UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

SEMINARIO DE GRADUACIÓN

Para optar por el grado de Bachillerato en Ingeniería en Informática

PROPUESTA PARA GESTIONAR LA CERTIFICACIÓN EN LA NORMA ISO/IEC 27001:2013 DE LA EMPRESA POPULAR PENSIONES, UBICADA EN SAN JOSÉ.

CHARLENE WILSHIRE CHARLES

AUTORA

CARLOS H. AGUILAR MORA

TUTOR

OLMAN NÚÑEZ PERALTA

LECTOR

San José, Costa Rica

ABRIL, 2020

DEDICATORIA

A Dios, por darme la oportunidad de continuar con mis estudios, guiarme en cada paso y llegar a este punto.

En especial a mi esposo Leonardo Barrios, por su amor, apoyo incondicional y ánimos que me da día con día para ser una mejor persona, esforzada y afrontar las cosas buenas y malas de la vida con optimismo.

A mi madre Dianisia por su ejemplo, dedicación y amor brindado; a mi hermana Shaneen, por estar pendiente y motivarme siempre con mis estudios. A mi padre Elvis (Q.E.P.D.), por sembrar en los inicios de la carrera.

Esto es por y para ustedes, los amo.

Charlene Wilshire Charles

AGRADECIMIENTOS

Quiero agradecer principalmente a Dios por brindarme la salud, el entendimiento y los recursos necesarios para lograr culminar esta etapa de mi vida.

A mi esposo Leonardo Barrios, quien ha sido mi apoyo incondicional y por siempre motivarme a seguir adelante con mis sueños.

A mi madre, quien con su ejemplo y amor me enseñó que nunca es tarde para cumplir las metas; a mi familia y amigos que de una u otra manera siempre creyeron en mí.

A mi tutor, Máster Carlos H. Aguilar, y a la directora de la carrera, Máster Olda Bustillos, por brindar su tiempo y conocimiento a lo largo de este proceso.

Charlene Wilshire Charles

CONTENIDO

LISTA DE ILUSTRACIONES Y TABLAS

Ilustraciones

Tablas

CAPÍTULO 1: INTRODUCCIÓN

Las amenazas en los activos de información de las empresas van creciendo día a día, cada vez son más atractivos para las personas maliciosas, con el fin de obtener información sensible y confidencial; el objetivo de apoderarse de dicha información va desde dañar la imagen de la empresa hasta sustraer –potencialmente- dinero. La tecnología avanza y con ella los ataques; se presentan distintos tipos de fraude, ya sean internos o externos, por ello, se debe tomar conciencia sobre cómo abarcar de forma holística la seguridad de la información en el negocio.

La información se ha convertido en un activo vital para las instituciones, la cual forma parte fundamental para el funcionamiento y el alcance de sus objetivos. Según Rodríguez (1995) "La información debería ser tratada como un recurso estratégico" (p.17), debido a esta importancia, las organizaciones necesitan proteger su información para asegurar que esté disponible cuando se necesite, que sea íntegra y confiable. La seguridad de la información se ha convertido en un enfoque renovado para todas las organizaciones debido al masivo procesamiento que tiene impacto directo en la economía mundial y competitividad en el mercado, por lo que Operadora de Planes de Pensiones Complementarias del Banco Popular no está exenta de esta realidad.

La institución, al gestionar de una forma eficaz la seguridad de la información, evita las inversiones mal dirigidas o desproporcionadas, que se producen por: contrarrestar amenazas sin una evaluación previa, desestimar riesgos, falta de contramedidas, implantar controles desproporcionados y de un coste más elevado del necesario, falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, entre otros motivos.

En virtud de lo anterior, es importante contar con un Sistema de Gestión de la Información en la entidad, para identificar los riesgos, amenazas y vulnerabilidades a los que puedan estar expuestos los activos de información organizacionales y así contar con un nivel de madurez adecuado de seguridad de la información.

Planteamiento del problema

Al no existir un Sistema de Gestión de Seguridad de la Información en Popular Pensiones, puede exponer a la empresa a múltiples vulnerabilidades, provocando la posible materialización de los siguientes riesgos:

Mal uso de la información de los afiliados y de la Operadora por parte de terceros.

