácter organizativo, tales como la actualización constante de normativas internas, campañas de concienciación dirigidas al personal, centralización de registros y revisiones periódicas de acceso. Esta combinación de estrategias fortalece la capacidad de la organización para anticiparse y responder de manera oportuna a incidentes de seguridad que, de no ser atendidos adecuadamente, podrían escalar en severidad.

Dentro de la categoría de riesgos clasificados como bajos se agrupan aquellos incidentes menos severos, entre los cuales se identifican aspectos vinculados con una capacitación insuficiente al personal, la gestión documental dispersa, la ausencia de medidas disciplinarias formalizadas ante incumplimientos y la falta de registros asociados a incidentes menores. Estos corresponden a los riesgos numerados como diez, once, dieciséis y veinte. Si bien su impacto individual es limitado en comparación con los riesgos críticos o medios, representan debilidades latentes en el sistema que, si no se abordan con oportunidad, podrían escalar con el tiempo y comprometer la estabilidad del sistema de gestión. La omisión de estos elementos puede generar un entorno propenso a la desorganización, con baja trazabilidad y menor capacidad de respuesta ante eventos de seguridad, afectando la madurez institucional y dificultando la implementación de mejoras continuas en la protección de los activos de información.

En resumen, la matriz construida ha permitido clasificar los riesgos identificados según su nivel de criticidad y ha evidenciado la necesidad de aplicar un enfoque diferenciado para su tratamiento. Los riesgos críticos demandan atención inmediata a través de la implementación de controles contundentes que reduzcan su impacto directo sobre la seguridad de los activos. Por su parte, los riesgos de nivel medio requieren medidas de mejora progresiva y sostenida, combinando recursos tecnológicos y organizativos para fortalecer las capacidades actuales. Finalmente, los riesgos de bajo impacto reflejan áreas de oportunidad donde es posible reforzar la cultura organizacional, elevando la madurez del sistema de gestión. Esta priorización proporciona una base metodológica sólida para la etapa siguiente de correlación y selección de controles, garantizando que los esfuerzos de mitigación se alineen con las prioridades estratégicas de protección de la información en Auxadi Costa Rica.

Tabla de Correlación Riesgo-Control

Objetivo de la Tabla

Establecer una correspondencia técnica entre los riesgos de seguridad identificados en Auxadi Costa Rica y los controles de seguridad propuestos en la norma ISO/IEC 27001:2022, con el fin de justificar la selección de medidas de tratamiento pertinentes que permitan fortalecer la

protección de los activos de información, reducir la exposición a amenazas y facilitar la toma de decisiones en la construcción de políticas y procedimientos específicos.

Alcance de la Tabla

Esta tabla comprende el análisis de los veinte principales riesgos identificados durante la fase diagnóstica, correlacionándolos con controles específicos de los dominios organizativos, de personas, físicos y tecnológicos de la norma ISO/IEC 27001:2022. El contenido se limita a los riesgos detectados en las áreas de gestión de dispositivos, seguridad de la comunicación y protección de datos, en coherencia con el enfoque establecido en el anteproyecto. A su vez, el análisis se fundamenta en criterios de aplicabilidad práctica dentro del entorno actual de la organización, tomando en cuenta sus procesos, recursos tecnológicos y normativas internas.

Resultados Tabla

Como parte del análisis estratégico de seguridad de la información en Auxadi Costa Rica, se construyó una matriz de correlación entre los principales riesgos identificados durante la fase diagnóstica y los controles seleccionados de la norma ISO/IEC 27001:2022. Esta matriz tiene como propósito establecer una trazabilidad directa entre las amenazas observadas y las medidas de tratamiento aplicables, permitiendo reforzar la postura de seguridad organizacional mediante un enfoque basado en riesgos.

Tabla 6

Tabla de correlación riesgo-control.

Nº	Riesgo identificado	Control ISO/IEC 27001:2022	Justificación del control aplicado
1	Pérdida de dispositivos sin respaldo ni cifrado	7.3 – Oficinas e instalaciones seguras 7.8 – Emplazamiento y protección de equipos 8.13 – Copias de seguridad 8.1 – Dispositivos de usuario	Garantiza la recuperación de datos mediante respaldos cifrados y protege físicamente los dispositivos en su ubicación; reduce el riesgo de pérdida total ante robo o extravío.
2	Uso compartido de credenciales o cuentas de usuario	5.15 – Control de acceso 5.18 – Derechos de acceso 8.5 – Autenticación segura	Se asignan credenciales únicas y se aplican reglas de acceso según rol; MFA refuerza autenticidad y trazabilidad de cada usuario.
3	Filtración de datos por error humano	5.14 – Transferencia de información	La capacitación reduce errores en el manejo de datos y el control de

		6.3 – Concienciación y capacitación	transferencia asegura el uso de canales cifrados y autorizados.
4	Accesos sin control en carpetas/sistemas críticos	5.18 – Derechos de acceso8.3 – Restricción de acceso	Obliga a asignar, revisar y revocar permisos; segmenta accesos para proteger información crítica y evitar privilegios residuales.
5	Uso inconsistente de contraseñas robustas	8.5 – Autenticación segura5.17 – Información de autenticación	Se establecen políticas de contraseñas fuertes, gestión adecuada de autenticadores y educación al personal sobre su resguardo.
6	Falta de MFA en accesos críticos	8.5 – Autenticación segura	Se implementa autenticación multifactor en accesos sensibles, mitigando riesgos de robo de credenciales.
7	Transmisión de información sin cifrado	5.14 – Transferencia de Información 8.24 – Criptografía	Se asegura la confidencialidad y autenticidad de datos en tránsito mediante cifrado y protocolos seguros.
8	DRP/BCP sin pruebas integrales	5.29 – Seguridad durante interrupciones 5.30 – Continuidad de las TIC	Obliga a validar periódicamente los planes de continuidad y probarlos para garantizar resiliencia ante contingencias.
9	Protección insuficiente de datos personales	5.12 – Clasificación de la información 5.34 – Privacidad y protección de PII 6.6 – Acuerdos de confidencialidad	Se asegura el tratamiento legal y seguro de los datos personales, su clasificación adecuada y el compromiso formal de los usuarios.
10	Gestión documental dispersa	5.33 – Protección de registros 5.37 – Procedimientos documentados	Centraliza registros de incidentes y accesos, protegiéndolos contra pérdida o alteración y asegurando trazabilidad.
11	Capacitación insuficiente en seguridad	6.3 – Concienciación y capacitación	Refuerza la cultura de seguridad con programas periódicos que eleven la madurez y reduzcan brechas humanas.
12	BYOD sin controles específicos	5.10 – Uso aceptable de activos 8.1 – Dispositivos de usuario	Define reglas claras para BYOD y protege los dispositivos personales usados en red corporativa con medidas técnicas.
13	Phishing e ingeniería social	6.3 – Concienciación y capacitación 6.8 – Informes de eventos de seguridad	La capacitación en reconocimiento de amenazas y los canales de reporte oportuno reducen impacto de ataques sociales.
14	Políticas/procedimientos desactualizados	5.1 – Políticas de seguridad de la información 5.36 – Cumplimiento de políticas	Garantiza la revisión periódica de políticas y la verificación de su cumplimiento frente a cambios regulatorios o tecnológicos.
15	Monitoreo y registro de accesos/cambios insuficiente	5.2 – Funciones y responsabilidades 8.15 – Registro 8.16 – Actividades de supervisión	Obliga a mantener registros completos de accesos/cambios, supervisar actividades y definir responsables de monitoreo.
16	Ausencia de sanciones formales	6.4 – Proceso disciplinario	Define un esquema de sanciones y medidas correctivas frente a incumplimientos, reforzando la cultura de seguridad.
17	Fallas de disponibilidad en servicios críticos	5.30 – Continuidad de las TIC 8.14 – Redundancia de instalaciones	Planes de continuidad y redundancia tecnológica minimizan interrupciones en correo, ERP o bases de datos.
18	Cobertura limitada de riesgos en nube/teletrabajo	5.23 – Seguridad en servicios en la nube 6.7 – Trabajo remoto	Define requisitos de seguridad en contratos de nube y medidas técnicas para proteger datos en entornos remotos.

19	Software sin actualizaciones verificadas	8.8 – Gestión de vulnerabilidades 8.9 – Gestión de la configuración	Establece controles para identificar y aplicar parches, asegurando configuraciones seguras y actualizadas.
20	Incidentes menores sin registro sistemático	5.27 – Aprender de incidentes 6.8 – Informes de eventos	Exige documentar incidentes menores, extraer lecciones y retroalimentar controles para la mejora continua.

Fuente: Elaboración propia

A partir del ejercicio de correlación entre los riesgos identificados y los controles establecidos por la norma ISO/IEC 27001:2022, se obtuvo una representación sistemática que muestra cómo cada escenario puede ser mitigado de manera específica mediante la aplicación de uno o más controles. Esta tabla no solo facilita el análisis técnico de la relación riesgo-control, sino que también aporta una perspectiva estratégica que fortalece la toma de decisiones orientada a la mitigación efectiva. Los controles seleccionados responden a criterios de aplicabilidad contextual, vinculados a las condiciones reales de infraestructura, operación y madurez de Auxadi Costa Rica. En este sentido, el ejercicio no se limita a establecer una relación mecánica entre riesgos y controles, sino que, valida la pertinencia de cada medida frente a la naturaleza del riesgo, reforzando el principio de proporcionalidad y efectividad que fundamenta la gestión de seguridad bajo estándares internacionales.

Durante el proceso se identificaron riesgos que, de forma intencionada, fueron asociados con múltiples controles, aplicando el principio de defensa en profundidad, el cual establece que la mitigación no puede depender de un único mecanismo, sino de la implementación de varias capas de protección complementarias. Esto se evidencia en escenarios críticos como la pérdida de dispositivos sin respaldo ni cifrado, el uso compartido de credenciales o la transmisión de información sin medidas de seguridad, donde fue necesario combinar controles tecnológicos, organizativos y físicos para reducir el nivel de exposición; de igual manera, en amenazas como el phishing y la ingeniería social se constató que la protección no puede limitarse únicamente a filtros técnicos, sino que debe reforzarse mediante programas de concienciación al personal y mecanismos de reporte oportuno. Bajo este enfoque, cada control funciona como una barrera adicional que, al integrarse con las demás, eleva la resiliencia institucional y disminuye la probabilidad de que un incidente aislado comprometa de manera significativa la seguridad de la información y la continuidad de las operaciones en Auxadi Costa Rica.

De igual forma, se logró establecer una correspondencia coherente entre la naturaleza de los riesgos y los dominios de control aplicados. Los riesgos asociados a la manipulación, pérdida o exposición de dispositivos fueron tratados con controles de seguridad física y tecnológica, mientras que aquellos relacionados con el factor humano, como el phishing, el error en la transferencia de información o la falta de capacitación, se abordaron con controles de los dominios de personas y organizativos. Esta alineación estratégica asegura que las medidas propuestas resulten pertinentes frente al tipo de amenaza y, al mismo tiempo, viables dentro del contexto operativo real de la empresa, aumentando la probabilidad de éxito en su implementación y contribuyendo al cumplimiento de los lineamientos de la norma ISO/IEC 27001:2022.

Asimismo, la correlación permitió identificar riesgos que, aunque no fueron clasificados como críticos por su nivel individual de impacto, requieren de un tratamiento más complejo debido a la combinación de controles necesarios para mitigarlos. Tal es el caso de los riesgos vinculados a la protección de datos personales, la falta de monitoreo sistemático o la cobertura insuficiente de escenarios de teletrabajo y servicios en la nube, que exigen una respuesta multifacética. Estos casos evidencian la importancia de combinar el cifrado de datos, políticas claras de uso, revisiones periódicas de accesos, formación continua del personal y la adopción de procesos de monitoreo constante.

En resumen, los resultados obtenidos reflejan un enfoque metodológico integral y plenamente alineado con el marco normativo adoptado, garantizando que la gestión de riesgos se traduzca en acciones concretas y verificables. La tabla de correlación aporta trazabilidad entre las amenazas detectadas y los controles de seguridad seleccionados, lo cual fortalece la justificación documental y sienta una base técnica confiable para la siguiente fase del proyecto. En este sentido, Auxadi Costa Rica dispone de un insumo estratégico que no solo orienta la priorización y selección de medidas de seguridad, sino que también asegura que dichas medidas estén alineadas con el objetivo central de esta investigación: diseñar políticas y procedimientos efectivos para la gestión de dispositivos, la seguridad en la comunicación y la protección de datos. De esta manera, la organización avanza hacia un modelo de gestión más maduro, con prácticas sustentadas en estándares internacionales que fortalecen la protección de sus activos críticos y contribuyen al cumplimiento de la norma ISO/IEC 27001:2022.

Informe de Validación y Ajustes Riesgo-Control

Objetivo del Informe

Se busca establecer en una sesión de análisis grupal con el equipo de TI de Auxadi Costa Rica, la pertinencia, viabilidad y suficiencia de los controles propuestos para cada riesgo identificado. En este espacio también se pretende validar que la tabla de riesgos elaborada, junto con su nivel de criticidad, sea reconocida como un insumo válido y ajustado a la realidad operativa por los responsables técnicos de la organización. El informe resultante busca confirmar qué controles funcionan en el contexto real de la empresa, qué ajustes o condiciones se requieren para aplicarlos y qué controles adicionales conviene considerar. Con ello se generan insumos claros y prácticos para que la organización pueda tomar decisiones informadas y avanzar con una propuesta de políticas y procedimientos alineada a su operación, recursos y nivel de madurez actual.

Alcance del Informe

El contenido abarca la validación de 20 riesgos relacionados con gestión de dispositivos, seguridad en la comunicación y protección de datos, considerando los dominios organizativos, de personas, físicos y tecnológicos de la ISO/IEC 27001:2022. La validación se realizó mediante entrevista grupal estructurada (sesión de análisis) con 3–5 integrantes de TI, enfocada en cuatro criterios por riesgo: adecuación del control, viabilidad con los recursos actuales, suficiencia o necesidad de controles adicionales y detalles prácticos para su implementación.

Entrevista para Validación de Controles Propuestos por Riesgo

Con el propósito de confirmar la pertinencia de los controles de seguridad propuestos y asegurar que estos se adapten al contexto real de la organización, se desarrolló una sesión de análisis con el equipo de Tecnologías de la Información de Auxadi Costa Rica. La dinámica consistió en una entrevista grupal estructurada, en la que los participantes evaluaron los riesgos identificados junto con los controles seleccionados para mitigarlos. Durante el ejercicio, se discutió

la adecuación de cada medida, su viabilidad práctica con los recursos actuales y los ajustes necesarios para fortalecer su implementación. Este proceso permitió obtener una validación consensuada, enriquecida con observaciones técnicas y recomendaciones específicas, lo cual garantiza que los resultados reflejen tanto las buenas prácticas internacionales como la realidad operativa de la empresa. Se utilizó el Apéndice F. Guía de Entrevista 3.

Resultados primer riesgo.

Riesgo: Pérdida de dispositivos sin respaldo ni cifrado.
Controles propuestos: 7.3, 7.8, 8.13, 8.1.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles seleccionados son pertinentes porque cubren tanto la protección física de los equipos como la gestión técnica (cifrado, respaldos y administración de dispositivos de usuario). Se resaltó que la combinación de controles tecnológicos (8.1, 8.13) y físicos (7.3, 7.8) responde de forma integral al riesgo.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional

Observaciones: Aunque Auxadi ya cuenta con respaldos en la nube, se validó que no existe un proceso formal de pruebas periódicas de restauración ni un lineamiento interno que exija el cifrado obligatorio de todos los portátiles. El grupo indicó que esto no requiere infraestructura nueva, pero sí políticas formales y procedimientos claros para garantizar la aplicación.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes

Controles adicionales sugeridos: Se recomendó complementar con el control 8.16 Actividades de supervisión, para asegurar que los respaldos y el cifrado sean monitoreados y auditados regularmente.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Procedimientos de supervisión y monitoreo.

Observaciones:

Política corporativa que obligue al cifrado en laptops con BitLocker o equivalente.

Registro documentado de pruebas de restauración de respaldos (mínimo 2 veces al año).

Checklist mensual de cumplimiento de cifrado y respaldos, supervisado por el área de TI.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: El riesgo se considera correctamente mitigado con los controles seleccionados, siempre y cuando se formalicen políticas internas de cifrado y pruebas de respaldo, y se añada un mecanismo de supervisión (8.16). El grupo coincidió en que la implementación es factible sin grandes inversiones, pero requiere disciplina organizativa y seguimiento continuo.

Resultados segundo riesgo.

Riesgo: Uso compartido de credenciales o cuentas de usuario.

Controles propuestos: 5.15, 5.18, 8.5.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo estuvo de acuerdo en que los controles seleccionados son pertinentes, ya que atacan directamente el problema de trazabilidad y acceso indebido. Control 5.15 establece lineamientos generales de acceso, 5.18 asegura la asignación correcta de derechos, y 8.5 garantiza autenticación robusta (MFA).

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Active Directory ya permite la administración de credenciales individuales y MFA en algunos sistemas. Sin embargo, aún hay aplicaciones heredadas que no soportan MFA, y en ciertos casos persisten cuentas genéricas. Se requiere plan de eliminación gradual de cuentas compartidas y ampliación de MFA a todos los sistemas críticos.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso incluir el control 8.16 Actividades de supervisión, para garantizar la revisión periódica de logs de acceso y detectar intentos indebidos.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Configuración técnica o herramienta específica.

Procesos de supervisión y monitoreo.

Observaciones:

Redactar una política explícita que prohíba el uso de cuentas compartidas, con sanciones claras.

Configurar revisiones trimestrales de permisos en AD y en sistemas críticos.

Extender el uso de MFA a VPN, correo y ERP.

Supervisión continua de accesos mediante reportes automáticos.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: El grupo validó que los controles seleccionados son adecuados y factibles, siempre que se refuercen con políticas claras, un plan de eliminación de cuentas compartidas y la ampliación del uso de MFA. Se acordó que estos ajustes permitirán lograr trazabilidad total y mayor seguridad en la autenticación.

Resultados tercer riesgo.

Riesgo: Filtración de datos por error humano.

Controles propuestos: 5.14, 6.3.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que ambos controles responden directamente al riesgo. 5.14 asegura que la transferencia de información se haga mediante canales cifrados y autorizados, mientras que 6.3 fortalece la cultura del personal mediante capacitación y concienciación.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Actualmente Auxadi cuenta con correo corporativo con opciones de cifrado, pero no siempre se utiliza. La capacitación en seguridad se realiza de manera puntual y no

periódica. Para que el control sea totalmente viable se requiere establecer un plan de formación continua y políticas que obliguen al uso de canales seguros.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso añadir el control 8.24 Criptografía, para reforzar la confidencialidad de la información en tránsito y garantizar que todos los correos y archivos sensibles se transmitan con cifrado obligatorio.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Capacitación del personal.

Procesos de supervisión y monitoreo.

Observaciones:

Implementar una política de “uso obligatorio de canales seguros” para transferencias de información.

Establecer capacitaciones semestrales obligatorias en buenas prácticas de manejo de información.

Habilitar auditorías aleatorias sobre correos y transferencias para verificar cumplimiento.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: El grupo validó que los controles seleccionados son correctos y factibles en Auxadi, pero requieren refuerzo con un plan formal de capacitación continua y con el uso obligatorio de cifrado en transferencias de datos. Se recomendó incluir criptografía (8.24) como control adicional para dar mayor solidez.

Resultados cuarto riesgo.

Riesgo: Accesos sin control en carpetas/sistemas críticos.
Controles propuestos: 5.18, 8.3.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles seleccionados son pertinentes porque establecen la necesidad de asignar, revisar y revocar derechos de acceso, además de segmentar los permisos para proteger sistemas y datos críticos.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya utiliza Active Directory y permisos por grupo, lo que facilita aplicar estos controles. Sin embargo, actualmente no se hacen revisiones sistemáticas ni existe un procedimiento documentado. Se requiere formalizar un proceso de revisión trimestral de accesos y un registro centralizado de autorizaciones.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso complementar con el control 8.16 Actividades de supervisión, para asegurar que los accesos sean monitoreados y que se revisen los registros de forma constante.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.
Procesos de supervisión y monitoreo.
Observaciones:
Crear política formal de gestión de accesos con revisiones trimestrales obligatorias.
Implementar registro centralizado de altas, bajas y modificaciones de permisos.
Designar responsables claros para autorizar y auditar accesos.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles propuestos son correctos y aplicables en Auxadi, pero se requiere formalizar procesos documentados y añadir monitoreo (8.16) para asegurar efectividad. El grupo consideró que, con estos ajustes, se logrará mayor trazabilidad y control sobre accesos a sistemas y carpetas críticas.

Resultados quinto riesgo.

Riesgo: Uso inconsistente de contraseñas robustas.
Controles propuestos: 8.5, 5.17.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo confirmó que los controles seleccionados son pertinentes, ya que garantizan la definición de contraseñas seguras, su gestión adecuada y la protección de la información de autenticación.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional

Observaciones: Active Directory ya permite aplicar políticas de complejidad y caducidad de contraseñas. Sin embargo, no todos los sistemas externos al dominio siguen las mismas políticas, y no se utiliza aún un gestor centralizado de contraseñas. Se requiere una ampliación de políticas a todas las aplicaciones críticas y capacitación de usuarios.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: El grupo recomendó añadir el control 6.3 Concienciación y capacitación, para reforzar la cultura de seguridad y evitar que los usuarios sigan reutilizando o compartiendo claves.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.
Capacitación del personal.
Configuración técnica o herramienta específica.
Observaciones:
Política unificada de contraseñas que abarque todos los sistemas críticos, no solo AD.
Implementar un gestor seguro de contraseñas para credenciales administrativas.
Capacitación semestral sobre riesgos de reutilizar contraseñas y phishing.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes

Notas finales: Los controles seleccionados son adecuados, pero se requiere extender las políticas de contraseñas a todos los sistemas, incluir un gestor de contraseñas y reforzar la capacitación de usuarios. Con estos ajustes, el riesgo puede ser mitigado de forma efectiva y sostenible.

Resultados sexto riesgo.

Riesgo: Falta de MFA en accesos críticos.
Control propuesto: 8.5.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, es adecuado.

Observaciones: El grupo coincidió en que el control 8.5 es el más pertinente, ya que la implementación de autenticación multifactor es la medida más efectiva para mitigar el riesgo de accesos indebidos en sistemas críticos.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya tiene habilitado MFA en algunos servicios de Office 365 y correo, lo cual muestra viabilidad. Sin embargo, existen limitaciones en aplicaciones heredadas que no soportan MFA de forma nativa, lo que requiere buscar soluciones intermedias (gateway de autenticación o migraciones graduales).

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficiente con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó complementar con el control 8.16 Actividades de supervisión, para monitorear intentos de acceso fallidos y alertar sobre intentos de intrusión.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Configuración técnica o herramienta específica.
Procesos de supervisión y monitoreo.
Observaciones:
Ampliar MFA a VPN, ERP y aplicaciones críticas en nube y on-prem.
Documentar procedimientos de activación y soporte para usuarios.
Monitorear accesos sospechosos con reportes automáticos.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes
Notas finales: El grupo validó que el control 8.5 es adecuado y viable, siempre que se planifique una ampliación progresiva a todos los accesos críticos. Se recomendó añadir supervisión activa (8.16) para complementar la efectividad del MFA.

Resultados séptimo riesgo.

Riesgo: Transmisión de información sin cifrado.
Controles propuestos: 5.14, 8.24.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que ambos controles son directamente pertinentes: 5.14 establece lineamientos de transferencia segura, mientras que 8.24 garantiza el uso de mecanismos de cifrado para proteger la confidencialidad de los datos.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya dispone de Office 365, que soporta cifrado en correos y documentos. No obstante, no todos los usuarios conocen cómo aplicarlo, y no está configurado como requisito obligatorio en todos los escenarios. Se requiere configuración adicional y capacitación.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó incluir 6.3 Concienciación y capacitación, para asegurar que los usuarios comprendan cómo y cuándo deben aplicar cifrado en la transferencia de información.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Configuración técnica o herramienta específica.

Capacitación del personal.

Observaciones:

Política de “cifrado obligatorio” para correos con información sensible.

Configuración automática de TLS/IRM en el correo corporativo.

Capacitación práctica para todos los usuarios sobre cifrado de correos y archivos.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: El grupo validó que los controles seleccionados son adecuados y viables, pero se requiere una política formal de cifrado, configuraciones automáticas en el correo y reforzar la capacitación a los usuarios para garantizar el cumplimiento.

Resultados octavo riesgo.

Planes de DRP/BCP sin pruebas integrales.

Controles propuestos: 5.29, 5.30.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles son pertinentes, ya que establecen la necesidad de garantizar seguridad en interrupciones y la continuidad de servicios TIC. Ambos responden de forma directa a la debilidad detectada en las pruebas incompletas.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya cuenta con infraestructura de respaldos y redundancia en nube, lo cual facilita aplicar estos controles. Sin embargo, el grupo reconoció que se requiere mayor formalización de pruebas integrales, con cronogramas definidos y participación de todas las áreas.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso añadir el control 8.16 Actividades de supervisión, para asegurar el registro y seguimiento de los resultados de pruebas de continuidad.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Procesos de supervisión y monitoreo.

Observaciones:

Definir política de pruebas anuales obligatorias de DRP/BCP.

Documentar resultados de cada simulacro, con indicadores de tiempo de recuperación (RTO/RPO).

Designar responsables en cada área para coordinar las pruebas.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados, pero requieren formalizar la práctica de simulacros integrales y documentar resultados. Con la adición de supervisión (8.16) y políticas claras, el riesgo puede mitigarse de manera efectiva en Auxadi.

Resultados noveno riesgo.

Protección insuficiente de datos personales.

Controles propuestos: 5.12, 5.34, 6.6.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles seleccionados son muy pertinentes: 5.12 establece la clasificación formal de información, 5.34 garantiza la protección de PII bajo lineamientos normativos, y 6.6 obliga a acuerdos de confidencialidad con el personal.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya tiene políticas de protección de datos, pero no un inventario consolidado de PII. También se requiere formalizar acuerdos de confidencialidad en contratos de todo el personal y proveedores. El grupo señaló que la implementación es viable con ajustes administrativos.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó incluir el control 5.33 Protección de registros, para garantizar la custodia adecuada de los documentos que contienen datos personales.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Procesos de supervisión y monitoreo.

Observaciones:

Crear inventario actualizado de datos personales almacenados y procesados.
Estandarizar formularios de consentimiento y actualización de datos.
Incluir acuerdos de confidencialidad en todos los contratos laborales y con proveedores.
Establecer auditorías internas periódicas sobre el uso y custodia de datos PII.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles propuestos son adecuados y viables, pero requieren ajustes prácticos como el inventario de PII, acuerdos contractuales y protección documental adicional. Con estas medidas, Auxadi podrá cumplir plenamente con la Ley 8968 y la norma ISO 27001 en materia de datos personales.

Resultados décimo riesgo.

Riesgo: Gestión documental dispersa.
Controles propuestos: 5.33, 5.37.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles propuestos son pertinentes porque permiten centralizar los registros, protegerlos contra alteración o pérdida, y establecer procedimientos estandarizados de documentación.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya usa repositorios en la nube (ej. OneDrive/SharePoint), pero no existe una política formal de clasificación ni de protección uniforme de los registros. Se validó que es viable implementar los controles, siempre que se unifique la plataforma documental y se designen responsables de custodia.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso añadir el control 8.16 Actividades de supervisión, para auditar periódicamente el cumplimiento de la política documental y detectar inconsistencias.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.
Procesos de supervisión y monitoreo.
Observaciones:
Definir política única de gestión documental.
Consolidar los registros de incidentes y accesos en un repositorio centralizado.
Designar responsables de actualización y protección de documentos.
Realizar auditorías periódicas de registros.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados, pero requieren ajustes en la práctica: centralizar la documentación, proteger los registros y establecer supervisión periódica. Con estas medidas, Auxadi podrá garantizar trazabilidad y fortalecer su capacidad de respuesta ante incidentes y auditorías.

Resultados undécimo riesgo.

Riesgo: Capacitación insuficiente en seguridad.

Control propuesto: 6.3.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, es adecuado.

Observaciones: El grupo estuvo de acuerdo en que el control 6.3 es pertinente porque aborda directamente la raíz del problema: la falta de concienciación y formación periódica en seguridad de la información.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Sí, totalmente viables.

Observaciones: Auxadi cuenta con recursos básicos (plataformas de e-learning, reuniones internas y personal de TI que puede impartir charlas) para implementar este control sin requerir grandes inversiones. El reto es establecer un cronograma y darle continuidad.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficiente con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó complementar con el control 6.8 Informes de eventos de seguridad, para reforzar que la capacitación incluya la práctica de reportar incidentes y comportamientos sospechosos.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Capacitación del personal.

Procesos de supervisión y monitoreo.

Observaciones:

Establecer un plan de capacitación semestral en seguridad de la información.

Incorporar evaluaciones cortas para medir comprensión y efectividad.

Incluir temas sobre phishing, manejo de contraseñas, uso seguro de dispositivos y protección de datos personales.

Definir métricas de asistencia y cumplimiento.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: El control 6.3 es suficiente y viable en Auxadi, siempre que se formalice un programa periódico de formación y se complemente con la práctica de reportes de incidentes. El grupo coincidió en que esto permitirá elevar la madurez en seguridad y reducir vulnerabilidades humanas.

Resultados duodécimo riesgo.

Riesgo: BYOD sin controles específicos.

Controles propuestos: 5.10, 8.1.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles son pertinentes porque establecen reglas claras para el uso aceptable de activos y definen medidas técnicas para la gestión segura de dispositivos de usuario, incluyendo los personales.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi cuenta con Microsoft Intune y capacidades de MDM (Mobile Device Management) que podrían aplicarse al BYOD, pero aún no hay políticas formales ni procesos implementados. La viabilidad es alta, pero requiere formalizar reglas y habilitar configuraciones técnicas.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso añadir el control 5.14 Transferencia de información, para asegurar que desde dispositivos personales solo se utilicen canales cifrados y autorizados.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Configuración técnica o herramienta específica.

Procesos de supervisión y monitoreo.

Observaciones:

Crear política formal de BYOD con requisitos mínimos de seguridad (antivirus, cifrado, bloqueo automático).

Configurar MDM para controlar accesos y borrar datos en caso de pérdida o salida del colaborador.

Restringir el uso de aplicaciones personales no autorizadas para manejar datos corporativos.

Establecer reportes mensuales de accesos desde dispositivos BYOD.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles propuestos son adecuados y viables en Auxadi, siempre que se formalice una política clara de BYOD y se configure un sistema de MDM para asegurar cumplimiento. Con estos ajustes, se puede reducir significativamente el riesgo de fuga o compromiso de datos desde dispositivos personales.

Resultados décimo tercer riesgo.

Riesgo: Phishing e ingeniería social.

Controles propuestos: 6.3, 6.8.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles seleccionados son pertinentes porque fortalecen la educación del personal frente a amenazas sociales y establecen canales claros para reportar incidentes.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya envía campañas internas de concienciación, pero no son regulares ni incluyen simulaciones de phishing. Además, aunque existen canales de soporte TI, no hay un procedimiento estandarizado para reportar intentos de phishing.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso añadir el control 8.16 Actividades de supervisión, para monitorear reportes de intentos de phishing y generar métricas sobre incidentes.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Capacitación del personal.

Procesos de supervisión y monitoreo.

Observaciones:

Establecer un programa semestral de simulación de phishing para medir la respuesta del personal.

Formalizar un procedimiento para reportar intentos de ingeniería social.

Crear un canal dedicado (ej. correo “phishing@auxadi.com”) para recibir reportes.

Generar estadísticas periódicas de incidentes detectados.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados, pero requieren formalizar un procedimiento de reporte, capacitaciones periódicas y simulaciones prácticas. Con la adición de supervisión (8.16), Auxadi podrá reducir significativamente la exposición a ataques de phishing y fortalecer su resiliencia frente a ingeniería social.

Resultados décimo cuarto riesgo.

Riesgo: Políticas/procedimientos desactualizados.
Controles propuestos: 5.1, 5.36.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles son pertinentes: 5.1 obliga a la existencia de políticas formales de seguridad, mientras que 5.36 garantiza su cumplimiento y revisión constante.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya dispone de un marco documental de políticas, pero no existe un ciclo de revisión definido. Es viable implementar este control, siempre que se establezca un cronograma anual y un comité responsable de revisiones.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso añadir el control 5.37 Procedimientos documentados, para reforzar que la actualización de políticas vaya acompañada de procedimientos claros y actualizados.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.
Procesos de supervisión y monitoreo.
Observaciones:
Definir cronograma anual de revisión y actualización de políticas.
Establecer comité de seguridad encargado de aprobar cambios.
Documentar versiones anteriores para asegurar trazabilidad.

Realizar auditorías internas de cumplimiento.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados, pero requieren ajustes prácticos: ciclo de revisión anual, comité responsable y procedimientos documentados que aseguren cumplimiento. Con estas medidas, Auxadi podrá mantener sus políticas actualizadas frente a cambios regulatorios y tecnológicos.

Resultados décimo quinto riesgo.

Riesgo: Monitoreo y registro de accesos/cambios insuficiente.
Controles propuestos: 5.2, 8.15, 8.16.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles seleccionados son pertinentes: 5.2 asigna responsabilidades claras, 8.15 exige mantener registros completos y 8.16 obliga a supervisar continuamente dichos registros.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya cuenta con registros en AD y logs de sistemas, pero no se consolidan ni se revisan con frecuencia. Se requiere asignar responsables y utilizar herramientas de correlación de eventos para hacer viable la aplicación integral de los controles.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se sugirió incluir el control 5.25 Revisión independiente de la seguridad de la información, para asegurar que las revisiones de accesos y cambios sean verificadas por una segunda parte.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Procesos de supervisión y monitoreo.

Configuración técnica o herramienta específica.

Observaciones:

Asignar responsables formales para la revisión periódica de registros.

Centralizar los logs en una herramienta única de monitoreo (ej. SIEM).

Definir alertas automáticas para accesos no autorizados o cambios críticos.

Realizar revisiones trimestrales documentadas.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados, pero requieren complementar con supervisión independiente y consolidación de registros en una herramienta centralizada. Con estos ajustes, Auxadi podrá fortalecer la trazabilidad y detección temprana de incidentes.

Resultados décimo sexto riesgo.

Riesgo: Ausencia de sanciones formales.

Control propuesto: 6.4.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, es adecuado

Observaciones: El grupo coincidió en que el control 6.4 es pertinente, ya que define un marco disciplinario claro y proporcional ante incumplimientos de seguridad, fomentando la responsabilidad individual.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Sí, totalmente viables.

Observaciones: Auxadi ya cuenta con un reglamento interno de trabajo que podría ampliarse para incluir sanciones específicas en materia de seguridad de la información. No requiere inversión adicional, solo actualización documental y validación con el área legal.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficiente con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó reforzar con el control 5.36 Cumplimiento de políticas, para asegurar que las sanciones se apliquen de manera consistente y auditada.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Procesos de supervisión y monitoreo.

Observaciones:

Incluir un apartado disciplinario en la política de seguridad de la información.

Definir sanciones graduadas (advertencia, suspensión, despido) según gravedad de la falta.

Capacitar a los colaboradores sobre las consecuencias de incumplir normas de seguridad.

Documentar todos los casos de aplicación disciplinaria.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: El control 6.4 es adecuado y viable en Auxadi. Se recomienda integrarlo al reglamento interno y complementarlo con el control 5.36 para asegurar trazabilidad y consistencia. Con estos ajustes, el riesgo puede ser mitigado y se fortalecerá la cultura de cumplimiento.

Resultados décimo séptimo riesgo.

Riesgo: Fallas de disponibilidad en servicios críticos.

Controles propuestos: 5.30, 8.14.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados

Observaciones: El grupo validó que los controles son pertinentes: 5.30 asegura planes de continuidad para servicios TIC y 8.14 exige redundancia tecnológica para minimizar interrupciones en correo, ERP o bases de datos.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya utiliza respaldos en nube y redundancia en servidores físicos, lo que hace viables los controles. Sin embargo, se requiere fortalecer la documentación y formalizar pruebas periódicas de continuidad con participación de todas las áreas.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes

Controles adicionales sugeridos: Se recomendó incluir el control 5.29 Seguridad durante interrupciones, para reforzar las medidas de seguridad, mientras los sistemas están fuera de servicio.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Procesos de supervisión y monitoreo.

Observaciones:

Documentar procedimientos de continuidad con responsables y tiempos de recuperación (RTO/RPO).

Realizar pruebas integrales al menos una vez al año.

Establecer métricas de disponibilidad y reportes periódicos.

Incluir un plan de comunicación interna para interrupciones.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados y en gran medida ya viables en Auxadi, pero requieren ajustes como la documentación formal, pruebas periódicas y medidas adicionales de seguridad en interrupciones. Con estos ajustes, el riesgo puede mitigarse efectivamente.

Resultados décimo octavo riesgo.

Riesgo: Cobertura limitada de riesgos en nube/teletrabajo.

Controles propuestos: 5.23, 6.7.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo validó que los controles seleccionados son pertinentes: 5.23 establece requisitos de seguridad en los contratos de servicios en la nube y 6.7 define lineamientos para proteger información en entornos de teletrabajo.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi ya utiliza nube con Office 365 y respaldos, y tiene experiencia en teletrabajo, pero no existen políticas escritas ni procesos de supervisión. La aplicación de los controles es viable, siempre que se documenten y formalicen las medidas.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se propuso complementar con el control 8.24 Criptografía, para reforzar la seguridad de la información en tránsito desde accesos remotos.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.

Configuración técnica o herramienta específica.

Procesos de supervisión y monitoreo.

Observaciones:

Crear una política de teletrabajo con requisitos mínimos de seguridad en dispositivos personales y conexiones.

Incluir cláusulas contractuales de seguridad en los acuerdos con proveedores de nube.

Habilitar cifrado obligatorio en comunicaciones remotas (VPN, TLS).

Realizar monitoreo activo de accesos desde ubicaciones externas.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados y viables en Auxadi, pero requieren formalizar políticas de teletrabajo y seguridad en la nube, además de reforzar el cifrado en accesos remotos. Con estos ajustes, se puede cubrir de manera efectiva la exposición de datos en entornos externos.

Resultados décimo noveno riesgo.

Riesgo: Software sin actualizaciones verificadas.
Controles propuestos: 8.8, 8.9.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles propuestos son pertinentes: 8.8 establece procesos formales de gestión de vulnerabilidades y 8.9 garantiza configuraciones seguras y verificadas.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Actualmente, Auxadi aplica parches manualmente en algunos sistemas y no cuenta con una herramienta unificada de gestión. La implementación de estos controles es viable, pero requiere adquirir o configurar soluciones de actualización centralizada.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó incluir el control 8.16 Actividades de supervisión, para asegurar que los parches y configuraciones aplicadas sean revisados y validados periódicamente.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Configuración técnica o herramienta específica.
Procesos de supervisión y monitoreo.
Observaciones:
Implementar una solución centralizada de gestión de parches.
Definir un calendario de actualizaciones críticas y revisiones de configuración.
Documentar los cambios aplicados para asegurar trazabilidad.
Establecer métricas de cumplimiento de actualizaciones.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados y viables, pero requieren reforzarse con monitoreo y herramientas centralizadas para la gestión de actualizaciones. Con estos ajustes, Auxadi podrá reducir vulnerabilidades y garantizar configuraciones seguras.

Resultados vigésimo riesgo.

Riesgo: Incidentes menores sin registro sistemático.
Controles propuestos: 5.27, 6.8.

- Pregunta 1: ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?

Sí, son adecuados.

Observaciones: El grupo coincidió en que los controles propuestos son pertinentes: 5.27 obliga a documentar incidentes para generar lecciones aprendidas y 6.8 establece reportes de eventos que permiten trazabilidad.

- Pregunta 2: ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?

Parcialmente viables, requieren apoyo adicional.

Observaciones: Auxadi cuenta con registros de incidentes mayores, pero no tiene un procedimiento definido para los menores. Es viable implementar el control mediante un sistema de tickets o un registro unificado, con capacitación al personal para reportar eventos.

- Pregunta 3: ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?

Suficientes con pequeños ajustes.

Controles adicionales sugeridos: Se recomendó complementar con el control 8.16 Actividades de supervisión, para asegurar que los reportes se revisen periódicamente y no queden sin seguimiento.

- Pregunta 4: ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?

Políticas internas adicionales.
Procesos de supervisión y monitoreo.
Observaciones:
Establecer un procedimiento formal de registro de incidentes menores.
Habilitar un sistema sencillo (ej. tickets en Service Desk) para documentar eventos.
Capacitar a los usuarios en la importancia de reportar incluso incidentes menores.
Generar reportes trimestrales de incidentes y acciones preventivas aplicadas.

- Pregunta 5: Conclusión grupal sobre el riesgo y sus controles asociados:

Validado con ajustes.

Notas finales: Los controles seleccionados son adecuados y viables, pero requieren formalizar un proceso de registro de incidentes menores y reforzarlo con supervisión periódica. Con estos ajustes, Auxadi podrá aprender de todos los eventos y fortalecer su sistema de mejora continua.

Resultados Informe

El proceso de validación inició con la revisión de la tabla de riesgos identificados y su nivel de criticidad, la cual fue validada en primera instancia por el equipo de TI como insumo confiable y ajustado a la realidad operativa. Posteriormente, durante la sesión grupal, se confirmó que dichos riesgos eran pertinentes y se procedió a analizarlos uno por uno mediante preguntas específicas asociadas a cada caso. Esta dinámica permitió confirmar que los controles seleccionados en la fase anterior son en su mayoría adecuados para responder a los riesgos identificados. El grupo de análisis coincidió en que existe una correspondencia clara entre cada amenaza y las medidas de mitigación propuestas, lo que asegura que la organización cuenta con una base sólida para estructurar políticas y procedimientos efectivos. No obstante, también se evidenció la necesidad de realizar ciertos ajustes y condiciones prácticas para que su implementación sea realmente viable dentro del entorno operativo de Auxadi Costa Rica.

Tabla 7

Tabla de validación y ajustes Riesgo-Control.

Nº	Riesgo identificado	Controles propuestos	Veredicto del grupo	Ajustes / Condiciones necesarias	Controles adicionales sugeridos
1	Pérdida de dispositivos sin respaldo ni cifrado	7.3 – Oficinas e instalaciones seguras 7.8 – Emplazamiento y protección de equipos 8.13 – Copias de seguridad 8.1 – Dispositivos de usuario	Validado con ajustes	Se requiere aplicar cifrado obligatorio en laptops y dispositivos móviles, establecer política formal de respaldos automáticos y asegurar que los dispositivos críticos estén protegidos físicamente en oficinas seguras.	6.3 – Concienciación y capacitación
2	Uso compartido de credenciales o cuentas	5.15 – Control de acceso 5.18 – Derechos de acceso	Validado con ajustes	Es necesario reforzar la política de credenciales únicas, ampliar MFA en accesos críticos y establecer revisiones periódicas de cuentas para asegurar trazabilidad y responsabilidad individual.	8.16 – Actividades de supervisión

		8.5 – Autenticación segura			
3	Filtración de datos por error humano	5.14 – Transferencia de información 6.3 – Concienciación y capacitación	Validado con ajustes	Se deben definir lineamientos claros para la transferencia de datos, aplicar canales cifrados obligatorios y reforzar al personal mediante capacitaciones periódicas sobre buenas prácticas de manejo de información.	8.24 – Criptografía
4	Accesos sin control en carpetas/sistemas críticos	5.18 – Derechos de acceso 8.3 – Restricción de acceso	Validado con ajustes	Se requiere segmentar accesos en función del rol, revisar y revocar permisos inactivos regularmente, y documentar procesos para evitar acumulación de privilegios residuales.	8.16 – Actividades de supervisión
5	Uso inconsistente de contraseñas robustas	8.5 – Autenticación segura 5.17 – Información de autenticación	Validado con ajustes	Es necesario unificar la política de contraseñas fuertes, habilitar el uso de gestores de credenciales seguros y realizar capacitaciones sobre almacenamiento y manejo adecuado de contraseñas.	6.3 – Concienciación y capacitación
6	Falta de MFA en accesos críticos	8.5 – Autenticación segura	Validado con ajustes	Se debe ampliar MFA a VPN, ERP y aplicaciones críticas, documentar los procedimientos de activación para usuarios y habilitar monitoreo de intentos fallidos con alertas automáticas.	8.16 – Actividades de supervisión
7	Transmisión de información sin cifrado	5.14 – Transferencia de información 8.24 – Criptografía	Validado con ajustes	Es necesario aplicar política de cifrado obligatorio en correos con datos sensibles, configurar TLS/IRM en correo corporativo y capacitar a usuarios en el uso correcto de herramientas de cifrado.	6.3 – Concienciación y capacitación
8	DRP/BCP sin pruebas integrales	5.29 – Seguridad durante interrupciones 5.30 – Continuidad de las TIC	Validado con ajustes	Se debe formalizar un cronograma de simulacros integrales de continuidad, documentar resultados y lecciones aprendidas, e involucrar a todas las áreas críticas en las pruebas.	8.16 – Actividades de supervisión
9	Protección insuficiente de datos personales	5.12 – Clasificación de la información 5.34 – Privacidad y protección de PII 6.6 – Acuerdos de confidencialidad	Validado con ajustes	Es necesario consolidar un inventario actualizado de PII, estandarizar formularios de consentimiento, incluir cláusulas de confidencialidad en contratos y establecer auditorías periódicas.	5.33 – Protección de registros
10	Gestión documental dispersa	5.33 – Protección de registros 5.37 – Procedimientos documentados	Validado con ajustes	Se requiere unificar los registros en un repositorio centralizado, asignar responsables de custodia, establecer procedimientos uniformes y realizar auditorías periódicas de cumplimiento.	8.16 – Actividades de supervisión
11	Capacitación insuficiente en seguridad	6.3 – Concienciación y capacitación	Validado con ajustes	Se debe implementar un plan semestral de capacitación con evaluaciones, incluir simulaciones de phishing y establecer métricas de participación y efectividad.	6.8 – Informes de eventos de seguridad
12	BYOD sin controles específicos	5.10 – Uso aceptable de activos 8.1 – Dispositivos de usuario	Validado con ajustes	Es necesario crear una política formal de BYOD, habilitar MDM para controlar accesos y borrar datos en caso de pérdida, y restringir	5.14 – Transferencia de información

				aplicaciones no autorizadas en dispositivos personales.	
13	Phishing e ingeniería social	6.3 – Concienciación y capacitación 6.8 – Informes de eventos de seguridad	Validado con ajustes	Se debe establecer un programa semestral de simulaciones de phishing, formalizar el canal de reporte de intentos y generar estadísticas de incidentes detectados.	8.16 – Actividades de supervisión
14	Políticas/procedimientos desactualizados	5.1 – Políticas de seguridad de la información 5.36 – Cumplimiento de políticas	Validado con ajustes	Es necesario definir un ciclo anual de revisión, crear un comité de seguridad responsable de actualizaciones y documentar versiones anteriores para asegurar trazabilidad.	5.37 – Procedimientos documentados
15	Monitoreo y registro de accesos/cambios insuficiente	5.2 – Funciones y responsabilidades 8.15 – Registro 8.16 – Actividades de supervisión	Validado con ajustes	Se requiere consolidar logs en una herramienta SIEM, definir alertas automáticas, asignar responsables de revisión y realizar auditorías trimestrales de accesos y cambios.	5.25 – Revisión independiente de la seguridad de la información
16	Ausencia de sanciones formales	6.4 – Proceso disciplinario	Validado con ajustes	Se debe integrar un esquema de sanciones en el reglamento interno, definir niveles según la gravedad de faltas y documentar todos los casos para garantizar trazabilidad y consistencia.	5.36 – Cumplimiento de políticas
17	Fallas de disponibilidad en servicios críticos	5.30 – Continuidad de las TIC 8.14 – Redundancia de instalaciones	Validado con ajustes	Es necesario documentar procedimientos de continuidad con tiempos RTO/RPO, realizar pruebas anuales, definir métricas de disponibilidad y establecer un plan de comunicación en interrupciones.	5.29 – Seguridad durante interrupciones
18	Cobertura limitada de riesgos en nube/teletrabajo	5.23 – Seguridad en servicios en la nube 6.7 – Trabajo remoto	Validado con ajustes	Se debe formalizar una política de teletrabajo, incluir cláusulas de seguridad en contratos de nube, habilitar cifrado obligatorio en accesos remotos y monitorear sesiones externas.	8.24 – Criptografía
19	Software sin actualizaciones verificadas	8.8 – Gestión de vulnerabilidades8.9 – Gestión de la configuración	Validado con ajustes	Es necesario implementar una herramienta de gestión de parches centralizada, definir un calendario de actualizaciones críticas y documentar los cambios aplicados para trazabilidad.	8.16 – Actividades de supervisión
20	Incidentes menores sin registro sistemático	5.27 – Aprender de incidentes 6.8 – Informes de eventos de seguridad	Validado con ajustes	Se requiere establecer un procedimiento formal de registro de incidentes menores, capacitar al personal en su reporte y generar reportes trimestrales con métricas de lecciones aprendidas.	8.16 – Actividades de supervisión

Fuente: Elaboración propia

En los riesgos clasificados como críticos, como la pérdida de dispositivos sin medidas de protección y el uso compartido de credenciales, se determinó que los controles propuestos son pertinentes, pero requieren acciones adicionales como el cifrado obligatorio, la aplicación extendida de autenticación multifactor y la creación de políticas claras sobre gestión de accesos.

Estas medidas fueron validadas como prioritarias, ya que inciden directamente en la confidencialidad y trazabilidad de la información, elementos fundamentales para la seguridad de los activos críticos. Además, el grupo coincidió en que su implementación debe realizarse de forma inmediata y acompañada de un monitoreo constante, pues cualquier retraso en su aplicación mantendría a la organización expuesta a incidentes que podrían tener un impacto severo en la continuidad del negocio y en el cumplimiento normativo.

En el caso de los riesgos de nivel medio, que abarcan una amplia gama de escenarios como filtraciones de datos por error humano, uso inconsistente de contraseñas, transmisión de información sin cifrado o pruebas insuficientes de planes de continuidad, la validación evidenció que los controles seleccionados son adecuados siempre que se acompañen de capacitaciones constantes, procedimientos documentados y herramientas de supervisión. Se recalcó que estas medidas, aunque no requieran grandes inversiones, son esenciales para fortalecer la cultura de seguridad y prevenir incidentes recurrentes. Asimismo, se destacó que la correcta implementación de estos controles contribuye a consolidar un marco preventivo más robusto, permitiendo que la organización responda de manera oportuna frente a amenazas comunes y, al mismo tiempo, mejore gradualmente la madurez de su sistema de gestión de seguridad de la información.

Por su parte, los riesgos de bajo impacto como la ausencia de sanciones formales, la dispersión de documentos o la falta de registro de incidentes menores, también fueron validados como relevantes, ya que, si bien no generan consecuencias inmediatas de gran magnitud, su acumulación puede debilitar la madurez institucional y dificultar auditorías futuras. Para estos casos se sugirió principalmente reforzar las políticas internas, formalizar procesos de registro y establecer medidas disciplinarias que promuevan una cultura de cumplimiento. Además, se subrayó que atender estos aspectos fortalece la trazabilidad y orden documental, previene malas prácticas que pueden normalizarse con el tiempo y refuerza el compromiso del personal con las directrices de seguridad, garantizando así una mejora continua en la gestión de la información.

En general, la validación grupal concluyó que todos los controles seleccionados son pertinentes, aunque la mayoría de ellos requieren ajustes específicos para adaptarse plenamente a la realidad de la empresa. Estos ajustes incluyen la definición de políticas internas más claras, la

consolidación de procesos de supervisión, la implementación de herramientas técnicas de apoyo y la integración de métricas que permitan evaluar la efectividad de cada medida. El ejercicio no solo confirmó la validez de los controles, sino que también proporcionó recomendaciones valiosas que servirán de guía para el diseño de políticas y procedimientos formales en las siguientes etapas del proyecto.

Informe de Viabilidad Técnica y Organizacional

Objetivo del Informe

El objetivo de este informe es analizar la capacidad actual de Auxadi Costa Rica para implementar los controles seleccionados durante la fase de validación de riesgos. Se busca determinar si estos controles pueden adoptarse de manera efectiva considerando la infraestructura tecnológica disponible, la preparación del personal y los procesos internos existentes. Asimismo, se pretende identificar posibles limitaciones y proponer estrategias de adaptación que permitan garantizar la viabilidad práctica de las medidas de seguridad, asegurando así su alineación con el contexto operativo de la empresa.

Alcance de la Revisión

La revisión abarca los 20 riesgos previamente identificados y validados en el apartado anterior, junto con los controles seleccionados y los ajustes propuestos. Para cada riesgo se evaluó la viabilidad técnica en relación con la infraestructura, herramientas y capacidades tecnológicas disponibles, y la viabilidad organizacional en términos de políticas, procedimientos, roles y competencias del personal. Además, se definieron estrategias de adaptación que orienten a la empresa sobre cómo superar las barreras detectadas. El alcance de este análisis es interno y se limita al contexto real de Auxadi Costa Rica, constituyendo un insumo clave para la posterior formulación de políticas y procedimientos formales en el marco de la norma ISO/IEC 27001:2022.

Resultados Informe

El análisis de viabilidad técnica y organizacional constituye una etapa clave para asegurar que los controles seleccionados en la fase de validación puedan ser implementados de manera efectiva en Auxadi Costa Rica. Este apartado se centra en evaluar la capacidad real de la empresa para adoptar dichas medidas, considerando tanto la infraestructura tecnológica existente como la preparación del personal y los procesos internos. A través de este ejercicio se busca determinar si los controles son plenamente aplicables en el contexto actual, qué limitaciones podrían presentarse y qué estrategias de adaptación conviene definir para superar dichas barreras. De esta forma, se garantiza que las propuestas de seguridad no se limiten a lineamientos teóricos, sino que respondan a condiciones prácticas y alcanzables dentro de la organización, fortaleciendo la resiliencia y asegurando la continuidad de las operaciones críticas.

Resultados primer riesgo.

Riesgo: Pérdida de dispositivos sin respaldo ni cifrado.
Controles propuestos: 6.3, 7.3, 7.8, 8.13, 8.1.

- Viabilidad técnica: Auxadi ya dispone de infraestructura tecnológica que permite aplicar estos controles, como el uso de respaldos en la nube mediante servicios de Microsoft 365 y la posibilidad de habilitar BitLocker para el cifrado de discos en laptops. Sin embargo, se identificó que no existe un proceso formalizado para realizar pruebas de restauración periódicas ni un monitoreo automatizado del estado del cifrado. Esto indica que, aunque la capacidad técnica está presente, se requiere reforzar los mecanismos de control para garantizar continuidad y resiliencia frente a incidentes.
- Viabilidad organizacional: Actualmente, las prácticas relacionadas con respaldos y cifrado no están respaldadas por políticas claras ni procedimientos documentados. El personal de TI tiene la competencia técnica para implementar estas medidas, pero sin una política corporativa formal y sin asignación de responsabilidades, existe el riesgo de que se apliquen de forma inconsistente. Además, se resaltó que es necesario incluir campañas de concienciación (control 6.3) para que los usuarios comprendan la importancia del cifrado y los respaldos, reforzando así la responsabilidad compartida entre TI y colaboradores.

- Estrategia de adaptación: La adopción de este conjunto de controles se puede lograr mediante tres pasos principales: primero establecer una política obligatoria de cifrado en todos los dispositivos de usuario y servidores, segundo implementar un calendario de pruebas de restauración de respaldos al menos dos veces por año, y generar un checklist mensual, supervisado por TI, que confirme el cumplimiento de estas medidas. De forma complementaria, se deben realizar capacitaciones semestrales para sensibilizar al personal sobre el uso seguro de dispositivos y la importancia de las copias de seguridad. Con ello, las capacidades técnicas existentes se transforman en prácticas sostenibles y verificables dentro de la organización.

Resultados segundo riesgo.

Riesgo: Uso compartido de credenciales o cuentas de usuario.
Controles propuestos: 5.15, 5.18, 8.5, 8.16.