No aplicar de forma adecuada la normativa, controles y procedimientos del manejo de la información, puede provocar incumplimientos de las buenas prácticas internacionales en esta materia, como las contenidas en la norma ISO/IEC 27001:2013.

Alteración, pérdida o divulgación de la información por deficiencias en la gobernabilidad de seguridad.

Insuficiencia en la aplicación y monitoreo de controles de seguridad, en cuanto a políticas, procedimientos, guías y directrices en la organización.

Robo de la información al no contar con los controles de seguridad apropiados, según los establecidos en la norma.

La norma ISO/IEC 27001:2013 abarca de forma holística catorce dominios dentro de la organización; procesos que van desde la alta gerencia hasta la seguridad física del edificio, si no se tienen establecidos los procedimientos y políticas para cada control se puede omitir gestiones importantes, por consiguiente, provocar una brecha de información.

Materialización de riesgos de Tecnología de Información por inadecuada gestión de los activos de información.

La definición de los activos de información, será de beneficio para identificar responsables, probabilidad de impacto financiero, legal, económico o daño de imagen; clasificar la información ya sea en confidencial, uso interno o uso público, así como especificar los custodios de la información y el periodo de almacenamiento.

Objetivo General

Elaborar una propuesta para la gestión de la certificación en la norma ISO/IEC 27001:2013 de la empresa Popular Pensiones.

Objetivos Específicos

1. Diagnosticar el estado actual del negocio, basado en las mejores prácticas establecidas en la norma ISO/IEC 27001:2013, detallando el grado de madurez y valorando lineamientos existentes de seguridad de la información, identificando puntos de mejora y el nivel de cumplimiento.

2. Determinar las brechas existentes según lo estipulado en la norma ISO/IEC 27001:2013; identificando las acciones para la gestión y cierre de brechas entre el estado actual y el requerido.

3. Elaborar una propuesta para la atención de las brechas encontradas, estableciendo las actividades, recomendaciones y recursos necesarios para la atención del cierre de brechas.

4. Analizar el costo/beneficio en el cual se reflejen las ventajas de la aplicación de las buenas prácticas establecidas en la norma ISO/IEC 27001:2013, así como el costo asociado correspondiente a la implementación para la empresa, determinando los recursos necesarios para la ejecución del plan de acción.

Justificación

Al implementar un Sistema de Gestión de Seguridad de la Información en la institución, el cual mitigue riesgos tecnológicos y de la información del negocio, considerando aspectos de amenazas, riesgos y vulnerabilidades que puedan poner en peligro la confidencialidad, integridad

y disponibilidad de la información durante todo su ciclo de vida, se pretende asegurar de forma razonable la protección de los activos de información del negocio y de los afiliados, así como garantizar el cumplimiento regulatorio en el marco normativo ISO/IEC 27001:2013.

Beneficios:

- Oportunidad de lograr la certificación en la norma ISO/IEC 27001:2013, para distinguirse en el mercado (siendo la primera operadora de pensiones complementarias del país en obtener la certificación).

- Dar seguridad a los afiliados de que la información que administra la organización está siendo gestionada de forma segura, aplicando los controles establecidos en la norma.

- Contar con un inventario de activos de información en la Dirección de Tecnología de Información, donde se tendrán identificados los responsables, exposición de riesgos, formato del activo de información (digital – físico), tiempo en custodia, impactos (financiero, legal, entre otros).

Viabilidad

Apartado que demostrará si la investigación es realizable a nivel técnico, económico, temporal y operativo, con el objetivo de determinar los alcances de la investigación y mostrará que el estudio de la investigación es viable, a saber:

Viabilidad técnica

Se cuenta con recurso tanto humano como de *software* (Excel, Project) disponibles en la organización, para implementar políticas, procedimientos, controles y mejorar el sistema de gestión de seguridad de la información. Cabe resaltar que la norma ISO/IEC 27001:2013 no indica que el

cumplimiento de algún dominio o proceso de dicha norma deba ser automatizado, por lo que será de una ventaja a futuro, si la organización automatiza algún proceso de la norma.