- Viabilidad técnica: Auxadi ya cuenta con Active Directory para la gestión de usuarios, lo que permite administrar credenciales individuales y definir derechos de acceso de forma granular. Además, algunos sistemas críticos ya utilizan autenticación multifactor (MFA) a través de Office 365. No obstante, se identificaron limitaciones en aplicaciones heredadas que no soportan MFA de manera nativa, lo que representa un reto técnico que deberá abordarse mediante soluciones de integración o migración a plataformas más modernas. Por lo tanto, la viabilidad técnica es buena, pero requiere ajustes para garantizar cobertura total en todos los sistemas críticos.
- Viabilidad organizacional: A nivel de procesos, todavía se mantienen cuentas genéricas en uso y no existe una política formal que prohíba expresamente esta práctica. Esto genera debilidades en la trazabilidad de las acciones de los usuarios. El equipo de TI tiene la capacidad para implementar y administrar los controles, pero se necesita apoyo de la dirección para formalizar reglas y sanciones que refuercen el cumplimiento. Asimismo, el control 8.16 resalta la importancia de supervisar de forma constante los registros de acceso, lo cual exige designar responsables internos y crear un esquema de auditoría periódica que asegure disciplina en la revisión.

- Estrategia de adaptación: Para viabilizar la adopción de estos controles, se recomienda un plan en tres fases: primero, emitir una política corporativa que prohíba el uso de cuentas compartidas y establezca sanciones claras en caso de incumplimiento; segundo, diseñar un plan de eliminación gradual de cuentas genéricas, priorizando los sistemas críticos y migrando progresivamente los accesos hacia credenciales individuales con MFA; y tercero, habilitar revisiones trimestrales de permisos en Active Directory y otros sistemas clave, acompañadas de la supervisión definida en el control 8.16. Con estas acciones, Auxadi podrá alcanzar trazabilidad total de accesos y fortalecer la seguridad de autenticación en todos los entornos.

Resultados tercer riesgo.

Riesgo: Filtración de datos por error humano.
Controles propuestos: 5.14, 6.3, 8.24.

- Viabilidad técnica: Auxadi ya cuenta con servicios corporativos de correo electrónico en Office 365 que permiten aplicar cifrado en la transferencia de información, lo que facilita el cumplimiento del control 5.14. Sin embargo, el cifrado no está configurado como obligatorio, lo que deja espacio a errores humanos en el manejo de datos sensibles. Además, la incorporación de mecanismos criptográficos más estrictos (8.24) es técnicamente viable con la infraestructura existente, pero requiere ajustes de configuración y activación de licencias específicas. En este sentido, la empresa tiene los recursos necesarios, aunque la aplicación depende de ajustes técnicos puntuales y de una mayor disciplina en su uso.
- Viabilidad organizacional: Actualmente, el uso de canales seguros para transferencias de datos no está respaldado por políticas internas obligatorias, lo que genera que los usuarios, por desconocimiento o descuido, empleen medios no autorizados. El personal de TI puede aplicar las configuraciones técnicas, pero sin capacitación recurrente (6.3) es probable que las buenas prácticas no se mantengan en el tiempo. Por lo tanto, la viabilidad organizacional es media, ya que depende de formalizar normativas y reforzar la cultura de seguridad para lograr un cumplimiento sostenido.

- Estrategia de adaptación: Para asegurar la efectividad de estos controles, se recomienda establecer una política que exija el uso exclusivo de canales cifrados en transferencias de información, habilitar de forma predeterminada la opción de cifrado en correos corporativos y archivos sensibles, y realizar capacitaciones semestrales sobre el manejo seguro de la información. De forma complementaria, deben implementarse auditorías aleatorias para verificar que los usuarios cumplan las directrices, fortaleciendo así la trazabilidad y reduciendo la probabilidad de incidentes por error humano.

Resultados cuarto riesgo.

Riesgo: Accesos sin control en carpetas/sistemas críticos.
Controles propuestos: 5.18, 8.3, 8.16.

- Viabilidad técnica: Auxadi cuenta con Active Directory y permisos por grupos, lo que permite implementar controles de asignación y restricción de accesos de forma eficiente (5.18 y 8.3). Sin embargo, actualmente no existe un procedimiento formalizado para la revisión y revocación periódica de permisos. La aplicación del control adicional 8.16, orientado a la supervisión, es técnicamente viable mediante las herramientas de logs y auditorías disponibles, aunque requiere consolidar la información en reportes periódicos. En términos técnicos, la empresa tiene la capacidad instalada, pero necesita estructurar un modelo de monitoreo más consistente.
- Viabilidad organizacional: En el plano organizativo, si bien el equipo de TI aplica segmentación de accesos en los sistemas, no hay un proceso documentado que establezca revisiones regulares ni responsables claros. Esto representa un riesgo de acumulación de privilegios innecesarios. El personal de TI tiene la preparación para ejecutar los controles, pero se requiere definir responsabilidades formales y un flujo de aprobación de accesos. Por lo tanto, la viabilidad organizacional es alta, siempre que se formalicen procedimientos y se integre la supervisión dentro de las rutinas de gestión.
- Estrategia de adaptación: Para fortalecer la implementación, se recomienda diseñar una política de gestión de accesos que incluya revisiones trimestrales obligatorias, un

registro centralizado de altas y bajas de usuarios, y la designación de responsables específicos para autorizar y auditar accesos. Asimismo, se deben habilitar reportes periódicos que verifiquen la efectividad del control 8.16, asegurando que las actividades de monitoreo sean constantes y auditables. Estas medidas permitirán que los accesos a carpetas y sistemas críticos estén debidamente controlados y trazables.

Resultados quinto riesgo.

Riesgo: Uso inconsistente de contraseñas robustas.
Controles propuestos: 8.5, 5.17, 6.3.

- Viabilidad técnica: Auxadi ya utiliza Active Directory para gestionar contraseñas en el dominio, lo que permite aplicar requisitos de complejidad y caducidad (8.5 y 5.17). No obstante, algunas aplicaciones externas al dominio aún no aplican políticas de seguridad homogéneas, lo que dificulta un control centralizado. La integración de un gestor de contraseñas corporativo sería técnicamente viable y contribuiría a mejorar la gestión de credenciales. Por lo tanto, la viabilidad técnica es buena, pero requiere ampliar las configuraciones a todos los sistemas críticos y considerar herramientas adicionales para garantizar uniformidad.
- Viabilidad organizacional: Desde la perspectiva organizativa, la aplicación de contraseñas robustas no está unificada en toda la empresa y no existe una política clara que abarque los distintos entornos tecnológicos. Esto provoca que algunos usuarios reutilicen claves o no sigan buenas prácticas de resguardo. La capacitación (6.3) es clave para generar conciencia en los colaboradores y reforzar la responsabilidad individual en el manejo de credenciales. En consecuencia, la viabilidad organizacional depende de formalizar directrices y acompañarlas con sesiones periódicas de sensibilización.
- Estrategia de adaptación: Para garantizar la efectividad de estos controles, se recomienda unificar la política de contraseñas a nivel corporativo, abarcando tanto el dominio como las aplicaciones externas. Además, se sugiere implementar un gestor seguro de contraseñas para cuentas administrativas y realizar capacitaciones

semestrales sobre los riesgos asociados al uso inadecuado de claves. Estas acciones, combinadas con un seguimiento constante de cumplimiento, permitirán fortalecer la protección de credenciales y reducir la posibilidad de accesos indebidos por malas prácticas de los usuarios.

Resultados sexto riesgo.

Riesgo: Falta de MFA en accesos críticos.
Controles propuestos: 8.5, 8.16.

- Viabilidad técnica: Auxadi ya tiene habilitado el uso de MFA en algunos servicios de Office 365 y en el correo electrónico corporativo, lo que demuestra que la infraestructura técnica básica para aplicar el control 8.5 está disponible. Sin embargo, existen limitaciones en aplicaciones heredadas y en ciertos accesos remotos que no soportan multifactor de forma nativa. Para estos casos, sería necesario implementar soluciones intermedias, como gateways de autenticación o la migración gradual a plataformas que soporten MFA. El control 8.16 también es técnicamente viable, ya que los sistemas actuales permiten generar reportes de intentos fallidos y accesos sospechosos, aunque se requiere centralizar la supervisión en un sistema de monitoreo más robusto.
- Viabilidad organizacional: Desde el punto de vista organizativo, el personal de TI tiene experiencia con la administración de MFA y puede gestionar su extensión a más entornos. No obstante, se requiere que la empresa defina una política corporativa que obligue al uso de MFA en todos los accesos críticos y que contemple procedimientos de soporte para los usuarios. Además, es necesario asignar responsables de supervisión para dar seguimiento a los reportes de accesos fallidos y responder oportunamente a posibles incidentes. La viabilidad organizacional es alta, pero depende de formalizar reglas internas y asegurar compromiso gerencial.
- Estrategia de adaptación: Para garantizar la adopción de este control, se recomienda establecer un plan de despliegue progresivo que inicie con sistemas críticos como ERP, VPN y plataformas en la nube. Este plan debe incluir la documentación de

procedimientos de activación de MFA, sesiones de capacitación a usuarios sobre su uso, y la integración de alertas automáticas que permitan al equipo de TI detectar intentos indebidos en tiempo real. Con ello, se asegura que la empresa alcance un nivel de autenticación robusto y trazable en todos sus accesos sensibles.

Resultados séptimo riesgo.

Riesgo: Transmisión de información sin cifrado.
Controles propuestos: 5.14, 8.24, 6.3.

- Viabilidad técnica: Auxadi utiliza Office 365, el cual soporta cifrado en correos electrónicos y documentos compartidos, lo que facilita la implementación de los controles 5.14 y 8.24. Sin embargo, estas funciones no están configuradas como obligatorias en todos los escenarios, lo que deja espacio para que algunos datos sensibles sean transmitidos sin la debida protección. A nivel técnico, la infraestructura ya existe, pero es necesario activar configuraciones predeterminadas que fuercen el uso de TLS e IRM en correos y documentos, además de aplicar reglas de cifrado automático en casos específicos (ej. envío de datos personales o financieros).
- Viabilidad organizacional: Actualmente no existe una política formal que obligue al cifrado en la transferencia de información, lo que genera variabilidad en el cumplimiento. El personal cuenta con conocimientos básicos sobre cómo aplicar el cifrado manualmente, pero no hay capacitaciones recurrentes ni procedimientos claros. Aquí, el control 6.3 cobra importancia, ya que las capacitaciones periódicas permitirían que los usuarios comprendan cuándo y cómo deben aplicar el cifrado en su trabajo diario. En términos organizativos, la viabilidad es alta siempre que se formalicen políticas y se brinde entrenamiento constante.
- Estrategia de adaptación: Se recomienda establecer una política corporativa que disponga el cifrado obligatorio en todas las transferencias de datos sensibles. A nivel técnico, deben configurarse reglas automáticas en el correo electrónico para detectar y cifrar información confidencial. Además, se sugiere realizar capacitaciones prácticas semestrales sobre cifrado de correos y archivos, acompañadas de auditorías aleatorias

para verificar cumplimiento. Estas medidas asegurarán que el cifrado no dependa únicamente de la acción manual del usuario, sino que forme parte del flujo operativo estándar de la organización.

Resultados octavo riesgo.

Riesgo: Planes de DRP/BCP sin pruebas integrales.
Controles propuestos: 5.29, 5.30, 8.16.

- Viabilidad técnica: Auxadi ya dispone de respaldos en la nube y redundancia básica en su infraestructura, lo que permite cumplir parcialmente con los controles 5.29 y 5.30. Sin embargo, no existe un esquema sistemático para realizar simulacros integrales que involucren a todas las áreas. Técnicamente, es posible ejecutar pruebas de continuidad con los sistemas actuales, pero se requiere definir indicadores como RTO y RPO, así como mecanismos para documentar y supervisar los resultados, lo cual estaría cubierto con el control adicional 8.16.
- Viabilidad organizacional: La organización tiene experiencia en la recuperación de incidentes menores, pero no cuenta con procesos formalizados para coordinar simulacros de continuidad a nivel global. Esto limita la capacidad de respuesta en escenarios críticos. El personal de TI está capacitado para ejecutar pruebas técnicas, pero se necesita involucrar a otras áreas de la empresa y designar responsables que garanticen la coordinación y documentación. La viabilidad organizacional depende de que la alta dirección impulse y respalde estas actividades.
- Estrategia de adaptación: Para adaptar estos controles al contexto de Auxadi, se recomienda establecer un cronograma anual de pruebas integrales de DRP/BCP, con participación de todas las áreas clave. Los resultados deben documentarse y analizarse, generando indicadores de recuperación que permitan identificar brechas y oportunidades de mejora. Asimismo, debe implementarse un sistema de supervisión que registre la ejecución y efectividad de los simulacros, asegurando la trazabilidad de las acciones realizadas. Con estas medidas, la empresa fortalecerá su capacidad de resiliencia frente a interrupciones mayores.

Resultados noveno riesgo.

Riesgo: Protección insuficiente de datos personales.
Controles propuestos: 5.12, 5.33, 5.34, 6.6.

- Viabilidad técnica: Auxadi ya maneja datos personales en sistemas corporativos como correo, ERP y repositorios en la nube, los cuales cuentan con funciones de clasificación y protección que pueden ser aprovechadas para cumplir con los controles 5.12 y 5.34. Sin embargo, no existe un inventario consolidado de datos personales ni un esquema unificado de clasificación, lo que limita la aplicación práctica. El control 5.33 es técnicamente viable mediante la centralización de registros y copias seguras, mientras que los acuerdos de confidencialidad (6.6) requieren un soporte documental más riguroso que no implica barreras tecnológicas.
- Viabilidad organizacional: Actualmente, la empresa cuenta con políticas de protección de datos, pero no están acompañadas de procesos estandarizados para su actualización ni de un inventario actualizado de PII. Además, no todos los contratos laborales y de proveedores incluyen cláusulas explícitas de confidencialidad, lo que genera un vacío organizativo. El personal de TI y administrativo está preparado para apoyar en la custodia de datos, pero es necesario mayor involucramiento del área legal y de recursos humanos para garantizar cumplimiento normativo.
- Estrategia de adaptación: Para viabilizar la aplicación de estos controles, se recomienda consolidar un inventario actualizado de todos los datos personales procesados por la organización, clasificarlos según sensibilidad y aplicar medidas específicas de protección. Adicionalmente, se debe estandarizar el uso de formularios de consentimiento, incluir acuerdos de confidencialidad en todos los contratos laborales y con terceros, y establecer auditorías internas periódicas que revisen la custodia y tratamiento de la información personal. Estas acciones aseguran tanto el cumplimiento de la Ley 8968 en Costa Rica como de los lineamientos de la ISO 27001.

Resultados décimo riesgo.

Riesgo: Gestión documental dispersa.
Controles propuestos: 5.33, 5.37, 8.16.

- Viabilidad técnica: Auxadi ya utiliza plataformas como OneDrive y SharePoint para almacenar y compartir información, lo que facilita aplicar los controles 5.33 y 5.37. Sin embargo, la ausencia de una política corporativa unificada y de un repositorio único genera dispersión y dificulta el control. El control 8.16 es técnicamente viable mediante la creación de reportes automáticos y auditorías periódicas de accesos y modificaciones en los documentos. Las capacidades tecnológicas están presentes, pero requieren ser organizadas bajo un marco común de gestión.
- Viabilidad organizacional: Actualmente, cada área maneja sus propios registros con criterios distintos, lo que reduce la trazabilidad y aumenta el riesgo de inconsistencias. El personal de TI y administrativo puede dar soporte a la consolidación de documentos, pero sin reglas claras de clasificación y sin responsables definidos, es difícil garantizar la protección y actualización de la información. La viabilidad organizacional es media, dependiendo de la definición de responsabilidades y del compromiso de todas las áreas para adoptar un esquema centralizado.
- Estrategia de adaptación: Para aplicar estos controles de manera efectiva, se recomienda establecer una política única de gestión documental, consolidar todos los registros en un repositorio centralizado con permisos segmentados y asignar responsables de custodia y actualización. Además, se deben programar auditorías periódicas de cumplimiento y generar reportes que aseguren la trazabilidad de accesos y cambios. Con estas medidas, se podrá reducir la dispersión documental, mejorar la eficiencia en la gestión de la información y garantizar que los registros sean íntegros y accesibles en todo momento.

Resultados undécimo riesgo.

Riesgo: Capacitación insuficiente en seguridad.

Controles propuestos: 6.3, 6.8.

- Viabilidad técnica: Auxadi dispone de herramientas tecnológicas que facilitan la capacitación, como plataformas de e-learning, correo corporativo y espacios de reunión virtual. Estas herramientas permiten implementar el control 6.3 (concienciación y capacitación) sin necesidad de realizar inversiones significativas. El control 6.8 (informes de eventos de seguridad) también es técnicamente viable, pues los sistemas actuales ya generan registros que pueden usarse en actividades formativas. El reto radica en estructurar un programa continuo que use estas herramientas de manera consistente.
- Viabilidad organizacional: La empresa cuenta con personal dispuesto a recibir formación, pero actualmente las capacitaciones son esporádicas y no se mide su efectividad. Para lograr resultados sostenibles, se requiere un plan semestral que establezca temas, frecuencia y responsables. Asimismo, es necesario integrar las capacitaciones con métricas de participación y evaluaciones breves que aseguren la comprensión del contenido. La viabilidad organizacional es alta, siempre que exista compromiso por parte de la gerencia para formalizar y dar seguimiento al programa.
- Estrategia de adaptación: Se recomienda implementar un plan semestral de capacitación en seguridad de la información, incluyendo temas clave como phishing, contraseñas, uso seguro de dispositivos y protección de datos personales. Cada sesión debe ir acompañada de evaluaciones cortas para medir su efectividad, y complementarse con simulaciones de incidentes que refuercen el aprendizaje práctico. Además, los informes de eventos (6.8) pueden usarse como insumo real para discutir fallos y buenas prácticas, integrando el aprendizaje con la realidad de la empresa. Estas medidas fortalecerán la cultura de seguridad y reducirán la vulnerabilidad asociada al factor humano.

Resultados duodécimo riesgo.

Riesgo: BYOD sin controles específicos.
Controles propuestos: 5.10, 8.1, 5.14.

- Viabilidad técnica: Auxadi cuenta con Microsoft Intune y funciones de MDM (Mobile Device Management), lo que permite aplicar controles técnicos para la gestión de dispositivos personales (8.1) y garantizar que solo se utilicen canales seguros para la transferencia de información (5.14). Sin embargo, estas capacidades aún no han sido configuradas ni aplicadas al BYOD, por lo que existe un vacío en su uso. El control 5.10, referente al uso aceptable de activos, es técnicamente factible mediante configuraciones de seguridad y restricciones aplicadas en dispositivos, siempre que se acompañe de lineamientos claros.
- Viabilidad organizacional: Actualmente no existe una política formal de BYOD en Auxadi, lo que genera incertidumbre en el uso de dispositivos personales para tareas laborales. El personal de TI tiene el conocimiento técnico para implementar controles de seguridad, pero la organización necesita definir requisitos mínimos de protección (cifrado, antivirus, bloqueo automático) y comunicar estas reglas a los colaboradores. La viabilidad organizacional es alta, pero depende de la formalización de políticas y de la disposición de los usuarios para aceptar medidas de seguridad en sus dispositivos personales.
- Estrategia de adaptación: Para implementar de forma efectiva estos controles, se recomienda crear una política de BYOD que defina claramente los requisitos de seguridad y responsabilidades del usuario. Esta política debe incluir el uso de MDM para controlar accesos, habilitar el borrado remoto en caso de pérdida o salida del colaborador y restringir aplicaciones no autorizadas. Asimismo, se debe asegurar que toda transferencia de datos desde dispositivos personales se realice mediante canales cifrados y aprobados por la organización. Con estas medidas, se reducirá el riesgo de fuga de información y se garantizará un uso seguro de dispositivos personales en el entorno laboral.

Resultados décimo tercer riesgo.

Riesgo: Phishing e ingeniería social.
Controles propuestos: 6.3, 6.8, 8.16.

- Viabilidad técnica: Auxadi ya cuenta con infraestructura tecnológica que permite reforzar la capacitación y la gestión de reportes. El control 6.3 es viable a través de sesiones de concienciación y simulaciones de phishing utilizando herramientas disponibles en Microsoft 365. El control 6.8 también es aplicable, pues los sistemas corporativos permiten generar registros y reportes de incidentes de seguridad. El control adicional 8.16 es igualmente viable, dado que los sistemas de correo y seguridad ya generan logs que pueden centralizarse para supervisión continua.
- Viabilidad organizacional: El personal ha recibido capacitaciones básicas en seguridad, pero estas no son periódicas ni incluyen simulaciones prácticas. Además, los reportes de intentos de phishing se canalizan de manera informal, sin un procedimiento estandarizado. Organizacionalmente, la empresa tiene capacidad para implementar estos controles, siempre que se definan responsabilidades claras, se creen canales oficiales de reporte y se fomente la participación del personal en ejercicios de concienciación.
- Estrategia de adaptación: Para aplicar de forma efectiva estos controles, se recomienda establecer un programa semestral de simulaciones de phishing con métricas de participación y éxito. Asimismo, debe formalizarse un procedimiento para el reporte de intentos de ingeniería social, habilitando un canal dedicado (ej. correo o formulario interno). Los registros de incidentes deben ser monitoreados mediante el control 8.16 para generar estadísticas y retroalimentar el programa de capacitación. Con estas acciones, se fortalece la cultura de seguridad, se incrementa la resiliencia frente a amenazas sociales y se asegura trazabilidad en la gestión de incidentes.

Resultados décimo cuarto riesgo.

Riesgo: Políticas/procedimientos desactualizados.
Controles propuestos: 5.1, 5.36, 5.37.

- Viabilidad técnica: Auxadi ya dispone de un marco documental digital en plataformas como SharePoint, lo que permite aplicar los controles 5.1 y 5.36 para centralizar,

actualizar y dar seguimiento a las políticas de seguridad de la información. El control adicional 5.37 también es viable, ya que la herramienta permite versionar documentos y mantener procedimientos asociados a cada política. A nivel técnico, no se requieren inversiones adicionales significativas, sino un uso más disciplinado de las herramientas ya disponibles.

- Viabilidad organizacional: La empresa cuenta con políticas formales, pero no existe un cronograma definido para su revisión ni un comité encargado de supervisarlas. El personal administrativo y de TI tiene capacidad para actualizar documentos, pero sin procesos claros y responsabilidades asignadas, el riesgo de obsolescencia se mantiene. La viabilidad organizacional depende de que la dirección designe un comité de seguridad que coordine las revisiones anuales y asegure la actualización periódica de políticas y procedimientos.
- Estrategia de adaptación: Para lograr la aplicación de estos controles, se recomienda establecer un ciclo anual de revisión de políticas y procedimientos, con responsables formales de aprobación y documentación de cambios. Se debe mantener un historial de versiones para garantizar trazabilidad, y realizar auditorías internas que verifiquen el cumplimiento de las políticas actualizadas. Con estas medidas, Auxadi asegurará que su marco documental se mantenga vigente y alineado con los cambios regulatorios y tecnológicos, fortaleciendo la gobernanza en seguridad de la información.

Resultados décimo quinto riesgo.

Riesgo: Monitoreo y registro de accesos/cambios insuficiente.
Controles propuestos: 5.2, 8.15, 8.16, 5.25.

- Viabilidad técnica: Auxadi ya cuenta con registros en Active Directory y en algunos sistemas críticos, lo que permite implementar los controles 8.15 y 8.16. Sin embargo, estos registros no se consolidan en una herramienta única de monitoreo, lo que dificulta su análisis y seguimiento. El control 5.2 es técnicamente viable, pues la infraestructura ya permite definir roles y responsabilidades. El control adicional 5.25 puede aplicarse mediante auditorías externas o revisiones internas independientes. La capacidad técnica

está presente, pero requiere reforzarse con la integración de un sistema SIEM o equivalente para consolidar los logs y generar alertas automáticas.

- Viabilidad organizacional: Actualmente, la revisión de accesos y cambios se realiza de manera puntual y reactiva, sin procesos estandarizados ni responsables formales. Esto reduce la trazabilidad y la capacidad de detección temprana. La organización tiene personal capacitado para llevar a cabo revisiones periódicas, pero es necesario designar roles claros y establecer procedimientos documentados para garantizar consistencia. La viabilidad organizacional depende de la asignación de responsabilidades y del compromiso de la dirección para implementar auditorías regulares.
- Estrategia de adaptación: Para aplicar estos controles de forma efectiva, se recomienda consolidar los registros en una plataforma centralizada (ej. SIEM), definir alertas automáticas para accesos indebidos o cambios críticos, y asignar responsables para revisiones periódicas. Asimismo, se debe complementar con revisiones independientes bajo el control 5.25, que garanticen objetividad y transparencia en el proceso. Con estas medidas, Auxadi podrá mejorar la trazabilidad de accesos y cambios, detectar incidentes de manera temprana y fortalecer su postura de seguridad.

Resultados décimo sexto riesgo.

Riesgo: Ausencia de sanciones formales.
Controles propuestos: 6.4, 5.36.

- Viabilidad técnica: Este riesgo no requiere infraestructura tecnológica compleja para su mitigación. Los controles 6.4 y 5.36 son plenamente aplicables mediante la actualización de documentos internos como el reglamento de trabajo y las políticas de seguridad de la información. Desde el punto de vista técnico, basta con contar con sistemas de gestión documental ya existentes (SharePoint, OneDrive) para almacenar y difundir las políticas, lo que asegura que estén accesibles y actualizadas para todo el personal.
- Viabilidad organizacional: Actualmente, Auxadi cuenta con un reglamento interno general, pero este no incluye sanciones específicas relacionadas con incumplimientos

de seguridad de la información. El personal de TI y de recursos humanos puede implementar este ajuste, pero se requiere la aprobación de la gerencia y la coordinación con el área legal para formalizar un marco disciplinario que sea proporcional y aplicable. La viabilidad organizacional es alta, ya que no requiere recursos adicionales, solo compromiso institucional y claridad en la ejecución.

- Estrategia de adaptación: Se recomienda actualizar el reglamento interno para incluir sanciones graduadas (advertencia, suspensión, despido) según la gravedad de la falta en materia de seguridad de la información. Además, estas sanciones deben estar vinculadas al cumplimiento de políticas documentadas (control 5.36), asegurando consistencia en su aplicación. El proceso debe complementarse con sesiones de comunicación y capacitación para que todos los colaboradores conozcan las consecuencias de incumplir las normas. Con estas acciones, la empresa fortalecerá la cultura de cumplimiento y reducirá la tolerancia a prácticas inseguras.

Resultados décimo séptimo riesgo.

Riesgo: Fallas de disponibilidad en servicios críticos.
Controles propuestos: 5.30, 8.14, 5.29.

- Viabilidad técnica: Auxadi ya cuenta con respaldos en la nube y servidores con redundancia, lo que facilita la aplicación de los controles 5.30 y 8.14. Sin embargo, aún no existe un procedimiento documentado que contemple pruebas periódicas de continuidad. El control adicional 5.29 es técnicamente viable mediante la integración de medidas de seguridad durante las interrupciones, como protocolos de recuperación segura y comunicación inmediata. La infraestructura actual permite implementar estas acciones sin necesidad de grandes inversiones, aunque requiere mayor formalización y disciplina en la ejecución.
- Viabilidad organizacional: La organización reconoce la importancia de la continuidad de servicios críticos como el correo corporativo, ERP y bases de datos, pero las pruebas integrales no se realizan de manera sistemática. El personal de TI tiene la capacidad técnica para llevarlas a cabo, aunque se necesita designar responsables claros y

establecer un cronograma obligatorio de simulacros. La viabilidad organizacional es alta, pero depende del compromiso de la gerencia para integrar estas prácticas dentro de las rutinas de control operativo.

- Estrategia de adaptación: Se recomienda documentar procedimientos de continuidad con tiempos de recuperación definidos (RTO y RPO), realizar al menos una prueba integral anual con participación de todas las áreas y definir métricas de disponibilidad que permitan medir la efectividad de las acciones. Además, deben establecerse protocolos de seguridad durante las interrupciones (5.29), asegurando la protección de datos y accesos mientras los sistemas están fuera de servicio. Con estas medidas, Auxadi podrá fortalecer su resiliencia y garantizar la continuidad de sus operaciones críticas frente a incidentes.

Resultados décimo octavo riesgo.

Riesgo: Cobertura limitada de riesgos en nube/teletrabajo.
Controles propuestos: 5.23, 6.7, 8.24.

- Viabilidad técnica: Auxadi utiliza servicios en la nube como Microsoft 365 y tiene experiencia en entornos de teletrabajo, lo que permite aplicar los controles 5.23 y 6.7 de forma práctica. Sin embargo, aún no existen configuraciones estandarizadas ni cláusulas contractuales específicas con proveedores que aseguren el cumplimiento de requisitos de seguridad. El control adicional 8.24 es técnicamente viable, ya que los sistemas corporativos permiten habilitar cifrado en conexiones remotas (VPN, TLS, IRM), aunque requiere ajustes de configuración y capacitación al personal.
- Viabilidad organizacional: El teletrabajo y el uso de la nube ya forman parte de las operaciones de Auxadi, pero las prácticas actuales no están formalizadas en políticas internas. El personal está habituado al trabajo remoto, pero sin lineamientos claros persisten inconsistencias en la aplicación de medidas de seguridad. Organizacionalmente, la viabilidad es alta siempre que se documenten reglas de teletrabajo, se comuniquen responsabilidades a los colaboradores y se incluya a los proveedores de nube en la gestión de seguridad.

- Estrategia de adaptación: Se recomienda crear una política formal de teletrabajo que establezca requisitos mínimos de seguridad en dispositivos, accesos y conexiones. Además, se deben incluir cláusulas específicas en los contratos con proveedores de nube para garantizar la protección de datos. El control 8.24 debe aplicarse configurando cifrado obligatorio en comunicaciones remotas y estableciendo monitoreo de accesos externos. Con estas acciones, Auxadi podrá fortalecer su postura de seguridad frente a riesgos derivados de la nube y el teletrabajo, alineando sus operaciones con buenas prácticas internacionales.

Resultados décimo noveno riesgo.

Riesgo: Software sin actualizaciones verificadas.
Controles propuestos: 8.8, 8.9, 8.16.

- Viabilidad técnica: Actualmente, Auxadi aplica actualizaciones manuales en algunos sistemas, lo que genera retrasos y posibles ventanas de vulnerabilidad. El control 8.8 es viable mediante la implementación de un proceso formal de gestión de vulnerabilidades que identifique, evalúe y priorice parches. El control 8.9 puede aplicarse a través de configuraciones seguras y procedimientos estandarizados de instalación. El control adicional 8.16 resulta igualmente viable, ya que permite integrar supervisión continua y validación de actualizaciones mediante registros automáticos o reportes de cumplimiento. Para ello, la empresa podría aprovechar soluciones de Microsoft o adquirir una herramienta centralizada de gestión de parches.
- Viabilidad organizacional: El personal de TI tiene la capacidad para gestionar actualizaciones, pero sin procesos documentados ni responsabilidades claras, la práctica se mantiene inconsistente. Además, la ausencia de métricas dificulta medir la efectividad de las actualizaciones. Organizacionalmente, la viabilidad depende de establecer roles formales para la gestión de parches y definir un calendario de aplicación obligatoria. Aunque implica un esfuerzo inicial de organización, no requiere grandes inversiones, más bien disciplina y control interno.

- Estrategia de adaptación: Para hacer efectivos estos controles, se recomienda implementar una herramienta de gestión de parches centralizada que consolide las actualizaciones de todos los sistemas. Asimismo, se debe definir un calendario de actualizaciones críticas, documentar los cambios aplicados para asegurar trazabilidad y habilitar métricas de cumplimiento supervisadas mediante el control 8.16. Con estas medidas, Auxadi podrá reducir las brechas de seguridad, minimizar el riesgo de explotación de vulnerabilidades y asegurar configuraciones consistentes en toda su infraestructura.

Resultados vigésimo riesgo.

Riesgo: Incidentes menores sin registro sistemático.
Controles propuestos: 5.27, 6.8, 8.16.

- Viabilidad técnica: Auxadi ya dispone de sistemas de Service Desk que podrían usarse para registrar incidentes de seguridad, pero en la práctica solo se documentan los de mayor impacto. Los controles 5.27 y 6.8 son técnicamente viables mediante la implementación de un flujo sencillo de tickets o formularios internos que permitan registrar todos los incidentes, incluso los menores. El control adicional 8.16 es aplicable al permitir la supervisión periódica de estos reportes y la generación de métricas. La capacidad técnica existe, aunque se requiere configurar el sistema para incluir categorías específicas de seguridad y entrenar al personal en su uso.
- Viabilidad organizacional: Actualmente no existe un proceso formal para registrar incidentes menores, lo que genera pérdida de trazabilidad y oportunidades de mejora. El personal de TI tiene la disposición para supervisar registros, pero se requiere compromiso institucional para que todos los colaboradores comprendan la importancia de reportar cualquier incidente, sin importar su magnitud. La viabilidad organizacional es alta, siempre que se comunique la política de reporte y se integren responsabilidades claras en las rutinas de trabajo.
- Estrategia de adaptación: Para aplicar estos controles, se recomienda establecer un procedimiento formal de registro de incidentes menores dentro del sistema de tickets

ya disponible. Esto debe incluir capacitaciones breves al personal sobre cómo y por qué reportar eventos aparentemente pequeños, además de generar reportes trimestrales que identifiquen tendencias y oportunidades de mejora. La supervisión mediante el control 8.16 permitirá validar que todos los incidentes sean revisados y tratados oportunamente. Con estas medidas, Auxadi podrá fortalecer su capacidad de aprendizaje organizacional y consolidar una cultura de mejora continua en seguridad de la información.

Propuesta de Políticas y Procedimientos de Seguridad para la Gestión de Dispositivos, Comunicación y Protección de Datos

La propuesta de políticas y procedimientos de seguridad de la información constituye la fase de consolidación del trabajo analítico y técnico realizado a lo largo del proyecto. Su desarrollo se basa directamente en los resultados obtenidos durante el diagnóstico inicial, la identificación y clasificación de riesgos, la selección de controles bajo la norma ISO/IEC 27001:2022 y la validación conjunta con el equipo de Tecnologías de la Información (TI) de Auxadi Costa Rica. Este proceso metodológico permitió que cada riesgo identificado se vinculara con controles específicos y posteriormente se tradujera en lineamientos prácticos y aplicables al contexto operativo de la organización.

La elaboración de esta estructura fue respaldada por un proceso de revisión documental, entrevistas y listas de verificación que sirvieron para evaluar el grado de cumplimiento de la empresa frente a las exigencias normativas, técnicas y organizacionales. Dichos instrumentos fueron aplicados de manera complementaria con el fin de reforzar la validez del análisis y garantizar que las políticas propuestas respondan a condiciones reales observadas en los procesos críticos. De este modo, se logró integrar tanto la perspectiva técnica de seguridad como la visión administrativa y regulatoria de la gestión de la información.

En la propuesta participan diversas áreas funcionales que aseguran su implementación y mantenimiento efectivo. El Departamento de TI asume la responsabilidad técnica sobre la administración de accesos, la gestión de dispositivos, los respaldos, la protección de la red y el

monitoreo centralizado de eventos. El área de Cumplimiento y Protección de Datos supervisa la aplicación de la Ley 8968 de Protección de Datos Personales en Costa Rica, evalúa el cumplimiento contractual con terceros y coordina auditorías de control interno y externo. Talento Humano colabora en la gestión de altas, bajas y cambios de roles, garantizando que las credenciales, autorizaciones y capacitaciones en materia de seguridad se mantengan actualizadas. Finalmente, la Gerencia de Operaciones funge como órgano decisor y asegura que las medidas implementadas estén alineadas con los planes de continuidad de negocio (BCP) y de recuperación ante desastres (DRP), fortaleciendo la resiliencia institucional.

Algunos de estos roles ya forman parte de la estructura organizativa existente, mientras que otros, como la función formal de Cumplimiento, se consolidan como una propuesta dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo establecer trazabilidad, responsabilidad y mejora continua. En conjunto, esta estructura refuerza el principio de defensa en profundidad, combinando controles técnicos, administrativos y humanos para garantizar la confidencialidad, integridad y disponibilidad de la información.

La propuesta se compone de tres políticas principales y sus respectivos procedimientos de aplicación, diseñados para cubrir las áreas más críticas detectadas en el diagnóstico de seguridad:

- Política de gestión de dispositivos y accesos corporativos.
    - Procedimiento de gestión de identidades, credenciales y accesos (IAM).
    - Procedimiento de gestión segura de dispositivos y BYOD.
    - Procedimiento de acceso remoto seguro.
- Política de seguridad en la comunicación corporativa.
    - Procedimiento de uso seguro de correo y documentos.
    - Procedimiento de protección frente a amenazas en comunicaciones.
- Política de protección de datos y continuidad de la información.
    - Procedimiento de copias de seguridad y continuidad del negocio.
    - Procedimiento de gestión de información, incidentes y cumplimiento.

En su conjunto, estas políticas representan un marco integral que combina los hallazgos del diagnóstico con la normativa internacional, estableciendo bases sólidas para una gestión

preventiva, estandarizada y medible de la seguridad de la información. Su diseño complementa las políticas institucionales ya existentes, reforzando su efectividad sin generar contradicciones, y aportando lineamientos concretos que fortalecen la madurez del sistema de gestión.

De forma complementaria, la siguiente tabla resume la correlación entre los riesgos identificados, los controles de la norma ISO/IEC 27001:2022 que los abordan y los procedimientos en los que cada uno se materializa dentro de la propuesta. Esta relación asegura coherencia entre el análisis inicial, la validación técnica realizada con el equipo TI y las medidas documentadas en la estructura final de políticas y procedimientos.

Tabla 8

Tabla de riesgos – controles – procedimientos.

Nº	Riesgo identificado	Controles ISO/IEC 27001:2022	Procedimiento en propuesta
1	Pérdida de dispositivos sin respaldo ni cifrado	7.3 Uso aceptable de activos 7.8 Eliminación de la información 8.13 Protección de datos en reposo 8.1 Gestión de configuración 6.3 Responsabilidades de seguridad de la información	1.2 Procedimiento de gestión segura de dispositivos y BYOD 3.1 Procedimiento de copias de seguridad y continuidad del negocio
2	Uso compartido de credenciales o cuentas	5.15 Identificación de requisitos de acceso 5.18 Gestión de derechos de acceso de usuarios 8.5 Gestión de autenticación 8.16 Supervisión de actividades	1.1 Procedimiento de gestión de identidades, credenciales y accesos (IAM)
3	Filtración de datos por error humano	5.14 Políticas para el uso de la información 6.3 Responsabilidades de seguridad de la información 8.24 Uso de criptografía	2.1 Procedimiento de uso seguro de correo y documentos
4	Accesos sin control en carpetas/sistemas críticos	5.18 Gestión de derechos de acceso de usuarios 8.3 Restricción de acceso a la información 8.16 Supervisión de actividades	1.1 Procedimiento de gestión de identidades, credenciales y accesos (IAM)
5	Uso inconsistente de contraseñas robustas	8.5 Gestión de autenticación 5.17 Segregación de funciones 6.3 Responsabilidades de seguridad de la información	1.1 Procedimiento de gestión de identidades, credenciales y accesos (IAM)
6	Falta de MFA en accesos críticos	8.5 Gestión de autenticación 8.16 Supervisión de actividades	1.1 Procedimiento de gestión de identidades, credenciales y accesos (IAM)

			1.3 Procedimiento de acceso remoto seguro
7	Transmisión de información sin cifrado	5.14 Políticas para el uso de la información 8.24 Uso de criptografía 6.3 Responsabilidades de seguridad de la información	2.1 Procedimiento de uso seguro de correo y documentos
8	DRP/BCP sin pruebas integrales	5.29 Planificación de continuidad 5.30 Pruebas de continuidad 8.16 Supervisión de actividades	3.1 Procedimiento de copias de seguridad y continuidad del negocio
9	Protección insuficiente de datos personales	5.12 Clasificación de la información 5.34 Cumplimiento de requisitos legales y contractuales 6.6 Acuerdos de confidencialidad	3.2 Procedimiento de gestión de información, incidentes y cumplimiento
10	Gestión documental dispersa	5.33 Gestión de la documentación 5.37 Retención de registros 8.16 Supervisión de actividades	3.2 Procedimiento de gestión de información, incidentes y cumplimiento
11	Capacitación insuficiente en seguridad	6.3 Responsabilidades de seguridad de la información 6.8 Concienciación, educación y formación	2.2 Procedimiento de protección frente a amenazas en comunicaciones 3.2 Procedimiento de gestión de información, incidentes y cumplimiento
12	BYOD sin controles específicos	5.10 Uso aceptable de los activos 8.1 Gestión de configuración 5.14 Políticas para el uso de la información	1.2 Procedimiento de gestión segura de dispositivos y BYOD
13	Phishing e ingeniería social	6.3 Responsabilidades de seguridad de la Información 6.8 Concienciación, educación y formación 8.16 Supervisión de actividades	2.2 Procedimiento de protección frente a amenazas en comunicaciones
14	Políticas/procedimientos desactualizados	5.1 Liderazgo y compromise 5.36 Revisión de políticas 5.37 Retención de registros	3.2 Procedimiento de gestión de información, incidentes y cumplimiento
15	Monitoreo insuficiente de accesos/cambios	5.2 Responsabilidades de la dirección 8.15 Registros de actividades 8.16 Supervisión de actividades 5.25 Contacto con autoridades	1.1 Procedimiento de gestión de identidades, credenciales y accesos (IAM) 3.2 Procedimiento de gestión de información, incidentes y cumplimiento
16	Ausencia de sanciones formales	6.4 Responsabilidades disciplinarias 5.36 Revisión de políticas	3.2 Procedimiento de gestión de información, incidentes y cumplimiento
17	Fallas de disponibilidad en servicios críticos	5.30 Pruebas de continuidad 8.14 Protección de servicios críticos 5.29 Planificación de continuidad	3.1 Procedimiento de copias de seguridad y continuidad del negocio
18	Cobertura limitada en nube/teletrabajo	5.23 Seguridad en servicios en la nube 6.7 Responsabilidades de terceros	1.3 Procedimiento de acceso remoto seguro

		8.24 Uso de criptografía	3.2 Procedimiento de gestión de información, incidentes y cumplimiento
19	Software sin actualizaciones verificadas	8.8 Gestión de vulnerabilidades técnicas 8.9 Instalación de software 8.16 Supervisión de actividades	1.2 Procedimiento de gestión segura de dispositivos y BYOD 3.2 Procedimiento de gestión de información, incidentes y cumplimiento
20	Incidentes menores sin registro sistemático	5.27 Notificación de eventos 6.8 Concienciación y formación 8.16 Supervisión de actividades	3.2 Procedimiento de gestión de información, incidentes y cumplimiento

Fuente: Elaboración propia

Política de Gestión y Control Seguro de Dispositivos

Objetivo.

Establecer lineamientos unificados para la administración, custodia y control de los dispositivos que acceden a la información corporativa de Auxadi Costa Rica. Esta política tiene como fin reducir los riesgos identificados en el diagnóstico, tales como la pérdida de equipos sin cifrado, el uso compartido de credenciales, la ausencia de autenticación multifactor en accesos críticos y las configuraciones inseguras. Asimismo, busca reforzar las medidas de seguridad ya implementadas en la organización, como el uso de MFA, el cifrado de discos con BitLocker, la protección mediante antivirus/EDR y el acceso remoto seguro a través de SSL VPN con auditoría. La política se fundamenta en la norma ISO/IEC 27001:2022, en los hallazgos de la matriz de riesgos y en las políticas vigentes de Auxadi, incluyendo la gestión de contraseñas con caducidad, el bloqueo por inactividad y los controles de cifrado de datos.

Alcance.

La política aplica a todos los colaboradores, contratistas y terceros que utilicen dispositivos para acceder a los sistemas, aplicaciones y servicios de Auxadi Costa Rica, ya sea en modalidad presencial o remota. Se incluyen laptops, computadoras de escritorio, teléfonos móviles, tabletas y dispositivos personales autorizados bajo el esquema Bring Your Own Device (BYOD). Quedan

excluidos los dispositivos no registrados en el inventario de TI o que incumplan con los requisitos mínimos de seguridad definidos por la organización.

Directrices.

Accesos e identidades.

- La creación, modificación o revocación de cuentas deberá gestionarse únicamente mediante notificación formal de Talento Humano.
- El área de TI será responsable de aprovisionar en Active Directory, sincronizar con Azure/O365, habilitar MFA y configurar el acceso a VPN y aplicaciones de acuerdo con el rol definido.
- Se prohíbe el uso de cuentas compartidas. Los permisos se asignarán bajo el principio de mínimo privilegio y, en funciones críticas, aplicando segregación de roles.

Protección del endpoint (corporativo y BYOD).

- Todos los dispositivos deberán contar con cifrado de disco completo (BitLocker/AES-256), antivirus/EDR corporativo, bloqueo automático tras inactividad y enrolamiento en MDM/Intune.
- Los dispositivos BYOD deberán cumplir los mismos requisitos y aceptar la posibilidad de borrado remoto en caso de pérdida, robo o desvinculación.
- Se prohíbe instalar software no autorizado y almacenar información sensible en nubes personales o medios no cifrados.

Actualización y configuración segura.

- Los dispositivos estarán sujetos a parches de seguridad periódicos y configuraciones de hardening bajo supervisión de TI.
- Las excepciones requerirán aprobación formal, documentación de justificación y fecha límite de corrección.

Acceso remoto seguro.

- El acceso remoto deberá realizarse exclusivamente a través de la VPN corporativa, con cifrado robusto, MFA habilitado y registro de auditoría.
- Se bloquearán automáticamente conexiones provenientes de dispositivos no conformes, ubicaciones no autorizadas o equipos sin enrolamiento en MDM.

Custodia física y continuidad.

- Los colaboradores son responsables de la custodia física de los equipos mediante candados, lockers o almacenamiento en áreas seguras.
- En escenarios de contingencia, se aplicarán las medidas definidas en el Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP).
- Los proveedores externos que administren o custodien equipos deberán demostrar cumplimiento mediante cláusulas contractuales de seguridad equivalentes.

Cumplimiento de contraseñas y MFA.

- Los parámetros mínimos corporativos son: contraseñas complejas, caducidad a 90 días, no reutilización de las últimas 24, bloqueo por inactividad y habilitación obligatoria de MFA.
- Los accesos privilegiados deberán contar con MFA reforzado y el uso obligatorio del gestor corporativo de credenciales.

Monitoreo, métricas y coordinación con incidentes.

- El área de TI implementará monitoreo centralizado (MDM/SIEM o equivalente) y consolidará reportes trimestrales de cumplimiento, midiendo indicadores como:
    - % de dispositivos cifrados.
    - % de dispositivos actualizados con parches críticos.

    - % de cuentas con MFA habilitado.
- Número de incidentes relacionados con accesos indebidos o pérdida de equipos.
- La revisión de cuentas privilegiadas será trimestral como medida de refuerzo.
- Los incidentes detectados serán gestionados según el procedimiento vigente de gestión de incidentes, con clasificación, escalado y medidas correctivas.

Revisión y actualización.

Esta política será revisada anualmente o de forma extraordinaria si se producen cambios relevantes en la infraestructura tecnológica, nuevas exigencias regulatorias o hallazgos en auditorías internas/externas. El área de TI coordinará la actualización en conjunto con Cumplimiento y Talento Humano, asegurando la documentación, la comunicación oportuna y la capacitación al personal sobre los cambios introducidos.

Procedimiento de gestión de identidades, credenciales y accesos (IAM).

Objetivo.

Definir controles formales para la administración integral del ciclo de vida de las identidades digitales y credenciales en Auxadi Costa Rica. Este procedimiento garantiza que los accesos a los sistemas corporativos se otorguen, gestionen y revoquen de manera controlada, trazable y alineada a las funciones asignadas. Con ello se busca mitigar riesgos críticos detectados en el diagnóstico, tales como el uso compartido de cuentas, la asignación indebida de privilegios, la ausencia de autenticación multifactor (MFA) en accesos críticos y la falta de revisiones periódicas. El procedimiento se fundamenta en la norma ISO/IEC 27001:2022, en la Política de gestión de contraseñas de Auxadi y en el procedimiento oficial de altas, bajas y modificaciones de usuarios.

Alcance.

Este procedimiento aplica a todos los colaboradores, contratistas y terceros que requieran acceso a sistemas, aplicaciones y servicios corporativos de Auxadi Costa Rica. Cubre los siguientes entornos:

- Active Directory (AD) y Azure AD.
- Office 365 (correo electrónico, Teams, OneDrive y SharePoint).
- Aplicaciones críticas (ERP, sistemas contables y de gestión).
- Infraestructura de red, VPN y entornos en la nube.

El ciclo de vida de la identidad inicia con la solicitud de acceso y finaliza con la revocación tras la desvinculación laboral o contractual.

Lineamientos y reglas de seguridad.

Solicitud, asignación y revocación de accesos.

- Toda solicitud deberá originarse en notificación formal de Talento Humano o del área usuaria autorizada.
- TI será responsable de ejecutar el aprovisionamiento en AD, la sincronización con Azure/O365, la habilitación de MFA y la asignación de permisos según el rol definido.
- La revocación de accesos deberá realizarse de inmediato ante desvinculación, cambio de funciones o incidentes de seguridad.
- Cada gestión quedará documentada en la mesa de servicio, vinculada a un ticket y con evidencia de cumplimiento.

Credenciales únicas y mínimo privilegio.

- Cada usuario tendrá credenciales individuales; las cuentas compartidas están estrictamente prohibidas.
- Los accesos se asignarán bajo el principio de mínimo privilegio y, en funciones críticas, aplicando segregación de roles para prevenir fraudes o abusos.

- Las cuentas de servicio deberán estar justificadas, documentadas y sujetas a controles adicionales de monitoreo.

Políticas de contraseñas y gestor corporativo.

- Se aplican los parámetros mínimos establecidos: longitud, complejidad, caducidad a 90 días, bloqueo por inactividad y no reutilización de las últimas 24 contraseñas.
- El almacenamiento de credenciales se permitirá únicamente en el gestor corporativo autorizado.
- Para cuentas administrativas y de servicio, el uso del gestor es obligatorio, con acceso restringido a perfiles designados de TI.

Autenticación multifactor (MFA).

- MFA será obligatoria en accesos a sistemas críticos (AD, VPN, Office 365, ERP y entornos en la nube).
- TI verificará periódicamente la activación de MFA en todas las cuentas y consolidará reportes de cumplimiento y desviaciones.

Revisión y auditoría de privilegios.

- Se realizará una revisión semestral de accesos generales y una revisión trimestral de cuentas privilegiadas.
- Hallazgos como cuentas inactivas, privilegios excesivos o accesos indebidos deberán corregirse de inmediato.
- Los resultados serán integrados en auditorías internas y externas como evidencia de cumplimiento del SGSI.

Registros y trazabilidad.

- Todas las altas, bajas y modificaciones quedarán registradas en la mesa de servicio y en las bitácoras automáticas de los sistemas involucrados.
- Los registros deberán conservarse por un período mínimo de tres años, como evidencia para auditorías, revisiones regulatorias y análisis de incidentes.

Revisión y actualización.

Este procedimiento será revisado de forma anual o anticipada si se producen incidentes relevantes, cambios tecnológicos significativos o modificaciones normativas. La responsabilidad recaerá en TI, en coordinación con Talento Humano (para garantizar la baja oportuna de usuarios) y Cumplimiento (para validar alineación con la normativa legal y de protección de datos).

Procedimiento de gestión Segura de dispositivos y BYOD.

Objetivo.

Establecer controles técnicos y administrativos que aseguren que todos los dispositivos que acceden a la infraestructura de Auxadi Costa Rica, ya sean corporativos o personales bajo modalidad BYOD, cumplan con requisitos de seguridad homogéneos y verificables. Este procedimiento busca reducir riesgos priorizados en el diagnóstico, tales como la pérdida de equipos sin cifrado, propagación de malware, uso de software no autorizado, custodia deficiente y accesos desde dispositivos no registrados. La propuesta se fundamenta en los controles de la norma ISO/IEC 27001:2022, en el Plan de Continuidad de Negocio (BCP), en el Plan de Recuperación ante Desastres (DRP), y en las políticas internas de protección de datos y seguridad corporativa vigentes.

Alcance.

El procedimiento aplica a:

- Laptops, estaciones de trabajo y servidores.
- Dispositivos móviles, tabletas y periféricos conectados a la red corporativa.

- Equipos de red y almacenamiento gestionados por TI.
- Dispositivos personales (BYOD) previamente autorizados bajo acuerdo formal.

Abarca el ciclo de vida completo: registro, configuración inicial, uso operativo, monitoreo continuo, custodia física y disposición final de los equipos.

Lineamientos y reglas de seguridad.

Requisitos mínimos de Seguridad.

- Todo dispositivo deberá contar con cifrado completo de disco (BitLocker/AES-256), antivirus o EDR corporativo activo, bloqueo automático por inactividad y enrolamiento en MDM/Intune.
- Los dispositivos BYOD podrán conectarse únicamente si cumplen con los mismos estándares y tras la firma del acuerdo BYOD, que incluye autorización de borrado remoto en caso de pérdida, robo o desvinculación.

Registro y autorización de equipos.

- Ningún dispositivo podrá conectarse a la red sin estar previamente registrado en el inventario central de TI.
- La autorización de BYOD será válida por un año, renovable tras verificación de cumplimiento.
- Los equipos no autorizados serán bloqueados automáticamente por políticas de seguridad de red.

Uso aceptable de dispositivos.

- Los equipos deben emplearse exclusivamente para fines laborales y mediante aplicaciones autorizadas.

- Se prohíbe la instalación de software no corporativo, el uso de redes públicas sin VPN y el almacenamiento de datos sensibles en nubes personales o medios externos no cifrados.
- El incumplimiento podrá derivar en la suspensión del dispositivo del inventario y sanciones disciplinarias.

Gestión de parches y hardening.

- Los dispositivos estarán sujetos a actualizaciones periódicas de parches críticos y configuraciones de hardening (deshabilitación de servicios innecesarios, reforzamiento de firewall, protocolos seguros).
- TI será responsable de mantener evidencia documentada de todas las actualizaciones aplicadas.

Custodia física de equipos.

- Los colaboradores deberán custodiar sus equipos mediante candados de seguridad, lockers o almacenamiento en áreas restringidas.
- Queda prohibido dejar equipos en vehículos o lugares públicos sin supervisión.
- En caso de pérdida o robo, el incidente deberá reportarse de inmediato a TI, quien ejecutará el borrado remoto y notificará a Cumplimiento.

Monitoreo y métricas de cumplimiento.

- TI mantendrá monitoreo centralizado (MDM/SIEM) validando el estado de cifrado, antivirus, parches, BYOD y VPN.
- Se generarán reportes trimestrales que incluirán, al menos:
    - % de dispositivos cifrados.
    - % de dispositivos con parches críticos aplicados.
    - % de cuentas con MFA activo en endpoints.
    - Número de incidentes por accesos indebidos o pérdidas reportadas.

- Los hallazgos deberán integrarse en las revisiones de BCP y DRP, fortaleciendo la resiliencia de los procesos críticos.

Disposición final de equipos.

- Los equipos corporativos al finalizar su vida útil o tras la desvinculación del colaborador deberán entregarse a TI para borrado seguro de la información y desasignación del inventario.
- Los dispositivos BYOD quedarán desvinculados de los sistemas corporativos, eliminando todo acceso y configuración aplicada.

Registros y trazabilidad.

- Todas las altas, bajas y modificaciones de dispositivos, incluyendo BYOD, deberán documentarse en la mesa de servicio, con evidencia de autorización, configuración y nivel de cumplimiento.
- Los registros deberán conservarse por un período mínimo de 12 meses, considerando la posible extensión a 3 años para auditorías ISO, regulatorias y de cumplimiento.

Revisión y actualización.

El procedimiento será revisado anualmente o antes si ocurren:

- Incidentes graves relacionados con dispositivos.
- Incorporación de nuevas tecnologías o cambios normativos relevantes.
- Hallazgos de auditorías internas o externas.