Viabilidad económica

Para el cumplimiento de los controles establecidos en la norma, no implica la compra de algún *software*; sin embargo, requiere -como mínimo- contar con el *software* Microsoft Office y Project disponibles en la empresa. Asimismo, contar con la norma ISO/IEC 27001:2013, para efectos de retroalimentación y oportunidades de mejoras.

Viabilidad temporal

Es importante recalcar que, para lograr la certificación en ISO/IEC 27001:2013, no es necesario aplicar la norma en todos los procesos del negocio, por lo que el proyecto será enfocado en el proceso de Tecnología de Información, específicamente en la Dirección de Tecnología de Información de Popular Pensiones. En virtud de lo anterior y al tiempo establecido para la investigación, es viable.

Viabilidad operativa

La participación de la alta gerencia, así como de los Directores, es trascendental para la aplicación de un sistema de gestión de seguridad de la información en una empresa; contar con el apoyo para establecer normativas y directrices crea un compromiso en la organización y una cultura de seguridad en los empleados.

Viabilidad legal

Las regulaciones se basan en la norma ISO/IEC 27001:2013, empresas grandes o pequeñas pueden aplicar la norma, no hay restricciones, al contrario, son buenas prácticas dentro de cualquier institución; lograr la certificación genera una oportunidad en el mercado, al darle seguridad a los clientes de que su información está siendo administrada y gestionada de forma segura.

Proyección

Al tener identificados los riesgos en relación con los activos de información de la Dirección de Tecnología de Información, así como también el análisis efectuado en cuanto a cada dominio de la norma ISO/IEC 27001:2013, se establecerá el plan de acción, que constituirá controles para mitigar y reducir los riesgos que puedan materializarse y provocar pérdidas financieras o daño de imagen a la institución.

Cabe indicar que la documentación de activos y revisión de cumplimiento de la norma mediante le cuestionario, así como los controles establecidos de dicha investigación, facilitarán la mejora continua en materia de Seguridad de la Información y de la norma ISO/IEC 27001:2013 en la empresa, al efectuar el seguimiento de cumplimiento de los controles de forma periódica, se tiene la oportunidad de alcanzar y mantener la certificación de dicha norma.

CAPÍTULO II: MARCO DE REFERENCIA

Los conceptos de la presente investigación tienen como objetivo expresar el problema al que se enfrenta la organización al no contar con un sistema robusto de seguridad de la información; gracias a la norma internacional ISO/IEC 27001:2013, se puede abarcar de forma holística 14 dominios que la organización debe intervenir, para asegurar de forma razonable la información, sin importar el medio en el que se encuentre, ya sea de forma digital o física.

Rodríguez (1995) explicó que "El principal desafío (y riesgo) para la seguridad está representado no por la tecnología sino por la gente involucrada" (p.18); se concuerda con él, la organización podrá extremarse en controles, sin embargo, en la cadena de seguridad, el usuario es el eslabón más débil. Se debe crear conciencia, una cultura de seguridad de la información en la organización, para que los controles sean efectivos. Por ello, para nuestro estudio, se ha elegido la Norma ISO/IEC 27001:2013. Esta norma es un estándar de seguridad informática para implementar un Sistema de Gestión de Seguridad de la Información, que posee 14 dominios, a saber:

- Políticas de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Seguridad ligada a los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y ambiental.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Relación con proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio
- Cumplimiento.

Según la Norma ISO/IEC 27001 (2014): “Se ha preparado con el fin de proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización” (p.4). La norma guía para aplicar en el negocio las mejores prácticas a nivel internacional; se considera indispensable aplicar un Sistema de Gestión de Seguridad de la Información en la empresa, con el fin de proteger los tres grandes pilares: disponibilidad, confidencialidad e integridad de la información.

Asimismo, la Norma ISO/IEC 27001 (2014) indica que “El sistema de gestión de seguridad informática preserva dichos pilares mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente” (p.4). Por ello se considera un conjunto de políticas, procedimientos, guías y controles para identificar y minimizar los riesgos de los activos de información del negocio, con el fin proteger los pilares de la información mencionados anteriormente.