La revisión estará a cargo de TI, en coordinación con Cumplimiento y la Gerencia de Operaciones, asegurando que las actualizaciones se integren a los planes de continuidad (BCP/DRP) y a las políticas generales de seguridad de Auxadi Costa Rica.

Procedimiento de acceso remoto seguro

Objetivo.

Garantizar que los accesos remotos a los sistemas y servicios de Auxadi Costa Rica se realicen de manera controlada, segura y conforme a los estándares internacionales de seguridad de la información. El procedimiento tiene como fin mitigar riesgos como accesos no autorizados, intrusiones, robo de credenciales, fuga de información y pérdida de disponibilidad en escenarios de teletrabajo o conexiones externas. Se fundamenta en los controles de la norma ISO/IEC 27001:2022, en los hallazgos de la matriz de riesgos y en las medidas vigentes en la organización (uso de SSL VPN, autenticación multifactor y auditoría de sesiones).

Alcance.

Aplica a colaboradores, contratistas y terceros autorizados que requieran conectarse de manera remota a los sistemas corporativos de Auxadi Costa Rica. Incluye accesos a:

- Aplicaciones críticas (ERP, M365, correo electrónico, bases de datos).
- Servidores on-premise y carpetas compartidas.
- Entornos en la nube integrados a la operación corporativa.

Lineamientos y reglas de seguridad.

Uso exclusivo de VPN corporativa.

- Todo acceso remoto deberá realizarse únicamente a través de la VPN corporativa gestionada por TI, configurada con cifrado robusto (ej. AES-256) y autenticación segura.
- La VPN deberá registrar de forma automática todas las conexiones establecidas, generando evidencia de trazabilidad y auditoría.
- Se prohíbe estrictamente el acceso a sistemas corporativos desde redes abiertas o sin el uso de la VPN.

Autenticación multifactor (MFA).

- MFA será obligatoria para todos los accesos remotos, combinando credenciales corporativas con un segundo factor (token, aplicación móvil o clave dinámica).
- TI será responsable de configurar y verificar la aplicación de MFA, consolidando reportes periódicos de cumplimiento y desviaciones detectadas.

Restricciones de dispositivos y ubicaciones.

- Solo se permitirá la conexión desde dispositivos previamente registrados en el inventario de TI y que cumplan con las políticas de seguridad (cifrado activo, antivirus actualizado, parches al día y enrolamiento en MDM).
- Los intentos de conexión desde equipos no autorizados o ubicaciones geográficas no habituales serán bloqueados automáticamente.
- Los accesos desde dispositivos personales (BYOD) estarán sujetos a los mismos controles de seguridad que los equipos corporativos.

Monitoreo y registro de sesiones.

- Todas las conexiones remotas quedarán registradas en bitácoras centralizadas, analizadas mediante la plataforma de monitoreo (SIEM o equivalente).
- Se generarán alertas automáticas ante comportamientos inusuales, tales como: múltiples intentos fallidos de inicio de sesión, accesos en horarios no laborales, conexiones simultáneas desde diferentes ubicaciones o transferencias de datos atípicas.
- Los hallazgos deberán integrarse en los reportes trimestrales de seguridad de TI.

Gestión de incidentes.

- Cualquier anomalía detectada será tratada según el procedimiento de gestión de incidentes vigente, que contempla bloqueo preventivo de cuentas, análisis de causa raíz, aplicación de medidas correctivas y comunicación inmediata a Cumplimiento.
- Las lecciones aprendidas se documentarán y se integrarán en revisiones posteriores de este procedimiento.

Registros y trazabilidad.

- TI será responsable de mantener registros actualizados de accesos remotos, dispositivos autorizados y evidencias de cumplimiento de MFA y VPN.
- Dichos registros deberán conservarse por un mínimo de doce meses y estarán disponibles para auditorías internas, externas y regulatorias.

Revisión y actualización.

Este procedimiento será revisado de forma anual o antes si ocurren cambios tecnológicos relevantes, incidentes graves o modificaciones normativas. La revisión estará a cargo de TI, en coordinación con Cumplimiento y el área de Continuidad de Negocio, asegurando su integración con el BCP y el DRP de Auxadi Costa Rica.

Política de Seguridad en la Comunicación Corporativa

Objetivo.

Definir lineamientos claros para proteger la información en tránsito y durante la colaboración interna y externa de Auxadi Costa Rica, reduciendo riesgos priorizados en el diagnóstico: transmisión sin cifrado, filtración por error humano, intentos de phishing e ingeniería social, uso de canales no autorizados y exposición indebida en compartición externa. La política se fundamenta en la norma ISO/IEC 27001:2022, en los controles validados con TI y en las estrategias de adopción de seguridad. A su vez, se integra con el marco normativo y organizacional

vigente: Protección de Datos, Código Ético, Planes de Continuidad (BCP/DRP), Gestión de Incidentes y Política de Contraseñas.

Alcance.

Aplicable a todos los colaboradores, contratistas y terceros que utilicen canales corporativos para el envío, recepción o intercambio de información de Auxadi Costa Rica. Comprende:

- Correo electrónico corporativo (M365/Exchange Online).
- Teams, chat, SharePoint, OneDrive y portales ERP.
- Servicios de colaboración en la nube integrados a la operación.

Quedan excluidos los canales personales (correos privados, mensajería instantánea, nubes externas), cuyo uso para fines corporativos está prohibido, salvo autorización documentada y validada por Cumplimiento y TI.

Directrices.

Canales autorizados y uso aceptable.

- El correo corporativo, Teams, SharePoint/OneDrive y aplicaciones aprobadas por TI son los únicos medios permitidos para comunicaciones de trabajo.
- Se prohíbe el uso de WhatsApp, Telegram, correos privados o plataformas públicas para intercambio de información corporativa.
- La información sensible debe compartirse preferiblemente mediante enlaces seguros en SharePoint/OneDrive, con permisos mínimos y caducidad, en lugar de adjuntos.

Cifrado y protección de la información en tránsito.

- Todo correo externo utilizará TLS forzado; la información sensible (PII, nómina, contratos, credenciales, datos financieros) deberá protegerse con cifrado/IRM (Sensitivity Labels, OME).
- Se aplicarán reglas automáticas (DLP/transport rules) para detectar y cifrar envíos con datos sensibles. Las excepciones requerirán aprobación formal y registro.
- Los correos salientes que incluyan datos clasificados deberán contener avisos de confidencialidad.

Gestión segura de documentos y compartición externa (M365).

- Todo almacenamiento deberá realizarse en SharePoint/OneDrive con control de versionado, registros y políticas de retención. Se prohíbe almacenar datos sensibles en unidades locales o medios no cifrados.
- La compartición externa deberá configurarse con enlaces restringidos a destinatarios específicos, caducidad definida, permisos de solo lectura por defecto, watermark cuando corresponda y revisiones periódicas.
- Los accesos externos se revisarán mensualmente para eliminar enlaces innecesarios.

Protecciones de correo y dominios.

- TI deberá garantizar la configuración y mantenimiento de SPF, DKIM y DMARC.
- Se mantendrán activos los controles antispam/antimalware y análisis de adjuntos/enlaces (Safe Links/Attachments o equivalente).
- Los correos sospechosos pasarán a cuarentena y contarán con flujo de aprobación; se conservarán bitácoras y message trace para auditoría.

Concienciación, simulaciones y reporte.

- Se realizarán campañas semestrales de concienciación sobre phishing, cifrado, clasificación y manejo seguro de adjuntos.

- Se aplicarán simulaciones de phishing con métricas de desempeño (clic, reporte y tiempo de respuesta). Las lecciones aprendidas ajustarán reglas DLP/IRM.
- Los usuarios contarán con un canal formal para reportar incidentes (p. ej., botón "Report phishing" o correo phishing@auxadi), con SLA de respuesta definido.

Roles y responsabilidades.

- TI: Configuración de M365 (TLS, IRM, DLP, ATP), dominios (SPF, DKIM, DMARC), telemetría, bitácoras y soporte.
- Cumplimiento/Protección de Datos: Definición de categorías de datos sensibles, revisión de excepciones y cláusulas con terceros.
- Dueños de proceso: Clasificación de información y validación de destinatarios/permisos mínimos.
- Usuarios: Uso exclusivo de canales autorizados, cifrado de información sensible, verificación de destinatarios y reporte de correos sospechosos.

Monitoreo, métricas y auditoría.

- Los eventos (envíos cifrados, bloqueos DLP, enlaces externos, reportes de phishing) se consolidarán en el SIEM.
- Métricas mínimas trimestrales: % de envíos cifrados, incidentes DLP por área, tasa de clic vs. reporte en simulaciones, tiempos de contención y accesos externos activos.
- Se realizará una revisión anual independiente (interna o externa) del cumplimiento de esta política.

Integración con otras políticas y procedimientos.

- IAM: credenciales únicas, MFA y mínimo privilegio como base para accesos.
- Endpoints/BYOD y Acceso remoto: seguridad del dispositivo y VPN/MFA como prerrequisitos para comunicaciones seguras.

- Gobernanza e incidentes: clasificación de datos, cláusulas de confidencialidad y gestión de incidentes.
- BCP/DRP: continuidad de correo y canales críticos en escenarios de recuperación.

Revisión y actualización.

La política será revisada anualmente o antes si ocurren cambios tecnológicos en M365/DLP/IRM, incidentes relevantes, modificaciones legales (incluyendo ajustes a la Ley 8968 en Costa Rica) o hallazgos de auditoría. TI será responsable de coordinar la actualización en conjunto con Cumplimiento y Talento Humano, asegurando la capacitación del personal y la trazabilidad de cambios mediante gestión documental formal.

Procedimiento de uso seguro de correo y documentos.

Objetivo.

Definir controles formales que aseguren que las comunicaciones electrónicas y la compartición de documentos en Auxadi Costa Rica se realicen de forma segura, confiable y conforme a la clasificación de la información corporativa. El procedimiento busca mitigar riesgos como la transmisión de datos sensibles sin cifrado, el uso de canales no autorizados, la exposición en repositorios no seguros y la falta de trazabilidad en las auditorías de cumplimiento.

Alcance.

Este procedimiento aplica a todos los colaboradores, contratistas y terceros que utilicen correo electrónico corporativo (M365/Exchange Online), Teams, SharePoint y OneDrive para el intercambio y almacenamiento de información. Incluye:

- Envío de correos electrónicos.
- Compartición de archivos y enlaces.
- Almacenamiento en repositorios corporativos.
- Uso de etiquetas de seguridad y clasificación (IRM/Sensitivity Labels).

El uso de correos personales, mensajería instantánea no autorizada o nubes externas para fines laborales queda estrictamente prohibido.

Lineamientos y reglas de seguridad.

Canales autorizados y cifrado en transferencias.

- El correo corporativo y los repositorios de M365 son los únicos canales permitidos para comunicaciones laborales.
- Todo correo o documento que contenga información clasificada como sensible (datos financieros, PII, nómina, contratos, credenciales o información de clientes) deberá transmitirse con cifrado obligatorio mediante las herramientas corporativas (Office Message Encryption, Sensitivity Labels o equivalente).
- El cifrado TLS forzado estará activo por defecto en todas las transferencias externas de correo electrónico.

Configuración predeterminada de seguridad en M365.

- Se aplicarán reglas automáticas de prevención de pérdida de datos (DLP) para identificar información sensible en correos y documentos, aplicando acciones como cifrado, bloqueo o notificación al remitente.
- El uso de IRM (Information Rights Management) y etiquetas de clasificación será obligatorio para documentos sensibles.
- Todo archivo compartido externamente desde SharePoint u OneDrive deberá configurarse con enlaces restringidos a destinatarios específicos, permisos mínimos (solo lectura por defecto) y fecha de caducidad definida.

Almacenamiento seguro en repositorios corporativos.

- Los documentos deberán almacenarse únicamente en repositorios autorizados (SharePoint y OneDrive), con versionado activo y registro de actividad habilitado.
- Se prohíbe almacenar información en unidades locales sin cifrado, en dispositivos personales no registrados o en nubes externas.
- Los permisos en carpetas compartidas deberán revisarse de forma periódica para eliminar accesos innecesarios.

Auditorías y control de cumplimiento.

- El área de TI consolidará en el SIEM o plataforma equivalente los eventos relacionados con cifrado, bloqueos DLP y accesos externos.
- Se generarán reportes trimestrales con métricas clave:
    - Porcentaje de correos cifrados con datos sensibles.
    - Número de incidentes DLP detectados.
    - Cantidad de enlaces externos activos y su caducidad.
- Las desviaciones detectadas serán notificadas a Cumplimiento e integradas en el procedimiento de Gestión de Incidentes.

Registros y trazabilidad.

- Todos los eventos relacionados con correos cifrados, bloqueos automáticos, compartición de documentos y auditorías de accesos quedarán registrados en la mesa de servicio y en las bitácoras de M365.
- Estas evidencias servirán como insumo para auditorías internas, externas y revisiones regulatorias.

Revisión y actualización.

El procedimiento será revisado anualmente o antes si se presentan incidentes graves de filtración de datos, cambios relevantes en la infraestructura de M365, actualizaciones normativas (p. ej., Ley 8968 en Costa Rica) o hallazgos de auditoría. TI será responsable de liderar la revisión,

en coordinación con Cumplimiento y Protección de Datos, garantizando que los cambios sean comunicados y que el personal reciba capacitación adecuada sobre las modificaciones implementadas.

Procedimiento de protección frente a amenazas en comunicaciones.

Objetivo.

Establecer controles técnicos, organizativos y de concienciación que protejan a Auxadi Costa Rica frente a amenazas en el correo electrónico y otros canales de comunicación corporativa. Este procedimiento busca reducir riesgos como phishing, spam, malware, enlaces maliciosos, ingeniería social y uso indebido de credenciales, reforzando los controles de la norma ISO/IEC 27001:2022 y las políticas de seguridad vigentes.

Alcance.

Aplica a todos los colaboradores, contratistas y terceros que utilicen correo electrónico (Exchange Online/M365), Teams, SharePoint y demás canales corporativos para fines laborales. Incluye la recepción de mensajes externos y la gestión de amenazas internas, como el envío indebido de información, el uso de macros maliciosas o el manejo inadecuado de adjuntos sospechosos.

Lineamientos y reglas de seguridad.

Filtros de correo y protección técnica.

- Se habilitarán de manera obligatoria filtros antispam y antimalware gestionados centralmente, con análisis en tiempo real de adjuntos y enlaces.
- TI mantendrá configuradas y monitoreadas las medidas de autenticación de dominios (SPF, DKIM y DMARC) para reducir la suplantación de identidad.

- Los correos sospechosos o con adjuntos bloqueados serán redirigidos automáticamente a cuarentena, con notificación inmediata al usuario.

Campañas de concienciación y simulaciones de phishing.

- Se realizarán campañas de concienciación semestrales enfocadas en amenazas de ingeniería social, aplicables a todo el personal.
- Cumplimiento y TI coordinarán simulaciones de phishing para evaluar indicadores como tasa de clics, tasa de reportes oportunos y tiempo de reacción.
- Los resultados se utilizarán para ajustar la capacitación, priorizando las áreas de mayor exposición (ejemplo: finanzas, contabilidad, TI)

Canal formal de reporte de incidentes.

- Se establece un canal único para reportar mensajes sospechosos (ejemplo: buzón phishing@auxadi.com o botón “Report phishing” en Outlook).
- Todo usuario tiene la obligación de reportar de inmediato intentos de phishing, correos con enlaces dudosos o adjuntos maliciosos.
- TI será responsable de analizar el reporte, contener el incidente y documentar las acciones tomadas en la mesa de servicio.

Auditoría y métricas de efectividad.

- TI generará métricas trimestrales que incluirán, al menos:
    - Número de correos maliciosos bloqueados por filtros.
    - Tasa de clics en simulaciones de phishing.
    - Tiempo promedio de reporte y contención de incidentes.
- Los resultados se presentarán en auditorías internas y se integrarán a los planes de mejora continua del SGSI.

Registros y trazabilidad.

- Todos los eventos de bloqueo (SPF, DKIM, DMARC, antispam, antimalware) quedarán registrados en la consola de M365 y en el SIEM corporativo.
- Los reportes de simulaciones de phishing, métricas de capacitación y resultados de incidentes deberán conservarse como evidencia documental durante al menos 24 meses.

Revisión y actualización.

Este procedimiento será revisado de manera anual o antes si se detectan nuevas campañas de ataque, cambios tecnológicos en la plataforma de correo o incidentes significativos de phishing o malware. La revisión estará a cargo del área de TI, en coordinación con Cumplimiento y Protección de Datos, garantizando que se actualicen las medidas técnicas y que el personal reciba capacitación sobre las mejoras implementadas.

Política de Protección de Datos y Continuidad de la Información

Objetivo.

Definir lineamientos claros para salvaguardar la información corporativa de Auxadi Costa Rica en condiciones normales de operación y en escenarios de contingencia. Esta política busca garantizar la confidencialidad, integridad, disponibilidad y cumplimiento normativo de los datos, mitigando riesgos identificados en el diagnóstico: pérdida de información crítica, clasificación inadecuada, incumplimiento de la Ley 8968 de Protección de Datos Personales y ausencia de planes de continuidad y recuperación (BCP/DRP) robustos. La política se fundamenta en la norma ISO/IEC 27001:2022, en la matriz de riesgos y en los procedimientos vigentes relacionados con respaldos, gestión de incidentes y planes de contingencia.

Alcance.

La política aplica a colaboradores, contratistas y terceros que manejen, procesen o custodien información de Auxadi, incluyendo:

- Datos personales y sensibles de clientes, proveedores y colaboradores (PII).
- Información financiera, contractual, contable y de nómina.
- Documentación estratégica y operativa.
- Sistemas y aplicaciones críticas, tanto en entornos on-premise como en la nube.

Quedan excluidos los datos ajenos a la operación corporativa o almacenados en dispositivos personales no autorizados.

Directrices.

Gobernanza de la información.

- La información deberá clasificarse según niveles de sensibilidad: pública, interna, confidencial y restringida.
- Todo repositorio corporativo deberá contar con control de versiones, registros de auditoría y políticas de retención.
- El ciclo de vida de la información incluirá: creación, uso, almacenamiento seguro, revisión anual y disposición final mediante borrado seguro o destrucción controlada.

Protección de datos personales y confidencialidad.

- El tratamiento de PII cumplirá con la Ley 8968 y normativa internacional aplicable.
- Los datos personales deberán cifrarse en tránsito y en reposo, y su acceso estará condicionado al uso de MFA.
- La recolección de datos estará sujeta a consentimiento informado y a acuerdos de confidencialidad para colaboradores y terceros.

Continuidad del negocio y copias de seguridad.

- Se implementarán respaldos automáticos cifrados, con pruebas de restauración periódicas documentadas.
- El BCP y DRP deberán contemplar RTO (Recovery Time Objective) y RPO (Recovery Point Objective) definidos según la criticidad del sistema o servicio.
- Se realizarán simulacros integrales de continuidad y recuperación al menos una vez al año, incluyendo escenarios de ciberataques, fallas técnicas y desastres naturales.

Gestión de incidentes y cumplimiento.

- Todo incidente que involucre pérdida, alteración, acceso indebido o fuga de datos deberá ser reportado de inmediato por el canal oficial.
- Los incidentes se clasificarán en menores o críticos, aplicando el ciclo de gestión: contención, análisis de causa raíz, medidas correctivas y documentación de lecciones aprendidas.
- El incumplimiento de esta política podrá derivar en sanciones disciplinarias internas o contractuales en el caso de terceros.

Seguridad en contratos de nube y proveedores.

- Los contratos con proveedores de servicios tecnológicos deberán incluir cláusulas de confidencialidad, protección de datos, seguridad y auditoría.
- Proveedores de servicios críticos deberán demostrar la existencia de planes equivalentes de BCP/DRP, con evidencias de cumplimiento.

Monitoreo y métricas de cumplimiento.

- TI y Cumplimiento consolidarán métricas en el SIEM o plataforma equivalente sobre respaldos, auditorías de acceso a PII, incidentes y simulacros de continuidad.
- Se generarán reportes trimestrales y revisiones independientes anuales para evaluar la efectividad de las medidas implementadas.

Revisión y actualización.

La política será revisada de forma anual o extraordinaria en caso de incidentes críticos, cambios tecnológicos relevantes (ejemplo: migraciones a la nube), exigencias regulatorias o hallazgos de auditoría. La actualización estará a cargo de TI, en coordinación con Cumplimiento, Protección de Datos y la Gerencia de Operaciones, asegurando la capacitación del personal y la comunicación oportuna de los cambios.

Procedimiento de copias de seguridad y continuidad del negocio.

Objetivo.

Garantizar la protección, disponibilidad y recuperación de la información crítica de Auxadi Costa Rica mediante la implementación de copias de seguridad cifradas, planes de continuidad (BCP) y planes de recuperación ante desastres (DRP). Este procedimiento busca mitigar riesgos priorizados como pérdida de datos, fallos en la restauración, interrupciones prolongadas de servicios y falta de pruebas de resiliencia, asegurando la continuidad operativa del negocio.

Alcance.

Este procedimiento aplica a:

- Bases de datos, sistemas contables y ERP.
- Archivos y repositorios corporativos en SharePoint/OneDrive.
- Servidores on-premise y máquinas virtuales.
- Correo electrónico y servicios en la nube (M365).
- Documentación crítica almacenada en repositorios internos.

Abarca entornos de producción y de contingencia, en los que se requiera garantizar la resiliencia operativa.

Lineamientos y reglas de seguridad.

Respaldos automáticos y cifrado.

- Las copias de seguridad deberán ejecutarse de forma automática y programada: diarias para datos críticos y semanales para información de menor sensibilidad.
- Todos los respaldos deberán cifrarse con algoritmos robustos (AES-256 o equivalente), tanto en tránsito como en reposo.
- Los respaldos deberán almacenarse en al menos dos ubicaciones distintas: almacenamiento local seguro y nube corporativa autorizada.

Pruebas de restauración.

- Se realizarán pruebas de restauración trimestrales para verificar la integridad y disponibilidad de los respaldos.
- Cada prueba deberá documentar: tiempo de restauración, éxito o fallo, y desviaciones respecto a los RTO/RPO definidos.
- Los resultados se reportarán a Cumplimiento y se conservarán como evidencia en auditorías internas y externas.

Plan de continuidad (BCP) y recuperación (DRP).

- El BCP contemplará medidas de teletrabajo, acceso remoto seguro y continuidad de servicios críticos en escenarios de contingencia.
- El DRP incluirá protocolos para fallos tecnológicos, ciberataques, desastres naturales y otros eventos disruptivos.
- Los tiempos objetivos de recuperación (RTO) y puntos de recuperación (RPO) se definirán según la criticidad de cada sistema y se revisarán anualmente.
- Se realizarán simulacros integrales de BCP/DRP al menos una vez por año, involucrando tanto áreas técnicas como de negocio.

Seguridad durante interrupciones críticas.

- En caso de incidentes mayores, TI activará el DRP según lo documentado y coordinará la comunicación con las áreas afectadas.
- El acceso a respaldos en contingencia quedará restringido al personal de TI autorizado.
- Todas las acciones deberán registrarse en la mesa de servicio para garantizar trazabilidad y análisis posterior.

Registros y trazabilidad.

- Todas las copias de seguridad, pruebas de restauración y simulacros deberán documentarse en informes oficiales.
- Los registros incluirán fecha, responsable, resultado y observaciones, almacenándose en repositorios de auditoría y la mesa de servicio.
- TI consolidará reportes trimestrales de cumplimiento en el SIEM o herramienta equivalente para monitoreo centralizado.

Revisión y actualización.

Este procedimiento será revisado anualmente o antes si ocurren:

- Incidentes de pérdida de datos o fallos en restauración.
- Cambios tecnológicos relevantes (migración de nube, actualización de infraestructura).
- Hallazgos en auditorías internas o externas.

La revisión estará a cargo de TI, en coordinación con Cumplimiento y la Gerencia de Operaciones, asegurando que los mecanismos de respaldo y continuidad permanezcan alineados con las necesidades del negocio y los marcos normativos aplicables.

Procedimiento de gestión de información, incidentes y cumplimiento.

Objetivo.

Establecer lineamientos claros para la clasificación, protección y gestión del ciclo de vida de la información en Auxadi Costa Rica, así como para la detección, reporte y tratamiento de incidentes de seguridad. El propósito es garantizar el cumplimiento normativo —incluyendo la Ley 8968 de Protección de Datos Personales—, reforzar la gobernanza documental y asegurar la trazabilidad de las acciones, reduciendo riesgos como filtración de datos, incumplimiento legal, uso inadecuado de información sensible y ausencia de respuesta efectiva ante incidentes.

Alcance.

Este procedimiento aplica a:

- Toda la información generada, procesada o almacenada en Auxadi Costa Rica, en formato físico o digital.
- Datos personales (PII), financieros, contractuales, credenciales, nómina y demás información clasificada como sensible o crítica.
- Colaboradores, contratistas y terceros que manejen información corporativa bajo contrato o acuerdo de confidencialidad.
- Proveedores de servicios tecnológicos o en la nube que procesen datos de Auxadi, sujetos a cláusulas contractuales de seguridad.

Lineamientos y reglas de seguridad.

Gobernanza documental y clasificación.

- La información corporativa se clasificará en categorías: pública, interna, confidencial y restringida, según criterios definidos por TI y Cumplimiento.
- Todo documento oficial deberá almacenarse en repositorios corporativos (SharePoint/OneDrive) con control de versiones, registro de auditoría y ciclo anual de revisión.

- Cada documento crítico deberá contar con un responsable designado que garantice su actualización y vigencia.

Gestión de datos personales y acuerdos de confidencialidad.

- El tratamiento de datos personales se realizará conforme a la Ley 8968 y políticas internas de Auxadi.
- Colaboradores, contratistas y proveedores con acceso a PII deberán firmar acuerdos de confidencialidad.
- Los contratos con proveedores tecnológicos o de nube deberán incluir cláusulas de privacidad, cifrado, protección de datos y auditoría de cumplimiento.

Gestión de incidentes de seguridad

- Los incidentes se clasificarán en menores (ej. intento de phishing bloqueado) y críticos (ej. fuga de datos, caída de sistemas clave).
- Todo usuario deberá reportar inmediatamente cualquier incidente a través de los canales oficiales (mesa de servicio o botón de reporte en Outlook).
- TI, en coordinación con Cumplimiento, será responsable de la contención, análisis de causa raíz, documentación de acciones correctivas y comunicación a las partes interesadas.
- Las lecciones aprendidas deberán incorporarse a las revisiones del SGSI, así como a los planes de BCP y DRP.

Monitoreo y auditorías.

- Se mantendrá monitoreo centralizado mediante SIEM o equivalente, consolidando eventos de acceso, filtración, incidentes DLP, reportes de phishing y métricas de respaldos.
- Se realizarán revisiones anuales independientes (internas o externas) para validar la efectividad de los controles.

- Cumplimiento consolidará un informe anual con métricas clave:
    - Número y tipo de incidentes reportados.
    - Tiempos promedio de detección y respuesta (MTTD/MTTR).
    - Nivel de cumplimiento en revisiones documentales y clasificación de información.

Proceso disciplinario y sanciones.

- El incumplimiento del procedimiento por parte de colaboradores estará sujeto a medidas disciplinarias conforme al Código Ético y legislación laboral de Costa Rica.
- En el caso de proveedores o terceros, se aplicarán sanciones contractuales, incluyendo suspensión o terminación del servicio en incumplimientos graves.

Registros y trazabilidad.

- Todos los reportes de incidentes, revisiones documentales, métricas de cumplimiento y auditorías deberán registrarse en la mesa de servicio y en los repositorios de Cumplimiento.
- Los registros deberán conservarse por un período mínimo de 3 años como evidencia para auditorías internas, externas o regulatorias.

Revisión y actualización.

El procedimiento será revisado de forma anual o antes si ocurren:

- Incidentes graves de fuga de información o incumplimiento legal.
- Cambios regulatorios en materia de protección de datos.
- Recomendaciones provenientes de auditorías internas o externas.

La responsabilidad de la revisión recaerá en Cumplimiento, en coordinación con TI y la Gerencia de Operaciones. Toda actualización deberá documentarse, comunicarse y acompañarse de la capacitación correspondiente al personal.

Informe de Costos y Recursos para Implementación

Objetivo del Informe

El objetivo de este informe es analizar los costos y recursos necesarios para la implementación de las políticas y procedimientos de seguridad de la información definidos en el proyecto, considerando los requerimientos tecnológicos, humanos y financieros asociados a cada control. Este análisis busca determinar la viabilidad económica y operativa de la propuesta, garantizando que las acciones planificadas sean sostenibles dentro de la capacidad estructural y presupuestaria de Auxadi Costa Rica, en concordancia con los principios de eficiencia y optimización establecidos en la norma ISO/IEC 27001:2022.

Alcance de la Revisión

La revisión abarcó la totalidad de las políticas y procedimientos propuestos para Auxadi Costa Rica. Se analizaron los requerimientos técnicos, humanos y financieros de cada uno, con base en entrevistas al equipo de Tecnologías de la Información y en la revisión de presupuestos y licencias corporativas vigentes. El estudio incluyó la identificación de costos reales, oportunidades de ahorro, estrategias de optimización y acciones formativas necesarias para garantizar la implementación efectiva de los controles, asegurando asi coherencia entre los recursos disponibles y la propuesta realizada.

Análisis de Requerimientos por Política y Procedimiento

Política de gestión y control seguro de dispositivos.

- Requerimientos tecnológicos: La correcta aplicación de esta política requiere una infraestructura robusta de administración centralizada de endpoints a través de Microsoft Intune (MDM), que permita controlar configuraciones, actualizaciones y cumplimiento de políticas de seguridad. Debe complementarse con mecanismos de

cifrado de disco completo mediante BitLocker con TPM 2.0 y soluciones de protección avanzada (EDR) con capacidad de telemetría para detectar anomalías en tiempo real. Adicionalmente, es fundamental mantener un canal de acceso remoto seguro mediante VPN SSL con autenticación multifactor (MFA), junto con un sistema de auditoría centralizada y herramientas de monitoreo (SIEM) que registren eventos y generen alertas preventivas.

- Requerimientos humanos: El cumplimiento de esta política implica una coordinación constante entre las áreas de TI, Talento Humano y Cumplimiento. El departamento de TI es responsable del aprovisionamiento, soporte y supervisión de dispositivos, asegurando la correcta aplicación de las configuraciones de seguridad. Talento Humano debe colaborar en la gestión de altas, bajas y modificaciones de usuarios, mientras Cumplimiento y Gerencia supervisan la adherencia a los lineamientos ISO/IEC 27001. Además, todos los usuarios deben recibir capacitaciones periódicas sobre custodia física, uso responsable y buenas prácticas en seguridad de la información.
- Requerimientos financieros: El presupuesto proyectado contempla las licencias MDM/Intune (ya incluidas en Microsoft 365 E3 o superior), la renovación del antivirus corporativo y mantenimiento de la VPN. También se considera la inversión en elementos de seguridad física como candados o lockers, junto con capacitaciones anuales. De ser necesario, podrían contemplarse costos menores asociados a la actualización de equipos que no cumplan con los requisitos de cifrado TPM 2.0.

Procedimiento de gestión de identidades, credenciales y accesos (IAM).

- Requerimientos tecnológicos: La gestión segura de identidades se sustenta en la integración entre Active Directory (AD) y Azure AD, permitiendo un control centralizado y sincronizado de usuarios y privilegios. El procedimiento exige la aplicación de MFA, uso de gestores corporativos de contraseñas, auditorías automáticas de accesos y reportes históricos generados desde la mesa de servicio o portales de seguridad. Estas herramientas permiten asegurar la trazabilidad de privilegios, detectar accesos indebidos y mantener evidencia digital de todos los movimientos.

- Requerimientos humanos: El área de TI debe administrar los accesos, privilegios y grupos de seguridad, mientras Talento Humano autoriza los cambios de personal. Cumplimiento se encarga de revisar las evidencias de auditoría y velar por la aplicación de las políticas de control de acceso. Se recomienda la designación de un responsable interno de IAM con competencias en ciberseguridad, encargado de documentar y coordinar las revisiones mensuales de privilegios.
- Requerimientos financieros: Los costos principales corresponden al mantenimiento del directorio activo, al uso del MFA (ya cubierto por Microsoft 365) y al posible licenciamiento de software complementario de gestión de contraseñas. También se debe considerar un presupuesto para la capacitación técnica del personal de TI en administración de identidades híbridas y automatización de procesos de auditoría mediante PowerShell o Microsoft Compliance Manager.

Procedimiento de gestión segura de dispositivos y BYOD.

- Requerimientos tecnológicos: Este procedimiento requiere el uso del sistema MDM/Intune para la gestión y control de dispositivos, el cifrado de discos con BitLocker, políticas de red bajo el esquema NAC (Network Access Control) y la integración con sistemas antivirus corporativos y SIEM para el monitoreo continuo. También debe habilitar funciones de borrado remoto y garantizar la inclusión de todos los dispositivos (corporativos o personales) en el inventario oficial de TI.
- Requerimientos humanos: El equipo de TI es responsable de validar configuraciones, ejecutar auditorías y mantener actualizado el inventario de dispositivos. Cumplimiento debe supervisar la aplicación de las políticas en el marco BYOD, gestionando los acuerdos formales con los colaboradores. La Gerencia aprueba las excepciones y asegura la coherencia entre los controles técnicos y las políticas internas.
- Requerimientos financieros: Los requerimientos económicos incluyen la ampliación de licencias MDM, campañas de sensibilización, y posible compra de certificados o tokens de seguridad para reforzar la autenticación. La mayoría de los costos pueden optimizarse aprovechando los servicios y licencias ya disponibles bajo Microsoft 365, minimizando la necesidad de nuevas inversiones.

Procedimiento de acceso remoto seguro.

- Requerimientos tecnológicos: El acceso remoto debe sustentarse en una VPN SSL corporativa con cifrado AES-256, autenticación multifactor (MFA) y un sistema de monitoreo de logs en tiempo real mediante SIEM. Se requiere la creación de listas de dispositivos autorizados, gestión de ubicaciones seguras y alertas automáticas que detecten patrones sospechosos de conexión o accesos no autorizados.
- Requerimientos humanos: El área de TI se encarga de la configuración y mantenimiento de la VPN, así como del análisis de eventos registrados. Cumplimiento revisa los reportes de seguridad y los informes de auditoría, garantizando la trazabilidad. Por su parte, los usuarios remotos deben firmar acuerdos de acceso seguro y participar en capacitaciones periódicas sobre buenas prácticas en teletrabajo protegido.
- Requerimientos financieros: Los costos se asocian al mantenimiento de la VPN, renovación de certificados digitales, soporte técnico y capacitaciones. En la práctica, la mayoría de los servicios se encuentran cubiertos bajo la infraestructura Microsoft 365, lo cual reduce la necesidad de inversiones adicionales significativas.

Política de seguridad en la comunicación corporativa.

- Requerimientos tecnológicos: Esta política depende del uso del centro de seguridad y cumplimiento de Microsoft 365 (Security & Compliance Center), con configuraciones de DLP, IRM, TLS forzado, autenticación SPF/DKIM/DMARC y protección avanzada ATP. Además, debe integrarse con el SIEM para obtener visibilidad centralizada y trazabilidad de incidentes.
- Requerimientos humanos: El departamento de TI configura las reglas de seguridad y dominios seguros, mientras Cumplimiento define categorías de datos sensibles y revisa excepciones. Los usuarios finales deben participar en programas de capacitación orientados al reconocimiento de intentos de phishing y uso correcto de canales de comunicación institucional.

- Requerimientos financieros: El costo se centra en la renovación de licencias Microsoft 365, campañas de concientización y mantenimiento de la plataforma de seguridad. No se prevén inversiones adicionales en infraestructura, ya que las herramientas están incluidas en los servicios en la nube corporativa.

Procedimiento de uso seguro de correo y documentos.

- Requerimientos tecnológicos: Este procedimiento exige la aplicación de cifrado TLS y OME, políticas DLP e IRM, y etiquetado de sensibilidad para clasificar documentos. La información debe almacenarse en SharePoint y OneDrive bajo control de versiones y con auditorías activas que aseguren la trazabilidad de cada acción.
- Requerimientos humanos: El área de TI mantiene las configuraciones técnicas, mientras Cumplimiento revisa los reportes de DLP y los incidentes detectados. Los usuarios son responsables de aplicar correctamente las etiquetas y el cifrado al manejar información sensible, recibiendo capacitación continua sobre seguridad documental y manejo responsable de la información.
- Requerimientos financieros: Los costos principales corresponden a capacitaciones y monitoreo de cumplimiento. De ser necesario, podrían ampliarse las licencias de Microsoft 365 para habilitar funciones avanzadas de IRM, aunque la mayoría de los recursos ya están disponibles en el entorno actual.

Procedimiento de protección frente a amenazas en comunicaciones.

- Requerimientos tecnológicos: Requiere filtros antispam y antimalware, autenticación SPF, DKIM y DMARC, junto con funciones avanzadas de protección como Safe Links y Safe Attachments en Microsoft Defender. Estas herramientas deben integrarse con el SIEM para correlacionar eventos y generar reportes consolidados de seguridad.
- Requerimientos humanos: El área de TI administra las configuraciones de protección, Cumplimiento realiza simulaciones de phishing y revisa la efectividad de las campañas, mientras los usuarios reportan correos o actividades sospechosas mediante los canales

establecidos. Este proceso refuerza la cultura de seguridad y la respuesta temprana ante incidentes.

- Requerimientos financieros: Los costos incluyen campañas semestrales de concienciación, licencias de simuladores de phishing (preferiblemente integradas en Microsoft Defender) y soporte técnico especializado. Estos requerimientos se cubren casi en su totalidad con las licencias corporativas existentes.

Política de protección de datos y continuidad de la información.

- Requerimientos tecnológicos: Incorpora infraestructura de respaldo automatizado local y en la nube, cifrado de datos en tránsito y reposo, y documentación de los planes BCP y DRP para garantizar la continuidad operativa. Además, los incidentes deben ser monitoreados mediante herramientas SIEM o equivalentes para asegurar la respuesta oportuna.
- Requerimientos humanos: El área de TI ejecuta los respaldos y pruebas de restauración, mientras Cumplimiento y el delegado de Protección de Datos verifican el cumplimiento de la Ley 8968 y las normativas ISO. La Gerencia supervisa la disponibilidad operativa y autoriza la ejecución de simulacros o ejercicios de recuperación.
- Requerimientos financieros: Se proyecta inversión en almacenamiento en nube, licencias de software de respaldo (Azure Backup), simulacros anuales y auditorías externas. Sin embargo, parte importante de la infraestructura ya se encuentra cubierta por los servicios de Microsoft 365 y Azure, lo que reduce costos adicionales.

Procedimiento de copias de seguridad y continuidad del negocio.

- Requerimientos tecnológicos: Requiere sistemas de respaldo automatizado mediante Azure Backup, almacenamiento redundante, cifrado de respaldos, y ejecución periódica de pruebas de restauración. El monitoreo de estos procesos debe integrarse con el SIEM para asegurar trazabilidad y alertas ante fallos o inconsistencias.
- Requerimientos humanos: El personal de TI ejecuta los respaldos, verifica su integridad y documenta los resultados. Cumplimiento valida la información registrada y Gerencia

aprueba la ejecución de simulacros anuales, garantizando la disponibilidad de los datos críticos ante cualquier contingencia.

- Requerimientos financieros: Incluye licencias de almacenamiento, software de respaldo, capacitación técnica del personal y simulacros de continuidad. Dado que Auxadi ya dispone de infraestructura en la nube, los costos operativos se mantienen dentro de un rango controlado.

Procedimiento de gestión de información, incidentes y cumplimiento.

- Requerimientos tecnológicos: Se requiere una plataforma SIEM consolidada para la detección de incidentes, integrando registros DLP, logs de la mesa de servicio y repositorios documentales con auditoría activa. Estas herramientas permiten mantener la trazabilidad de eventos y respaldar los procesos de cumplimiento ante auditorías internas o externas.
- Requerimientos humanos: Cumplimiento lidera la gestión de incidentes y aplica medidas correctivas, mientras TI realiza el análisis técnico y documenta las causas raíz. Talento Humano y Gerencia se involucran cuando los eventos derivan en sanciones o acciones formativas. Este enfoque colaborativo garantiza una respuesta integral y coordinada ante incidentes.
- Requerimientos financieros: Los costos se asocian a las licencias SIEM, mantenimiento de la mesa de servicio y auditorías externas. Dado que Auxadi ya cuenta con soluciones integradas en Microsoft 365, los gastos adicionales se limitan a la ampliación de funcionalidades de monitoreo y capacitación continua en análisis forense digital.

Tabla 9

Tabla de requerimientos por política y procedimiento.

Política / Procedimiento	Requerimientos Tecnológicos	Requerimientos Humanos	Requerimientos Financieros
Política de gestión y control seguro de dispositivos	MDM/Intune, BitLocker TPM 2.0, EDR, VPN SSL con MFA, SIEM.	TI (gestión y soporte), Cumplimiento y Gerencia (verificación), usuarios (capacitación anual).	Licencias incluidas en M365, mantenimiento VPN y capacitación técnica.
Procedimiento de gestión de	AD local + Azure AD, MFA, gestor de	TI (gestión de accesos), Cumplimiento (auditorías),	Licencias M365, software de contraseñas,

identidades, credenciales y accesos (IAM)	contraseñas, auditorías automáticas.	Talento Humano (autorizaciones).	capacitación IAM avanzada.
Procedimiento de gestión segura de dispositivos y BYOD	Intune (MDM), BitLocker, antivirus corporativo, NAC, SIEM.	TI (validaciones), Cumplimiento (supervisión), Gerencia (autorizaciones).	Ampliación licencias MDM, campañas de concienciación, almacenamiento seguro.
Procedimiento de acceso remoto seguro	VPN SSL AES-256, MFA, SIEM, alertas automáticas.	TI (monitoreo), Cumplimiento (auditorías), usuarios (acuerdos y formación).	Licencias M365, mantenimiento VPN y capacitaciones en teletrabajo seguro.
Política de seguridad en la comunicación corporativa	M365 Security & Compliance Center, DLP, IRM, SPF/DKIM/DMARC, ATP.	TI (configuraciones), Cumplimiento (revisión), usuarios (prevención de phishing).	Renovación licencias M365, capacitación y campañas internas.
Procedimiento de uso seguro de correo y documentos	TLS/OME, DLP, IRM, etiquetado de sensibilidad, SharePoint/OneDrive.	TI (gestión técnica), Cumplimiento (revisión), usuarios (aplicación de cifrado).	Licencias M365, capacitación y monitoreo de cumplimiento.
Procedimiento de protección frente a amenazas en comunicaciones	Filtros antispam/malware, SPF/DKIM/DMARC, Safe Links, SIEM.	TI (configuración), Cumplimiento (simulaciones), usuarios (reporte de incidentes).	Campañas semestrales y capacitación; licencias M365 cubren lo esencial.
Política de protección de datos y continuidad de la información	Respaldo automatizado, cifrado, BCP/DRP, SIEM.	TI (respaldos), Cumplimiento y DPO (revisión normativa), Gerencia (simulacros).	Almacenamiento en nube, licencias backup y auditorías externas.
Procedimiento de copias de seguridad y continuidad del negocio	Azure Backup, almacenamiento redundante, cifrado, pruebas trimestrales.	TI (ejecución), Cumplimiento (validación), Gerencia (autorización de simulacros).	Licencias de almacenamiento, software de backup, capacitación técnica.
Procedimiento de gestión de información, incidentes y cumplimiento	SIEM, DLP, mesa de servicio, repositorio con auditorías.	Cumplimiento (lidera), TI (análisis técnico), Gerencia (supervisión).	Licencias SIEM, mantenimiento Help Desk y auditorías anuales.

Fuente: Elaboración propia

Entrevista para Validación de Requerimientos por Política y Procedimiento

Con el propósito de confirmar la pertinencia de los controles de seguridad propuestos y asegurar que estos se adapten al contexto real de la organización, se desarrolló una sesión de análisis con el equipo de Tecnologías de la Información de Auxadi Costa Rica. La dinámica consistió en una entrevista grupal estructurada, en la que los participantes evaluaron los riesgos

identificados junto con los controles seleccionados para mitigarlos. Durante el ejercicio, se discutió la adecuación de cada medida, su viabilidad práctica con los recursos actuales y los ajustes necesarios para fortalecer su implementación. Este proceso permitió obtener una validación consensuada, enriquecida con observaciones técnicas y recomendaciones específicas, lo cual garantiza que los resultados reflejen tanto las buenas prácticas internacionales como la realidad operativa de la empresa. Se utilizó el Apéndice G. Guía de Entrevista 4.

Resultados política de gestión y control seguro de dispositivos.

Recursos tecnológicos: MDM/Intune, BitLocker TPM 2.0, EDR, VPN SSL con MFA, SIEM.

Recursos humanos: TI (gestión y soporte), Cumplimiento y Gerencia (verificación), usuarios (capacitación anual).

Recursos financieros: Licencias incluidas en M365, mantenimiento VPN y capacitación técnica.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: La empresa ya dispone de licencias Microsoft 365 E3 con Intune, BitLocker y MFA activos. El SIEM se gestiona mediante telemetría integrada y no se requiere inversión adicional. Solo se recomienda evaluar la ampliación de monitoreo con reportes automáticos en Power BI.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El equipo de TI cuenta con personal técnico suficiente, pero se recomienda reforzar la formación en administración de Intune y gestión avanzada de BitLocker. Cumplimiento requiere lineamientos adicionales para documentar revisiones periódicas.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Sí, se cubren con el presupuesto actual

No se identifican costos nuevos significativos, dado que las licencias y plataformas están incluidas en los contratos vigentes. Solo se prevé una inversión menor para capacitaciones técnicas y reposición gradual de equipos antiguos sin TPM 2.0.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: La política se considera técnicamente viable con la infraestructura actual. Los ajustes necesarios se limitan a fortalecer la capacitación técnica y formalizar revisiones documentales de cumplimiento, sin necesidad de inversiones significativas.

Resultados procedimiento de gestión de identidades, credenciales y accesos (IAM).

Recursos tecnológicos: AD local, Azure AD, MFA, gestor de contraseñas, auditorías automáticas.

Recursos humanos: TI (gestión de accesos), Cumplimiento (auditorías), Talento Humano (autorizaciones).

Recursos financieros: Licencias M365, software de contraseñas, capacitación IAM avanzada.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi Costa Rica cuenta con un entorno híbrido operativo entre AD y Azure AD totalmente sincronizado. El MFA está habilitado y en uso por todo el personal. Se recomienda únicamente fortalecer la automatización de reportes de accesos y privilegios mediante PowerShell o herramientas nativas de Microsoft 365 Compliance.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El equipo de TI dispone de experiencia práctica en administración de usuarios y MFA, sin embargo, se recomienda una capacitación formal sobre gestión de identidades híbridas y automatización de auditorías. Se sugiere designar oficialmente a un responsable IAM dentro del área de TI para reforzar la trazabilidad de cambios y autorizaciones.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Sí, se cubren con el presupuesto actual

Observaciones: Las licencias Microsoft 365 ya incluyen MFA y herramientas de auditoría básicas. Solo se proyecta una inversión menor para capacitación técnica y, eventualmente, una licencia adicional para software de gestión de contraseñas si se busca una solución más avanzada (por ejemplo, LastPass Enterprise o Keeper Business).

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento es completamente aplicable al entorno actual de Auxadi Costa Rica. Los recursos tecnológicos y financieros ya están disponibles, y los ajustes necesarios se enfocan en fortalecer la capacitación del personal técnico y formalizar el rol de responsable IAM para garantizar un control continuo y documentado de accesos y privilegios.

Resultados procedimiento de gestión segura de dispositivos y BYOD.

Recursos tecnológicos: Intune (MDM), BitLocker, antivirus corporativo, NAC, SIEM.

Recursos humanos: TI (validaciones), Cumplimiento (supervisión), Gerencia (autorizaciones).

Recursos financieros: Ampliación licencias MDM, campañas de concienciación, almacenamiento seguro.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi Costa Rica ya utiliza Intune para la gestión de dispositivos corporativos y cuenta con BitLocker habilitado en equipos críticos. El SIEM y antivirus están implementados con cobertura total. Se sugiere incluir el control NAC dentro del roadmap de seguridad para fortalecer la verificación de cumplimiento antes de la conexión de dispositivos externos.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El personal de TI posee experiencia en la gestión de dispositivos, aunque se recomienda una capacitación específica sobre políticas BYOD, administración de Intune en escenarios híbridos y protocolos de borrado remoto. Se sugiere formalizar los acuerdos de uso de dispositivos personales con apoyo del área de Cumplimiento.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Parcialmente, se requiere ampliación o ajuste de presupuesto

Observaciones: Aunque la mayoría de las licencias están cubiertas por Microsoft 365, se prevé una inversión moderada en campañas de concienciación, almacenamiento adicional en nube y posibles certificados digitales. Los costos pueden optimizarse mediante la reutilización de recursos existentes y el aprovechamiento de programas de capacitación interna.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento es factible y coherente con la infraestructura actual de Auxadi Costa Rica. Las necesidades principales se centran en la capacitación en administración BYOD, la formalización de acuerdos internos y la incorporación progresiva de controles NAC. Las inversiones previstas son manejables y pueden ser cubiertas con ajustes mínimos al presupuesto operativo.

Resultados procedimiento de acceso remoto seguro.

Recursos tecnológicos: VPN SSL AES-256, MFA, SIEM, alertas automáticas.

Recursos humanos: TI (monitoreo), Cumplimiento (auditorías), usuarios (acuerdos y formación).

Recursos financieros: Licencias M365, mantenimiento VPN y capacitaciones en teletrabajo seguro.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi Costa Rica mantiene una VPN SSL estable y funcional con autenticación multifactor. Los dispositivos remotos se encuentran registrados y gestionados mediante Intune, lo que asegura trazabilidad. Se recomienda reforzar el sistema de alertas automáticas del SIEM para detección temprana de intentos no autorizados y vincular los reportes con el centro de cumplimiento.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Sí, el recurso humano es suficiente y capacitado

Observaciones: El equipo técnico y de cumplimiento demuestra competencia en la administración de accesos remotos y monitoreo de seguridad. Se recomienda mantener capacitaciones periódicas sobre gestión de accesos, nuevas amenazas asociadas al teletrabajo y protocolos de respuesta ante incidentes de conexión insegura.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Sí, se cubren con el presupuesto actual

Observaciones: No se requieren inversiones significativas. La suscripción de Microsoft 365 incluye MFA, gestión de dispositivos y soporte remoto. Solo se prevé un gasto menor en capacitaciones y mantenimiento preventivo anual del entorno VPN y sus certificados.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento se considera completamente viable, dado que la empresa ya cuenta con la infraestructura tecnológica, el personal capacitado y los recursos financieros necesarios para su aplicación. Las recomendaciones se centran en reforzar la detección automatizada de anomalías y mantener una cultura de seguridad activa entre los usuarios remotos.

Resultados política de seguridad en la comunicación corporativa.

Recursos tecnológicos: M365 Security & Compliance Center, DLP, IRM, SPF/DKIM/DMARC, ATP.

Recursos humanos: TI (configuraciones), Cumplimiento (revisión), usuarios (prevención de phishing).

Recursos financieros: Renovación licencias M365, capacitación y campañas internas.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi ya dispone de un entorno Microsoft 365 seguro y con herramientas avanzadas activas, incluyendo DLP, ATP y políticas de cifrado TLS. Se sugiere fortalecer la correlación de alertas entre DLP y SIEM para mejorar la trazabilidad de eventos y reforzar la detección de intentos de fuga de información en tiempo real.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El personal técnico cuenta con los conocimientos operativos básicos para la administración de DLP y ATP; sin embargo, se recomienda una capacitación complementaria para el equipo de Cumplimiento en el manejo de excepciones, análisis forense de alertas y revisión de reportes desde el portal de seguridad. También se sugiere reforzar las campañas de concientización a usuarios sobre correos fraudulentos y comunicación segura.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Parcialmente, se requiere ampliación o ajuste de presupuesto

Observaciones: Aunque la mayoría de los servicios se cubren con Microsoft 365, será necesario destinar un presupuesto adicional para capacitación técnica, renovación de licencias con acceso a funciones premium de ATP y campañas internas de sensibilización al personal, especialmente en simulaciones de phishing.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: La política se considera funcional y alineada a las capacidades actuales de Auxadi Costa Rica. No obstante, se recomienda invertir en formación continua, mejorar la correlación de eventos entre plataformas de seguridad y mantener campañas periódicas de educación digital para garantizar la efectividad sostenida del control comunicacional.

Resultados procedimiento de uso seguro de correo y documentos.

Recursos tecnológicos: TLS/OME, DLP, IRM, etiquetado de sensibilidad, SharePoint/OneDrive.

Recursos humanos: TI (gestión técnica), Cumplimiento (revisión), usuarios (aplicación de cifrado).

Recursos financieros: Licencias M365, capacitación y monitoreo de cumplimiento.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi cuenta con la infraestructura necesaria, ya que dispone de Microsoft 365 con DLP, OME y SharePoint configurados para el control de documentos. Sin embargo, se recomienda revisar la automatización del etiquetado de sensibilidad y reforzar la auditoría de documentos compartidos externamente para minimizar riesgos de exposición accidental.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El equipo de TI tiene dominio sobre las configuraciones técnicas, pero se detecta la necesidad de capacitación adicional para los colaboradores en la correcta aplicación de etiquetas de sensibilidad, cifrado manual de correos y uso seguro de los enlaces de OneDrive/SharePoint. También se sugiere involucrar más activamente al área de Cumplimiento en la revisión de métricas de DLP.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Sí, se cubren con el presupuesto actual

Observaciones: Las herramientas y licencias requeridas ya están incluidas en los planes de Microsoft 365 contratados por la empresa. Los costos adicionales serían mínimos y se limitarían a

la ejecución de talleres anuales de capacitación o actualización técnica sobre el uso seguro de correo y documentos.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento es totalmente viable con los recursos actuales de Auxadi Costa Rica. Se considera que la empresa dispone de la infraestructura necesaria y que el cumplimiento depende principalmente del refuerzo en la cultura de uso seguro de la información. Se recomienda mantener capacitaciones anuales y revisiones de cumplimiento semestrales para asegurar la efectividad continua del control.

Resultados procedimiento de protección frente a amenazas en comunicaciones.

Recursos tecnológicos: Filtros antispam/malware, SPF/DKIM/DMARC, Safe Links, SIEM.

Recursos humanos: TI (configuración), Cumplimiento (simulaciones), usuarios (reporte de incidentes).

Recursos financieros: Campañas semestrales y capacitación; licencias M365 cubren lo esencial.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi ya dispone de Microsoft Defender con funcionalidades de filtrado, Safe Links y Safe Attachments. No obstante, se sugiere configurar un tablero de métricas consolidado en SIEM para obtener visibilidad centralizada de intentos de phishing, correos bloqueados y tasas de respuesta de usuarios ante simulaciones.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El equipo técnico tiene experiencia suficiente en la administración de políticas de correo seguro. Sin embargo, se identificó la necesidad de fortalecer la capacitación de los usuarios finales en la detección de intentos de ingeniería social y en el uso adecuado del botón de reporte de phishing de Outlook. Se recomienda coordinar talleres semestrales junto con Cumplimiento y Talento Humano.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Sí, se cubren con el presupuesto actual

Observaciones: La empresa ya cuenta con licencias Microsoft 365 que incluyen la mayoría de las funciones requeridas, como Safe Links, Safe Attachments y simuladores de phishing. Los costos se limitan a la logística de capacitación y al mantenimiento preventivo del entorno de seguridad, sin implicar inversión significativa.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento es viable y en gran medida ya implementado en Auxadi Costa Rica. Los ajustes recomendados se enfocan en la automatización del monitoreo de incidentes y en el fortalecimiento de la capacitación del personal frente a amenazas de ingeniería social. Con estas mejoras, la organización refuerza su postura de ciberseguridad y consolida un entorno más resiliente frente a ataques por correo electrónico o canales digitales.

Resultados política de protección de datos y continuidad de la información.

Recursos tecnológicos: Respaldo automatizado, cifrado, BCP/DRP, SIEM.

Recursos humanos: TI (respaldos), Cumplimiento y DPO (revisión normativa), Gerencia (simulacros).

Recursos financieros: Almacenamiento en nube, licencias backup y auditorías externas.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi Costa Rica dispone de soluciones en la nube para respaldos automatizados y cifrado integrado, además de documentación inicial del BCP/DRP. Se recomienda fortalecer la integración de registros de respaldo con el SIEM y formalizar la programación automática de reportes de respaldo y restauración exitosos para auditoría.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El equipo de TI cuenta con la experiencia técnica necesaria para ejecutar los respaldos y planes de recuperación. No obstante, se identificó la necesidad de reforzar la capacitación en procedimientos de continuidad y respuesta ante incidentes, especialmente en el personal de cumplimiento y en las áreas operativas que participan en los simulacros.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Parcialmente, se requiere ampliación o ajuste de presupuesto.

Observaciones: Si bien la mayor parte de los recursos tecnológicos están cubiertos, se prevé un costo adicional por la realización de simulacros anuales, auditorías externas y capacitaciones. Se sugiere gestionar un presupuesto anual específico para continuidad del negocio, que contemple estos ejercicios y la renovación periódica de almacenamiento en la nube.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: La política se considera adecuada y viable para Auxadi Costa Rica, dado que la empresa cuenta con la infraestructura tecnológica y procesos básicos de respaldo. Los ajustes se centran en mejorar la trazabilidad de restauraciones, asignar presupuesto recurrente a simulacros y fortalecer la capacitación del personal involucrado en la continuidad operativa. Esto permitirá garantizar la resiliencia y el cumplimiento sostenido de la organización ante incidentes o interrupciones.

Resultados procedimiento de copias de seguridad y continuidad del negocio.

Recursos tecnológicos: Azure Backup, almacenamiento redundante, cifrado, pruebas trimestrales.

Recursos humanos: TI (ejecución), Cumplimiento (validación), Gerencia (autorización de simulacros).

Recursos financieros: Licencias de almacenamiento, software de backup, capacitación técnica.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Sí, reflejan la realidad actual.

Observaciones: Auxadi cuenta con sistemas automatizados de respaldo en la nube y almacenamiento redundante mediante Azure Backup. Se recomienda fortalecer la automatización de reportes SIEM para que reflejen los resultados de cada ciclo de respaldo y restauración, permitiendo auditorías más eficientes y trazables.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Parcialmente, requiere capacitación o reasignación de funciones.

Observaciones: El personal técnico posee la experiencia necesaria para ejecutar los respaldos y restauraciones, sin embargo, se recomienda capacitación complementaria en gestión de continuidad operativa y análisis de incidentes post-restauración, con el fin de mejorar la efectividad y la documentación de resultados.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Sí, se cubren con el presupuesto actual

Observaciones: La infraestructura de respaldo y las licencias principales ya están cubiertas por las suscripciones vigentes de Microsoft 365 y Azure. Solo se prevé un costo menor vinculado a la capacitación técnica anual y posibles auditorías de cumplimiento.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento se considera plenamente viable y ajustado a la realidad de Auxadi Costa Rica, ya que aprovecha herramientas existentes, como Azure Backup, para mantener la disponibilidad de la información y la recuperación rápida ante fallos. La única mejora sugerida

es fortalecer la trazabilidad mediante reportes automáticos y continuar con la capacitación del personal en escenarios de contingencia y continuidad operativa.

Resultados procedimiento de gestión de información, incidentes y cumplimiento.

Recursos tecnológicos: SIEM, DLP, mesa de servicio, repositorio con auditorías.
Recursos humanos: Cumplimiento (lidera), TI (análisis técnico), Gerencia (supervisión).
Recursos financieros: Licencias SIEM, mantenimiento Help Desk y auditorías anuales.

- Pregunta 1: ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?

Parcialmente, se requiere actualización o ampliación.

Observaciones: Auxadi cuenta con funcionalidades básicas de registro y seguimiento mediante la mesa de servicio y monitoreo centralizado a través de M365, sin embargo, se recomienda fortalecer la integración con una plataforma SIEM completa para correlacionar eventos, detectar anomalías y generar reportes automáticos de cumplimiento.

- Pregunta 2: ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?

Sí, el recurso humano es suficiente y capacitado.

Observaciones: El equipo actual dispone de la experiencia necesaria para ejecutar la gestión de incidentes y el cumplimiento normativo. No obstante, se sugiere realizar capacitaciones periódicas en análisis forense digital y documentación de incidentes críticos, con el fin de elevar la calidad de los registros y fortalecer la trazabilidad.

- Pregunta 3: ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?

Parcialmente, se requiere ampliación o ajuste de presupuesto.

Observaciones: El presupuesto actual cubre las operaciones básicas y el mantenimiento de la mesa de servicio, pero sería necesaria una inversión adicional moderada para adquirir licencias SIEM más avanzadas y realizar auditorías externas anuales que certifiquen la conformidad con los estándares ISO.

- Pregunta 4: Conclusión grupal sobre la validación del análisis de requerimientos:

Validado con ajustes.

Notas finales: El procedimiento fue validado por el equipo de TI, Cumplimiento y Gerencia, confirmando que los mecanismos actuales permiten una gestión efectiva de incidentes y cumplimiento normativo. Se acordó priorizar la ampliación del sistema SIEM y formalizar un calendario de auditorías anuales para mantener la trazabilidad, reforzando así la madurez del sistema de gestión de seguridad de la información.

Resultados Informe

El análisis detallado de costos y recursos se desarrolló tomando como base los resultados de la entrevista grupal con el equipo de Tecnologías de la Información de Auxadi Costa Rica, la cual permitió identificar con precisión los recursos tecnológicos, humanos y financieros disponibles, así como aquellos que requieren ajustes o fortalecimiento para garantizar la correcta implementación de las políticas y procedimientos definidos conforme a la norma ISO/IEC 27001:2022.

El propósito de esta etapa fue evitar duplicidades de inversión y reflejar únicamente los costos reales, enfocados en las actividades que efectivamente demandan mantenimiento, formación o actualización tecnológica. Se buscó, además, asegurar la sostenibilidad operativa del

sistema de gestión de seguridad de la información (SGSI), alineando cada gasto proyectado con la capacidad financiera y estructura actual de la empresa.

Para la estimación de valores económicos, se tomaron como referencia precios de mercado actualizados en Costa Rica (octubre 2025), consultando fuentes públicas, proveedores locales de tecnología, distribuidores oficiales de Microsoft y empresas especializadas en auditoría y ciberseguridad. Todos los valores se expresan en colones costarricenses (CRC), considerando el tamaño de Auxadi Costa Rica (aproximadamente 30 colaboradores) y su modelo de operación híbrido con servicios en la nube.

Asimismo, se revisaron los contratos vigentes de Microsoft 365 E3, que incluyen herramientas clave como Intune, BitLocker, MFA, Defender, Azure AD, SharePoint y OneDrive, determinándose que la infraestructura tecnológica base ya cubre la mayoría de los controles contemplados en las políticas. Esto permitió reducir significativamente el impacto financiero y centrar los costos proyectados en rubros de optimización continua.

Los costos estimados para capacitaciones, campañas, auditorías, simulacros, mantenimientos y renovaciones de certificados se fundamentaron en la estructura operativa actual de Auxadi y en las observaciones obtenidas durante la entrevista técnica. Cada rubro fue evaluado conforme a su frecuencia, dependencia interna y nivel de especialización requerido:

- Capacitaciones técnicas y talleres especializados: Se priorizó el modelo “train-the-trainer”, en el que el propio personal técnico de Auxadi (particularmente del área de TI y Cumplimiento) imparte las sesiones al resto del equipo. Estas capacitaciones se realizarían semestral o anualmente, aprovechando recursos gratuitos o subvencionados de Microsoft Learn, ESET Training o portales de ciberseguridad. Solo se presupuestaron gastos mínimos en materiales o participación en cursos externos específicos (por ejemplo, gestión de incidentes o auditorías ISO), sin recurrir a consultores permanentes.
- Campañas de concientización y cultura de seguridad: Se desarrollarán internamente, lideradas por Cumplimiento y Talento Humano, con apoyo del área de TI. Su ejecución se hará mediante canales corporativos digitales (Microsoft Teams, intranet, correo

institucional y carteleras informativas), por lo que no representan un gasto financiero adicional. Únicamente se asigna un margen menor para diseño gráfico o refuerzo comunicacional en caso de ser necesario.

- Renovación de certificados digitales y mantenimiento de VPN: Estas actividades serán responsabilidad directa del área de TI y forman parte de su labor rutinaria de mantenimiento preventivo. El costo considerado proviene únicamente del pago a la autoridad certificadora (como RACSA o DigiCert) por la emisión de certificados SSL/TLS, no de mano de obra interna.
- Monitoreo y mantenimiento del SIEM y herramientas de seguridad: Este trabajo se realizará de manera continua por el personal de TI, aprovechando Microsoft Defender y Sentinel. Se prevé solo un gasto marginal asociado a la actualización de licencias o soporte técnico, ya que el monitoreo, la revisión de logs y la generación de reportes se ejecutan internamente.
- Simulacros y pruebas de continuidad del negocio: u planificación y ejecución estarán a cargo de TI, Cumplimiento y Gerencia, como parte del plan BCP/DRP existente. Al ser una actividad interna, no genera costos adicionales más allá del tiempo operativo invertido. Únicamente se prevé un gasto menor si se decide validar el simulacro con una auditoría externa o consultoría puntual.
- Auditorías internas y externas de cumplimiento: Las auditorías internas serán realizadas por Cumplimiento y TI, mientras que las externas se ejecutarán anualmente mediante un proveedor especializado en ISO/IEC 27001. Por tanto, el único costo considerado en este rubro corresponde al servicio profesional externo para certificar la conformidad y emitir recomendaciones oficiales.

Los costos y estrategias que se presentan a continuación fueron calculados conforme a la metodología previamente descrita, considerando los resultados de la entrevista técnica y la disponibilidad real de recursos en Auxadi Costa Rica. Cada política y procedimiento refleja la relación entre los medios tecnológicos existentes, los recursos humanos asignados y las necesidades de inversión complementaria identificadas. En los casos donde la empresa ya dispone de las herramientas o servicios requeridos, se indica explícitamente, y solo se cuantifican aquellos rubros que implican un gasto real o mejoras en capacitación, mantenimiento o auditoría.

Política de gestión y control seguro de dispositivos.

Recursos ya disponibles.

- Licencias Microsoft 365 E3 con Intune, BitLocker y MFA.
- SIEM integrado mediante Microsoft Defender.
- VPN SSL corporativa funcional.

Costos requeridos.

- Reposición de equipos sin TPM 2.0 (aprox. ₡120 000 por equipo × 4 unidades): ₡480 000.
- Candados o lockers para resguardo físico (₡25 000 × 10 unidades): ₡250 000.
- Materiales para capacitación técnica anual (Intune, cifrado y políticas de custodia): ₡150 000.
- Costo total estimado: ₡880 000.

Estrategias de optimización.

- Aprovechar licencias incluidas en Microsoft 365.
- Centralizar compras de hardware y candados con proveedores corporativos.
- Realizar talleres internos con modalidad *train-the-trainer*.

Se propone optimizar el uso de Intune y BitLocker mediante la automatización de políticas de cumplimiento, lo que reducirá el tiempo de administración y los incidentes de configuración. Además, se recomienda aprovechar los reportes automáticos en Power BI integrados al SIEM, para obtener métricas de cumplimiento sin incurrir en costos adicionales. El enfoque principal es maximizar las licencias ya incluidas en Microsoft 365, destinando solo un pequeño presupuesto a capacitación técnica, con lo cual se garantiza eficiencia operativa y seguridad sostenida. Las capacitaciones serán internas, impartidas por el mismo equipo de TI bajo el formato “train-the-

trainer". Además, se concentrarán las compras de equipos y accesorios de seguridad mediante convenios corporativos, garantizando ahorro y homogeneidad.

Procedimiento de gestión de identidades, credenciales y accesos (IAM).

Recursos ya disponibles.

- AD y Azure AD sincronizados.
- MFA operativo en todo el personal.

Costos requeridos.

- Capacitación técnica avanzada para administración híbrida AD/Azure: ₡250 000.
- Posible licencia de gestor corporativo de contraseñas (por ejemplo, Keeper Business): ₡200 000.
- Costo total estimado: ₡450 000.

Estrategias de optimización.

- Automatizar reportes de accesos con PowerShell o Compliance Manager.
- Designar un responsable IAM interno sin contratar personal nuevo.
- Capacitaciones especializadas.

La estrategia se centra en consolidar la administración de identidades híbridas mediante Azure AD y MFA, implementando scripts de automatización para auditorías y reportes de accesos. Esto reduce la carga operativa y los errores humanos, además de mejorar la trazabilidad. Se recomienda capacitar al personal de TI en herramientas como PowerShell y Microsoft Compliance Manager, aprovechando recursos gratuitos o subvencionados por Microsoft. De esta forma, se eleva la eficiencia sin generar nuevos costos de licenciamiento. Las capacitaciones especializadas se realizarán una vez al año y podrán ser cubiertas parcialmente por programas gratuitos de

Microsoft. De esta manera se garantiza la eficiencia operativa y trazabilidad sin incrementar el gasto anual.

Procedimiento de gestión segura de dispositivos y BYOD.

Recursos ya disponibles.

- Intune activo, BitLocker implementado, antivirus corporativo.

Costos requeridos.

- Campañas de concienciación BYOD (materiales menores): ₡100 000.
- Almacenamiento adicional en nube para respaldos BYOD (espacio “cool tier”): ₡100 000.
- Certificados digitales para autenticación: ₡100 000.
- Costo total estimado: ₡300 000.

Estrategias de optimización.

- Limitar el esquema BYOD a personal autorizado.
- Aprovechar Intune y Azure AD para control remoto.
- Gestionar almacenamiento con niveles “cool” o “archive” en Azure.

Para optimizar costos, se sugiere ampliar gradualmente las políticas BYOD dentro de Intune sin adquirir licencias adicionales, utilizando configuraciones de seguridad personalizadas para los dispositivos personales. Además, se plantea reforzar la concientización mediante campañas internas en Teams y correos informativos, evitando gastos en material físico o consultorías externas. El almacenamiento en Azure se optimizará usando niveles de bajo costo para datos poco accedidos. Estas medidas consolidan la protección sin aumentar el presupuesto, priorizando la reutilización de la infraestructura y recursos humanos existentes.

Procedimiento de acceso remoto seguro.

Recursos ya disponibles.

- VPN SSL, MFA y licencias M365 activas.

Costos requeridos.

- Renovación anual de certificados digitales: ₡125 000.
- Costo total estimado: ₡125 000.

Estrategias de optimización.

- Uso de certificados agrupados bajo contratos existentes.
- Capacitaciones virtuales internas para reducir costo logístico.
- Mantenimiento anual de VPN.
- Talleres de teletrabajo seguro.

La optimización se logra mediante la integración total de la VPN con el ecosistema Microsoft 365 y Azure AD, habilitando alertas automatizadas en el SIEM y reforzando el monitoreo sin adquirir soluciones externas. Asimismo, se sugiere realizar capacitaciones virtuales sobre teletrabajo seguro utilizando plataformas internas, reduciendo costos logísticos. El mantenimiento de la VPN y el monitoreo se mantendrán internos bajo TI. Los talleres de teletrabajo seguro serán impartidos por Cumplimiento y TI en formato virtual, sin costo adicional. Los certificados digitales se agruparán bajo contratos vigentes, reduciendo la frecuencia de renovación y garantizando continuidad operativa. Con ello se garantiza un entorno remoto seguro y trazable, aprovechando los recursos tecnológicos ya disponibles en la organización.

Política de seguridad en la comunicación corporativa.

Recursos ya disponibles.

- DLP, ATP, TLS, SPF/DKIM/DMARC configurados en M365.

Costos requeridos.

- Actualización de licencias premium ATP: ₡200 000.
- Costo total estimado: ₡200 000.

Estrategias de optimización.

- Usar herramientas de simulación internas de Defender.
- Priorizar datos más críticos al activar políticas DLP.
- Capacitación avanzada en DLP/ATP.
- Campañas internas de concientización.

Se recomienda centralizar las políticas de DLP, IRM y ATP dentro del Centro de Cumplimiento de Microsoft 365, lo que elimina la necesidad de múltiples herramientas. También se propone realizar campañas semestrales de sensibilización digital aprovechando canales internos y simulaciones integradas de phishing. Las licencias se revisarán anualmente para determinar si las funciones premium son realmente necesarias, optimizando el gasto. Estas medidas reducen costos y aumentan la efectividad del personal frente a amenazas, promoviendo una cultura preventiva de seguridad sin incrementar gastos.

Procedimiento de uso seguro de correo y documentos.

Recursos ya disponibles.

- Infraestructura completa en Microsoft 365 (TLS, IRM, DLP, OneDrive, SharePoint).

Costos requeridos.

- Material para talleres anuales sobre cifrado y etiquetas: ₡100 000.
- Costo total estimado: ₡100 000.

Estrategias de optimización.

- Automatizar etiquetado mediante reglas en Exchange y SharePoint.
- Capacitación anual en uso de etiquetas y cifrado.
- Capacitar líderes internos para replicar la formación al resto del personal.
- Monitoreo de cumplimiento documental.

La estrategia consiste en automatizar el etiquetado de sensibilidad y la clasificación de documentos mediante las funciones nativas de Microsoft Purview, evitando configuraciones manuales que consumen tiempo y aumentan el riesgo humano. Se recomienda además realizar talleres prácticos sobre cifrado de correos y uso seguro de OneDrive, con sesiones breves en línea para todos los empleados. Así se optimiza el uso de licencias existentes y se mejora la productividad del personal sin costos adicionales relevantes.

Procedimiento de protección frente a amenazas en comunicaciones.

Recursos ya disponibles.

- Microsoft Defender (Safe Links, Safe Attachments, simulador de phishing).

Costos requeridos.

- Materiales o refuerzo visual para campañas internas: ₡100 000.
- Costo total estimado: ₡100 000.

Estrategias de optimización:

- Usar el simulador nativo de Microsoft Defender.
- Reutilizar material de capacitación entre departamentos.
- Talleres semestrales de concienciación.
- Campañas simuladas de phishing.

Se plantea fortalecer la integración entre Microsoft Defender y el SIEM para obtener reportes consolidados de intentos de phishing y malware, utilizando las herramientas incluidas en las licencias actuales. La capacitación del personal puede gestionarse internamente mediante simulaciones periódicas y escenarios reales supervisados por cumplimiento, evitando contratar servicios externos. Con ello, se mejora la resiliencia organizacional sin aumentar los costos de operación.

Política de protección de datos y continuidad de la información.

Recursos ya disponibles.

- Azure Backup activo, cifrado en tránsito y reposo, BCP/DRP inicial.

Costos requeridos.

- Simulacros externos anuales de recuperación: ₡200 000.
- Auditorías externas de cumplimiento: ₡350 000.
- Costo total estimado: ₡550 000.

Estrategias de optimización.

- Planificar simulacros internos antes de auditorías.
- Reutilizar almacenamiento cloud existente en modalidad “cool tier”.
- Capacitación en continuidad y respuesta a incidentes.

La optimización se basa en aprovechar al máximo los servicios de respaldo y cifrado incluidos en Azure Backup y OneDrive, reduciendo la dependencia de soluciones externas. Se recomienda establecer un plan anual de simulacros de continuidad y auditorías, utilizando la infraestructura actual de nube. Las capacitaciones y simulacros internos serán dirigidos por TI y Cumplimiento sin costo adicional. Se aprovechará el almacenamiento cloud existente en modalidad “cool tier” y se programarán auditorías externas alternadas por año fiscal para reducir la carga presupuestaria. Este enfoque permite mantener la resiliencia operativa y el cumplimiento normativo sin incurrir en gastos adicionales significativos.

Procedimiento de copias de seguridad y continuidad del negocio.

Recursos ya disponibles.

- Azure Backup y almacenamiento redundante operativos.

Costos requeridos.

- Auditorías internas y pruebas de restauración trimestrales: ₡150 000.
- Costo total estimado: ₡150 000.

Estrategias de optimización.

- Automatizar reportes en SIEM.
- Escalar restauraciones parciales para ahorrar tiempo y recursos.
- Capacitación técnica anual.

Se sugiere automatizar las pruebas de restauración y reportes de respaldo utilizando los flujos nativos de Azure Backup, lo que disminuye el tiempo de gestión manual. Además, las capacitaciones pueden integrarse al calendario de formación interna, reduciendo costos externos. El equipo de TI automatizará reportes de respaldo y restauración usando Power Automate,

integrando los resultados al SIEM. Las capacitaciones se incorporarán al plan de formación interna anual. Con ello se asegura trazabilidad y eficiencia operativa con costo mínimo. Con esta estrategia se garantiza un proceso más ágil, trazable y sostenible en el tiempo, manteniendo los costos dentro del presupuesto actual.

Procedimiento de gestión de información, incidentes y cumplimiento.

Recursos ya disponibles.

- Mesa de servicio operativa y registro básico en M365.

Costos requeridos.

- Ampliación funcionalidad SIEM (₡450 000).
- Auditorías externas anuales (₡350 000).
- Costo total estimado: ₡800 000.

Estrategias de optimización.

- Centralizar SIEM con Defender y Compliance Manager.
- Coordinar auditorías internas y externas escalonadas.
- Capacitación en análisis forense digital.

La optimización prioriza la ampliación del monitoreo SIEM con herramientas ya compatibles (Defender, Intune, Microsoft Sentinel), sin necesidad de adquirir licencias adicionales de alto costo. Asimismo, se recomienda desarrollar guías internas para el análisis forense digital, integrando las auditorías anuales dentro del calendario de cumplimiento existente. La capacitación en análisis forense digital será interna, basada en casos reales. Las auditorías internas se ejecutarán semestralmente por Cumplimiento, mientras las externas se realizarán una vez al año para garantizar conformidad y trazabilidad. Esta estrategia reduce gastos externos y eleva la capacidad interna de respuesta ante incidentes.

Recursos humanos requeridos

De acuerdo con las observaciones de la entrevista y el análisis consolidado, se determinó que Auxadi Costa Rica ya dispone del personal necesario para ejecutar las actividades previstas, por lo que no se consideran nuevas contrataciones. No obstante, se definieron los roles y responsabilidades generales que aseguran la aplicación integral del sistema:

- Área de Tecnologías de la Información (TI): responsable de la implementación técnica, monitoreo, respaldo, administración de accesos y soporte general de las herramientas de seguridad.
- Área de Cumplimiento: encargada de coordinar auditorías internas, validar políticas, liderar la gestión de incidentes y garantizar la trazabilidad de las acciones correctivas.
- Gerencia General: supervisa los planes de continuidad, autoriza presupuestos y aprueba las revisiones anuales de desempeño del SGSI.
- Talento Humano: gestiona las campañas de sensibilización, firma de acuerdos BYOD y medidas disciplinarias ante incumplimientos.
- Usuarios finales: cumplen las directrices y participan en los programas de capacitación y concientización.

En conjunto, esta estructura permite mantener un modelo de gobernanza horizontal y coordinado, donde las responsabilidades se distribuyen entre áreas ya establecidas, evitando duplicidad de funciones y optimizando la capacidad interna.

Tabla 10

Tabla de costos totales estimados.

Política / Procedimiento	Descripción de costo principal	Costo Estimado (₡ CRC)	Tipo de Costo
Política de gestión y control seguro de dispositivos	Reposición de equipos sin TPM 2.0, candados físicos y materiales de capacitación técnica interna	₡880 000	Inversión puntual
Procedimiento IAM (gestión de identidades, credenciales y accesos)	Capacitaciones avanzadas AD/Azure e implementación de gestor de contraseñas corporativo	₡450 000	Capacitación / Licencia menor

Procedimiento de gestión segura de dispositivos y BYOD	Materiales de campaña interna, almacenamiento cloud adicional y certificados digitales	₡300 000	Operativo / Seguridad
Procedimiento de acceso remoto seguro	Renovación de certificados digitales agrupados	₡125 000	Operativo anual
Política de seguridad en la comunicación corporativa	Actualización de licencias premium ATP	₡200 000	Licencia complementaria
Procedimiento de uso seguro de correo y documentos	Materiales para talleres anuales de cifrado y etiquetas	₡100 000	Formación interna
Procedimiento de protección frente a amenazas en comunicaciones	Material visual y refuerzo para campañas internas de concientización	₡100 000	Comunicación interna
Política de protección de datos y continuidad de la información	Simulacros externos anuales y auditorías externas ISO	₡550 000	Auditoría / Continuidad
Procedimiento de copias de seguridad y continuidad del negocio	Auditorías internas y pruebas de restauración trimestrales	₡150 000	Control interno
Procedimiento de gestión de información, incidentes y cumplimiento	Ampliación del SIEM y auditoría externa de cumplimiento	₡800 000	Auditoría / Monitoreo
Total anual estimado		₡3 655 000	

Fuente: Elaboración propia

Informe de Impacto y Beneficios

Objetivo del Informe

El presente informe tiene como propósito analizar los beneficios esperados derivados de la implementación de las políticas y procedimientos de seguridad de la información propuestos para Auxadi Costa Rica, en concordancia con la norma ISO/IEC 27001:2022 y la Ley N.º 8968 sobre protección de datos personales. Su objetivo principal es proyectar el impacto organizacional, técnico y financiero de las medidas planteadas, valorando cómo contribuyen a la reducción de riesgos, la optimización de los procesos operativos y el fortalecimiento del cumplimiento normativo en materia de seguridad de la información. De igual forma, busca estimar la rentabilidad global de la propuesta, identificando los efectos positivos que generará en la productividad, la continuidad de las operaciones y la madurez del sistema de gestión, asegurando que los resultados

esperados se alcancen mediante el aprovechamiento de los recursos internos y la sostenibilidad del modelo en el tiempo.

Alcance de la Revisión

El alcance de esta revisión comprende el análisis de los beneficios esperados de la propuesta de políticas y procedimientos diseñados, abordando ciertos ejes fundamentales como la seguridad de la información, el cumplimiento normativo y la eficiencia operativa y financiera. Este análisis se sustenta en los hallazgos obtenidos durante el diagnóstico técnico y organizacional, las observaciones de la entrevista con el equipo de TI y los resultados del informe de costos y recursos con estrategias de optimización. Dado que el estudio se desarrolla en el marco de una propuesta técnica aún no implementada, los resultados se presentan como estimaciones razonadas, fundamentadas en la capacidad operativa actual de la organización y en su infraestructura tecnológica basada en el ecosistema Microsoft 365 y Azure. En este contexto, la revisión tiene como alcance evaluar el impacto proyectado de las medidas de control, la viabilidad de su ejecución con los recursos disponibles y el fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en términos de madurez, trazabilidad y sostenibilidad institucional.

Resultados Informe

Este análisis tiene como propósito proyectar los beneficios esperados tras la implementación de las políticas y procedimientos de seguridad de la información propuestos para Auxadi Costa Rica, en correspondencia con la norma ISO/IEC 27001:2022 y la legislación nacional vigente. Dado que el estudio se desarrolla en el marco de una propuesta técnica aún no ejecutada, los resultados se presentan como estimaciones razonadas, sustentadas en la información obtenida del diagnóstico previo, los resultados de la entrevista con el equipo de TI, y el análisis detallado de costos y recursos.

El objetivo principal es evaluar el impacto esperado en ciertas dimensiones clave como: seguridad de la información, cumplimiento normativo y alineación internacional, y eficiencia operativa y financiera. Con ello se busca determinar la rentabilidad global de la propuesta y su

contribución al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización.

Beneficios esperados.

Seguridad de la información.

- En el eje de seguridad de la información, se prevé una disminución progresiva en la frecuencia e impacto de los incidentes gracias a la implementación de controles preventivos y correctivos en las áreas de autenticación, cifrado, monitoreo y administración de dispositivos. El despliegue de autenticación multifactor (MFA), el uso de cifrado completo con BitLocker, y la gestión unificada mediante Microsoft Intune y Defender permitirán una detección y respuesta más temprana ante eventos de riesgo.
- Asimismo, la integración del monitoreo en un sistema SIEM consolidado generará alertas automáticas y reportes de cumplimiento en tiempo real, mejorando la capacidad de contención de incidentes y la trazabilidad de las acciones correctivas.
- La correcta aplicación de los procedimientos de respaldo y continuidad del negocio (BCP/DRP) fortalecerá la resiliencia operativa, garantizando la recuperación de información ante posibles fallos, ataques o interrupciones.
- En conjunto, estas medidas reducirán la probabilidad de pérdida de datos, accesos no autorizados o interrupciones críticas, incrementando la madurez y disponibilidad del entorno tecnológico corporativo. Aunque los resultados finales se obtendrán tras la implementación, se proyecta una mejora sustancial en los indicadores de control preventivo, detección temprana y recuperación efectiva ante incidentes.

Cumplimiento normativo y alineación internacional.

- En cuanto al cumplimiento normativo y alineación internacional, la propuesta consolida los principios y controles establecidos en los dominios 5, 6, 7 y 8 de la norma

ISO/IEC 27001:2022, orientados a los ámbitos organizativo, humano, físico y tecnológico.

- La adopción formal de las políticas y procedimientos permite crear un marco de gobernanza documentado, donde cada proceso cuenta con responsables definidos, registros auditables y mecanismos de revisión continua. Esta estructura facilita las auditorías internas y externas, el seguimiento de hallazgos y la trazabilidad de evidencias ante evaluaciones de conformidad.
- Además, la articulación entre los controles técnicos de la norma y las capacidades del entorno Microsoft 365 y Azure garantiza la alineación con la Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, fortaleciendo la gestión ética y legal de la información sensible.
- En consecuencia, la empresa no solo cumple con los requisitos de seguridad internacionales, sino que también se posiciona como una organización con madurez normativa y transparencia operativa, capaz de demostrar su compromiso con la confidencialidad, integridad y disponibilidad de la información ante clientes, auditores y entes reguladores.

Eficiencia operativa y financiera.

- Desde la perspectiva de la eficiencia operativa y financiera, la propuesta se fundamenta en la optimización de los recursos ya disponibles y en la reducción de dependencias externas.
- El aprovechamiento integral de las licencias Microsoft 365 E3, que incluyen Intune, Defender, BitLocker, Azure AD y OneDrive, minimiza la necesidad de nuevas adquisiciones tecnológicas.
- A su vez, la implementación de procesos automatizados mediante PowerShell, Compliance Manager y Azure Backup reduce la carga administrativa del equipo técnico y los errores humanos asociados a la gestión manual de seguridad.
- El modelo de capacitación train-the-trainer, en el que el personal interno imparte talleres a otros colaboradores, refuerza la cultura de seguridad sin generar costos

adicionales significativos, mientras las campañas de concientización internas permiten mantener la sensibilización del personal con una inversión mínima.

- La rentabilidad proyectada se observa en la reducción de costos indirectos por incidentes, reprocesos o tiempos de inactividad, y en la mejora de la productividad al contar con sistemas más estables y autogestionables.
- De esta forma, Auxadi Costa Rica podrá mantener un equilibrio entre la sostenibilidad financiera y la excelencia operativa, logrando ahorros progresivos a mediano plazo, sin comprometer la calidad ni la seguridad de sus operaciones.

El estudio de impacto y rentabilidad confirma que la propuesta es técnica, financiera y operativamente viable, y que su implementación aportará beneficios sostenibles tanto a nivel de seguridad como de desempeño organizacional. El diseño integral de políticas y procedimientos permite consolidar un modelo de gestión robusto, con responsabilidades claras, trazabilidad documental y controles basados en la norma ISO/IEC 27001:2022, adaptados al contexto real de Auxadi Costa Rica.

A nivel institucional, se prevé una reducción significativa de los incidentes relacionados con la información, una mejora en la disponibilidad de los sistemas y una respuesta más rápida ante posibles amenazas. En el ámbito normativo, la organización alcanzará una mayor madurez en cumplimiento, fortaleciendo su imagen corporativa ante clientes y auditores, al tiempo que garantiza la protección de los datos personales y la continuidad de las operaciones. En términos económicos, la estrategia de optimización planteada permite maximizar el retorno de la inversión y minimizar los costos asociados a errores humanos, interrupciones o vulnerabilidades, lo que genera un impacto positivo en la rentabilidad global del sistema.

En resumen, la adopción de este marco de políticas y procedimientos convertirá a Auxadi Costa Rica en una organización con una gestión de seguridad madura, resiliente y sostenible, capaz de responder eficazmente a los desafíos tecnológicos actuales y de mantener la conformidad con los más altos estándares internacionales de seguridad de la información.

Tabla 11

Tabla resumen de beneficios esperados

Dimensión	Aspecto evaluado	Condición actual	Situación proyectada tras implementación	Beneficio esperado
Seguridad	Gestión de incidentes y vulnerabilidades	Control parcial mediante monitoreo básico y medidas reactivas	Control integral y automatizado mediante SIEM, Intune y planes de respaldo	Reducción significativa de incidentes, aumento de la capacidad de respuesta y mejora en la resiliencia operacional
Cumplimiento normativo	Adherencia a ISO/IEC 27001 y Ley 8968	Cumplimiento parcial sin documentación formal	Cumplimiento estructurado y auditable con políticas y procedimientos aprobados	Fortalecimiento de gobernanza, trazabilidad y mitigación de riesgos legales
Eficiencia operativa	Procesos manuales de configuración y revisión	Procesos automatizados e integrados en Microsoft 365 y Azure	Mayor productividad, reducción de errores humanos y tiempos de gestión	Optimización de procesos y aumento de la eficiencia general del sistema
Recursos financieros	Presupuesto fragmentado por áreas	Presupuesto consolidado y reutilización de licencias	Administración unificada del gasto y aprovechamiento de infraestructura existente	Ahorro progresivo en mantenimiento, soporte y capacitación externa
Cultura de seguridad	Conocimiento desigual entre usuarios	Sensibilización parcial y formación esporádica	Plan anual de capacitación y campañas internas continuas	Mayor madurez organizacional, comportamiento seguro y reducción del riesgo humano

Fuente: Elaboración propia

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se logró analizar el estado actual de la seguridad de la información en Auxadi Costa Rica, identificando las principales vulnerabilidades y riesgos asociados a la gestión de dispositivos, la seguridad en la comunicación y la protección de datos. Este análisis permitió evidenciar la ausencia de lineamientos formales documentados y la necesidad de establecer políticas integrales que fortalezcan los controles existentes. A través del diagnóstico y las entrevistas con el equipo de TI, se obtuvo una visión completa del entorno operativo y de los recursos disponibles, lo que permitió determinar las áreas prioritarias de mejora y establecer una base sólida para la estructuración de la propuesta conforme a la norma ISO/IEC 27001:2022.

Se seleccionaron los controles de seguridad aplicables de acuerdo con los resultados del análisis de riesgos y las necesidades específicas de la organización. Este proceso permitió vincular cada riesgo identificado con uno o más controles definidos en los dominios organizativos, de personas, físicos y tecnológicos de la norma ISO/IEC 27001:2022. La correlación riesgo–control garantizó que las medidas propuestas respondieran a escenarios reales y verificables, priorizando la protección de los activos críticos y la continuidad de los servicios esenciales. De esta manera, se estableció un marco de seguridad ajustado a la capacidad operativa y tecnológica de la empresa.

Se diseñó una propuesta estructurada de políticas y procedimientos de seguridad de la información que integra los componentes técnicos, humanos y organizativos necesarios para proteger los datos corporativos, garantizar la trazabilidad de las acciones y fortalecer la cultura de seguridad interna. La propuesta abarca los ámbitos de gestión de dispositivos, comunicación segura y protección de datos, incorporando lineamientos claros, procedimientos operativos, requerimientos tecnológicos, humanos y financieros, así como estrategias de optimización que aseguran su sostenibilidad. Este diseño permite a la empresa adoptar un modelo de gestión alineado con las mejores prácticas internacionales y adaptable a futuras auditorías o certificaciones.

Se evaluó la viabilidad económica, operativa y técnica de la propuesta, demostrando que Auxadi Costa Rica cuenta con la mayoría de los recursos necesarios para su implementación. El análisis detallado de costos y recursos, junto con el informe de impacto y beneficios, confirmó que la ejecución de las políticas no requiere grandes inversiones ni contrataciones adicionales, dado que la organización ya dispone de una infraestructura tecnológica sólida basada en licencias Microsoft 365 E3 y personal capacitado. Las inversiones proyectadas se enfocan en capacitación, auditorías externas y mantenimiento de sistemas, lo que garantiza una ejecución eficiente, sostenible y con retorno positivo a mediano plazo.

En cumplimiento del objetivo general, se desarrolló una propuesta integral de políticas y procedimientos de seguridad de la información adaptada al contexto operativo de Auxadi Costa Rica y en total alineación con la norma ISO/IEC 27001:2022. La propuesta consolida un sistema de gestión robusto, preventivo y medible, que contribuye a reducir incidentes, fortalecer la protección de datos y aumentar la resiliencia institucional. Su aplicación permitirá a la empresa elevar su nivel de madurez en seguridad de la información, mejorar su posicionamiento frente a auditorías y reforzar la confianza de sus clientes y aliados estratégicos, garantizando así la sostenibilidad y continuidad de sus operaciones bajo un enfoque de mejora continua.

Recomendaciones

Con base en los resultados obtenidos durante el desarrollo del proyecto, se recomienda a Auxadi Costa Rica fortalecer y ampliar la gestión de la seguridad de la información mediante acciones complementarias que no fueron incluidas dentro del alcance de esta investigación, pero que resultan esenciales para garantizar la mejora continua, la sostenibilidad del sistema y la reducción de riesgos tecnológicos y operativos a largo plazo. Estas recomendaciones se sustentan en las buenas prácticas establecidas por la norma ISO/IEC 27001:2022, el principio de mejora continua y la necesidad de mantener la resiliencia institucional ante posibles incidentes de seguridad.

En primera instancia, se sugiere implementar un plan de automatización de controles y procesos de respaldo de información, con el fin de optimizar las tareas operativas que actualmente

se ejecutan de manera manual y reducir la probabilidad de errores humanos. La automatización debe incluir procesos como la programación de copias de seguridad, la verificación periódica de políticas de acceso, la correlación automática de eventos y la generación de reportes de cumplimiento. Estas medidas permitirán mejorar la eficiencia de las operaciones, garantizar la trazabilidad de los eventos de seguridad y aumentar la capacidad de respuesta ante incidentes. Se recomienda que el proyecto sea liderado por el departamento de Tecnología de la Información, con apoyo de un proveedor especializado en ciberseguridad y continuidad del negocio, en un plazo estimado de tres a cuatro meses. El costo aproximado de implementación sería de ₡2 000 000, incluyendo licencias de software, configuración inicial y mantenimiento anual. Este valor fue calculado tomando como referencia los precios promedio de soluciones comerciales de respaldo automatizado y monitoreo continúo aplicadas en entornos corporativos híbridos.

De igual forma, se recomienda que, una vez consolidadas las políticas y procedimientos definidos en esta propuesta, la organización inicie el proceso formal de certificación bajo la norma ISO/IEC 27001:2022. Obtener la certificación permitiría reforzar la confianza de los clientes internacionales, demostrar el cumplimiento de buenas prácticas de seguridad y fortalecer la reputación institucional. Este proceso puede desarrollarse en un plazo de doce meses, dirigido por la Gerencia General y el departamento de Tecnología de la Información, con acompañamiento de un consultor externo certificado en ISO. El costo aproximado se estima en ₡3 000 000, lo cual contempla auditorías externas, revisión documental, talleres de ajuste y soporte técnico. Este valor se basa en los precios de mercado nacionales asociados a procesos de certificación en empresas del sector de servicios profesionales.

Finalmente, se recomienda considerar la implementación de un sistema de evaluación y mejora continua del SGSI, mediante auditorías internas semestrales, revisiones de desempeño y seguimiento de indicadores clave de control. Este proceso, aunque no fue parte del alcance del proyecto, permitiría garantizar que las políticas y procedimientos mantengan su vigencia y eficacia frente a cambios tecnológicos, regulatorios u organizacionales. La ejecución podría realizarse con el equipo interno de TI, apoyado por la gerencia de operaciones, en un plazo estimado de dos meses por ciclo y con una inversión aproximada de ₡500 000 por revisión, cubriendo horas técnicas, reportes de auditoría y mantenimiento de registros.

En conjunto, estas recomendaciones permitirán a Auxadi Costa Rica consolidar un modelo de gestión de seguridad de la información sostenible, orientado a la eficiencia operativa, la mejora continua y el cumplimiento de estándares internacionales, fortaleciendo la posición de la empresa como una organización confiable, moderna y comprometida con la protección de los datos y la continuidad del negocio.

Bibliografía

Asamblea Legislativa de Costa Rica. (2001). *Ley N.º 8148: Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal para reprimir y sancionar los delitos informáticos*. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=47430&nValor3=50318&param1=NRTC&strTipM=TC

Asamblea Legislativa de Costa Rica. (2011). *Ley N.º 8968: Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales*. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=70975&nValor3=85989&param1=NRTC&strTipM=TC

Baca Urbina, G. (2016). Introducción a la seguridad informática (1.ª ed. ebook). Grupo Editorial Patria.

Concepto.de. (s. f.). *Investigación documental – Qué es, tipos, técnicas y ejemplos*. https://concepto.de/investigacion-documental/

Explorable.com. (s. f.). *Variables conceptuales*. https://explorable.com/es/variables-conceptuales

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill - Interamericana Editores.

Hernández Sampieri, R, Méndez Valencia, S., Mendoza Torres, C., Cuevas Romo, A. (2017). Fundamentos de investigación. 1ª edición. México: McGraw-Hill Interamericana.

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana.

IBM. (s. f.). *¿Qué son los controles de seguridad?* IBM. https://www.ibm.com/es-es/topics/security-controls

Interpolados. (2020). Procedimientos de seguridad en la información. Interpolados. https://interpolados.wordpress.com/2020/01/06/procedimientos-de-seguridad-en-la-informacion/

ISO/IEC 27001:2022 (2022). Information Security Management. ISO Standards.

Kaspersky. (s. f.). *Seguridad de la información: ¿Qué es y por qué es importante?* https://www.kaspersky.es/resource-center/definitions/information-security

Lara Muñoz, E. M. (2011). *Fundamentos de investigación: Un enfoque por competencias*. Alfaomega Grupo Editor.

López, R. A. (2017). *Sistema de gestión de la seguridad informática*. Fundación Universitaria del Área Andina.

Mohamed, M. M. H., Martel Carranza, C. P., Huayta Meza, F. T., Rojas León, C. R., & Arias Gonzáles, J. L. (2023). Metodología de la investigación: Guía para el proyecto de tesis (1.ª ed. digital). Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú.

Moreno Galindo, E. (2018, 9 de marzo). *Definición instrumental de las variables*. Metodología de investigación, pautas para hacer tesis. http://tesis-investigacion-cientifica.blogspot.com/2018/03/definicion-instrumental-de-las-variables.html

OBSBUSINESS School. (s.f.). *Estudio de viabilidad de un proyecto: ¿qué es y cómo hacerlo?* https://www.obsbusiness.school/blog/estudio-de-viabilidad-de-un-proyecto-estructura-e-importancia

Perallis Security. (s. f.). *Gestión de riesgos en seguridad de la información*. https://www.perallis.com/noticias/gestion-de-riesgos-en-seguridad-de-la-informacion

Pirani Risk. (s. f.). *Matriz de riesgos: qué es, ejemplos y cómo crearla fácil*. Pirani Risk. https://www.piranirisk.com/es/blog/matriz-de-riesgos-que-es-ejemplos-y-como-crearla-facil

Protección de Datos LOPD. (s. f.). *Política de seguridad de la información: Qué es y ejemplos*. https://protecciondatos-lopd.com/empresas/politica-seguridad-informacion

Orsys-Le Mag. (s. f.). *Política de seguridad – definición y objetivos*. https://orsys-lemag.com/es/glosario/politica-de-seguridad-%F0%9F%9F%A9-documento/

Roa Buendía, J. F. (2013). *Seguridad informática*. McGraw-Hill Interamericana de España.

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzules, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Editorial Área de Innovación y Desarrollo, S.L.

SalusPlay. (s. f.). *Tema 2. Las variables de investigación*. SalusPlay Apuntes Metodología de la Investigación. https://www.salusplay.com/apuntes/apuntes-metodologia-de-la-investigacion/tema-2-las-variables-de-investigacion/1

Samaniego Mena, E. A., & Ponce Ponce, J. A. (2017). Fundamentos de seguridad informática. Grupo Compás.

Unifikas. (s. f.). *¿Qué es un checklist y cómo se utiliza?* https://www.unifikas.com/es/noticias/que-es-un-checklist-y-como-se-utiliza

Vega Briceño, E. (2021). *Seguridad de la información*. Área de Innovación y Desarrollo, S.L.

Apéndices

Apéndice A. Guía de Entrevista 1

Entrevista técnica para clasificación de activos de información

El objetivo de la entrevista es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Entidad	
Nombre del entrevistado	
Puesto del entrevistado	
Fecha	

1. ¿Cuál de los siguientes activos considera crítico para las operaciones diarias? *(Marque todos los que apliquen)*
   ☐ Servidores
   ☐ Equipos de usuario final (PC, laptops)
   ☐ Dispositivos móviles corporativos
   ☐ Aplicaciones internas
   ☐ Sistemas de respaldo
   ☐ Correo electrónico corporativo
   ☐ Plataforma contable o ERP
   ☐ Otro: _____

2. ¿Existe un inventario formal de activos tecnológicos?
   ☐ Sí
   ☐ No
   ☐ Parcialmente

3. ¿Cuál es el nivel de impacto para la empresa si el activo deja de funcionar? *(Seleccione una por activo relevante)*
   ☐ Alto (afecta operaciones y servicios críticos)
   ☐ Medio (afecta algunas áreas no críticas)
   ☐ Bajo (afecta mínimamente)

4. ¿Cuál es la disponibilidad deseada para los activos deseados?
   ☐ 24/7 sin interrupciones
   ☐ Horario laboral (ej. 8 a.m. – 6 p.m.)
   ☐ Acceso eventual según necesidad

5. ¿Quién clasifica actualmente los activos según criticidad?
   ☐ Departamento de TI
   ☐ Consultores externos
   ☐ No se realiza clasificación
   ☐ Otro: _____

6. ¿Cuál de las siguientes medidas de protección aplica a los activos identificados como críticos? *(Marque todas las que correspondan)*
   ☐ Control de accesos
   ☐ Cifrado de datos
   ☐ Monitoreo activo
   ☐ Copias de seguridad
   ☐ Procedimientos documentados
   ☐ Ninguna
   ☐ Otro: _____

7. ¿Existe una matriz de riesgos que relacione los activos con su nivel de criticidad y protección?
   ☐ Sí
   ☐ No
   ☐ Parcialmente

Apéndice B. Listas de Verificación 1

Listas de verificación de cumplimiento de políticas y procedimientos de seguridad

El objetivo de las listas de verificación es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
1.1	¿El procedimiento de altas y bajas documenta quién autoriza el acceso?			
1.2	¿Se establecen plazos para la baja de usuarios inactivos o desvinculados?			
1.3	¿Se aplican contraseñas con longitud y complejidad adecuadas?			
1.4	¿Se exige el cambio periódico de contraseñas?			

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
2.1	¿Existe una política de protección de datos personales?			
2.2	¿Se definen responsabilidades en el			

	tratamiento de datos sensibles?			
2.3	¿Se identifican los sistemas donde se almacena información personal?			

Ítem	**Verificación**	**Cumple (✓)**	**No cumple (✗)**	**Observación**
3.1	¿Existe un plan de continuidad documentado y vigente?			
3.2	¿El plan contempla responsables, tiempos de recuperación y escenarios críticos?			
3.3	¿Se realizan pruebas del plan de continuidad o recuperación?			

Ítem	**Verificación**	**Cumple (✓)**	**No cumple (✗)**	**Observación**
4.1	¿Las políticas están aprobadas y firmadas por la alta dirección?			
4.2	¿Se incluye una política de sanciones ante incumplimientos de seguridad?			

4.3	¿Se establece un procedimiento para gestión de incidentes?			
4.4	¿Se han actualizado las políticas en el último año?			

Apéndice C. Encuesta 1

Encuesta de percepción sobre riesgos de seguridad de la información

El objetivo de la encuesta es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Entidad	
Nombre	
Puesto	
Fecha	

1. ¿Ha detectado prácticas inseguras en el uso de dispositivos corporativos?
   ☐ Sí
   ☐ No

2. ¿Con qué frecuencia comparte información sensible por correo o WhatsApp?
   ☐ Frecuentemente
   ☐ Ocasionalmente
   ☐ Nunca

3. ¿Ha recibido capacitación reciente sobre seguridad de la información?
   ☐ Sí
   ☐ No

4. ¿Utiliza contraseñas seguras (largas, combinadas, únicas)?
   ☐ Siempre
   ☐ A veces
   ☐ Nunca

5. ¿Qué tan probable considera que ocurra una filtración de datos por error humano?
   ☐ Alta
   ☐ Media
   ☐ Baja

6. ¿Cuál sería el impacto si se perdiera acceso a un dispositivo sin respaldo ni cifrado?
   ☐ Crítico

☐ Medio
☐ Bajo

7. ¿Qué tan protegido cree que está el entorno digital de la empresa actualmente?
   ☐ Bien protegido
   ☐ Medianamente protegido
   ☐ Mal protegido

8. ¿Ha visto casos donde varios usuarios comparten una misma cuenta o acceso?
   ☐ Sí
   ☐ No
   ☐ No lo sé

Apéndice D. Guía de Entrevista 2

Entrevista para evaluación de accesos y privilegios de usuarios

El objetivo de la entrevista es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Entidad	
Nombre del entrevistado	
Puesto del entrevistado	
Fecha	

1. ¿Cuántos niveles de acceso están definidos actualmente en los sistemas? (Ej.: lectura, edición, administración)
   ☐ Solo lectura
   ☐ Edición o modificación
   ☐ Administración total
   ☐ Acceso temporal (por proyectos o tareas específicas)
   ☐ Otro (especifique): _____

2. ¿Los accesos se asignan con base en el rol, el área o criterios personalizados?
   ☐ Rol
   ☐ Área
   ☐ Otro (especifique): _____

3. ¿Existe un registro formal y actualizado de los accesos por usuario?
   ☐ Sí
   ☐ No
   ☐ Parcialmente

4. ¿Todos los usuarios utilizan credenciales únicas?
   ☐ Sí
   ☐ No
   ☐ Algunos

5. ¿Con qué frecuencia se revisan los permisos de acceso en los sistemas críticos?
   ☐ Mensual
   ☐ Trimestral
   ☐ Anual
   ☐ Nunca

6. ¿Existe un procedimiento documentado para dar de baja accesos cuando alguien deja la empresa?
   ☐ Sí
   ☐ No

7. ¿Quién autoriza los accesos y controla los cambios de permisos?
   ☐ El área de TI
   ☐ El jefe directo o supervisor
   ☐ Recursos Humanos
   ☐ Gerencia general
   ☐ Es un proceso compartido entre varias áreas
   ☐ No hay una persona o área definida
   ☐ Otro (especifique): _____

8. ¿Se auditan los accesos mediante bitácoras o registros de eventos?
   ☐ Sí
   ☐ No
   ☐ No se sabe

Apéndice E. Listas de Verificación 2

Lista de verificación de cumplimiento normativo y regulatorio

El objetivo de las listas de verificación es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
1.1	¿Existe una política formal de seguridad de la información firmada por la alta dirección?			
1.2	¿Está vigente y actualizada la política de protección de datos personales?			
1.3	¿Se definen claramente los roles y responsabilidades en el tratamiento de datos sensibles?			
1.4	¿Se han socializado estas políticas entre los empleados con acceso a datos críticos?			

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
2.1	¿Se cumple con los principios de la Ley 8968 sobre protección de datos personales?			
2.2	¿Se han implementado controles alineados con los dominios de la ISO/IEC 27001:2022?			
2.3	¿Existen registros que evidencien acciones correctivas ante desviaciones legales o normativas?			
2.4	¿Se incluye el cumplimiento normativo dentro de los procesos de auditoría interna?			

Ítem	Verificación	Cumple (✓)	No cumple (✗)	Observación
3.1	¿Se cuenta con procedimientos documentados de alta, baja y modificación de usuarios?			

3.2	¿Existe trazabilidad de la aprobación de accesos por parte de responsables autorizados?			
3.3	¿Están documentados y vigentes los planes de continuidad y recuperación ante desastres?			
3.4	¿Los incidentes de seguridad se registran y gestionan conforme al procedimiento formal?			

Apéndice F. Guía de Entrevista 3

Entrevista para validación de controles propuestos por riesgo

El objetivo de la entrevista es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Entidad	
Nombre de los entrevistados	
Puesto de los entrevistados	
Fecha	

Riesgo	
Controles propuestos	

1. ¿Considera que los controles propuestos para el riesgo son adecuados para mitigarlo en el contexto de Auxadi Costa Rica?
   ☐ Sí, son adecuados
   ☐ Parcialmente, requieren ajustes
   ☐ No, no son adecuados
   Observaciones / Ajustes sugeridos: _____

2. ¿Estos controles pueden implementarse de forma práctica con los recursos, sistemas y procesos actuales de Auxadi?
   ☐ Sí, totalmente viables
   ☐ Parcialmente viables, requieren apoyo adicional
   ☐ No viables con las condiciones actuales
   Observaciones / Condiciones necesarias: _____

3. ¿Los controles propuestos son suficientes para cubrir el riesgo, o sería necesario incluir controles adicionales?
   ☐ Suficientes
   ☐ Suficientes con pequeños ajustes

☐ No son suficientes, se requiere control adicional
Controles adicionales sugeridos: _____

4. ¿Qué detalles prácticos o medidas específicas considera necesarios para que los controles seleccionados funcionen en la realidad de Auxadi?
   ☐ Políticas internas adicionales
   ☐ Configuración técnica o herramienta específica
   ☐ Capacitación del personal
   ☐ Procesos de supervisión y monitoreo
   ☐ Otro: _____
   Observaciones: _____

5. Conclusión grupal sobre el riesgo y sus controles asociados:
   ☐ Validado
   ☐ Validado con ajustes
   ☐ No validado
   Notas finales: _____

Apéndice G. Guía de Entrevista 4

Entrevista para validación de requerimientos por política y procedimiento

El objetivo de la entrevista es para fines académicos, por lo que las respuestas serán de carácter confidencial.

Los resultados se utilizarán para desarrollar la propuesta del proyecto final de graduación.

Entidad	
Nombre de los entrevistados	
Puesto de los entrevistados	
Fecha	

Política / Procedimiento	
Requerimientos tecnológicos	
Requerimientos humanos	
Requerimientos financieros	

1. ¿Los recursos tecnológicos descritos (infraestructura, sistemas, licencias, herramientas o integraciones) reflejan de forma precisa los medios actuales con los que cuenta Auxadi Costa Rica para cumplir esta política o procedimiento?
   ☐ Sí, reflejan la realidad actual
   ☐ Parcialmente, se requiere actualización o ampliación
   ☐ No, existen brechas tecnológicas importantes
   Observaciones / Ajustes sugeridos: _____

2. ¿El personal asignado (áreas de TI, Cumplimiento, Talento Humano, Gerencia u otros) dispone de la capacidad, formación y tiempo necesario para mantener esta política o procedimiento?
   ☐ Sí, el recurso humano es suficiente y capacitado

☐ Parcialmente, requiere capacitación o reasignación de funciones
☐ No, se necesitan nuevos roles o personal adicional
Observaciones / Recomendaciones: _____

3. ¿Los costos asociados (licencias, mantenimiento, capacitación, hardware o auditorías) pueden cubrirse con el presupuesto actual de la empresa o requieren inversión adicional?
   ☐ Sí, se cubren con el presupuesto actual
   ☐ Parcialmente, se requiere ampliación o ajuste de presupuesto
   ☐ No, implica una inversión adicional significativa
   Observaciones / Condiciones financieras: _____

4. Conclusión grupal sobre la validación del análisis de requerimientos:
   ☐ Validado
   ☐ Validado con ajustes
   ☐ No validado
   Notas finales: _____