Se implementará en la organización, específicamente en la Dirección de Tecnología de Información, con el fin de establecer los controles adecuados para el resguardo de la información, tomando en cuenta los activos de información de los cuales son responsables en dicha dirección. Para efectos de este proyecto, un activo de información constituye todo lo que tenga valor para la empresa, puede estar de forma digital o física, desde un recurso tecnológico (computadoras, teléfonos, servidores, impresoras) hasta recursos almacenados de forma digital (bases de datos, documentos, registros, entre otros). Sin importar el medio en el cual se encuentre almacenado, se debe proteger ante cualquier riego.

Se diseñará un control sobre los activos de información de la Dirección de Tecnología de Información, en el cual se establecerán responsables, tipo de activo, tipos de impactos, clasificación del activo, ubicación, probabilidad de riesgo, entre otros.

La Norma ISO/IEC 27002:2009 señala:

> La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en filmes o hablada en conversación. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma debería ser siempre protegida adecuadamente. (p.4)

Tal y como lo indica la norma, la información es más que un dato y se puede presentar de distintas formas.

Debido a lo anterior, es importante protegerla ante posibles amenazas que constituyen una causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización (Norma ISO/IEC/27000:2014, p. 11); corresponde cuando aparece una acción o evento que puede vulnerar la seguridad y ocasionar perjuicio. La existencia de una vulnerabilidad en el sistema de gestión de seguridad de la información, en los activos de información o procesos, ya da cabida a una amenaza.

Existen diferentes tipos de amenazas, como lo son las internas y externas; las internas corresponden a personas dentro de la organización, pueden ser mal intencionadas al tratar de dañar un sistema o robar la información o por desconocimiento de uso, puede llegar eliminar la información. En cambio, las amenazas externas, se refieren a problemas del entorno donde está el activo o sistema, por ejemplo: sismos, desastres naturales, inundaciones, entre otros (Rodríguez, 1995, pp.38-40).

En virtud de lo anterior, la vulnerabilidad impulsa las amenazas a un sistema o activo de información, según Norma ISO/IEC/27000:2014 corresponde a “Debilidad de un activo o control, que puede ser explotado por una o más amenazas” (p.12), es considerada como una deficiencia o fallos en los controles, procesos y sistemas, que pueden ser aprovechados para afectar la seguridad de estos. Al tener identificadas las posibles amenazas sobre los activos de información y procesos, se podrán evaluar los riesgos a los que están sujetos; los cuales son “Efecto de la incertidumbre sobre los objetivos” (p. 8).

Según la norma, se considera una causa potencial para que una amenaza explote la vulnerabilidad de un activo, proceso, control o sistema y cause daño a la organización. Para evaluar el riesgo de un activo de información, se debe considerar el impacto que puede producir una amenaza y la probabilidad de que una vulnerabilidad permita la amenaza.

Las organizaciones deben conocer los riesgos a los cuales están expuestos sus activos de información y procesos en la empresa. Para ello, es importante evaluar la probabilidad de que una vulnerabilidad suceda y el impacto que pueda provocar la amenaza en el activo, ya sea económico, de imagen o legal.

Como lo indica Rodríguez, "cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos o externos, tan variables como su propio personal, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología usada" (p.148); dicha descripción es importante analizarla, se debe cuantificar el riesgo, para tomar medidas adecuadas y así poder reducirlo o inclusive en algunos casos, aceptarlo.

Es importante recalcar que la información del negocio se debe resguardar ante los riesgos, vulnerabilidades y posibles amenazas con el fin de preservar los pilares principales de seguridad de la información, como lo es la integridad de la información. Según la Norma ISO/IEC/27000:2014, "Propiedad de precisión e integridad" (p.5); se puede decir que la información no sea modificada por terceros no autorizados, desde su creación. Se debe garantizar el resguardo de validez y consistencia de la información definida como oficial o real, que no sea alterada, manipulada, ocultada o destruida, por terceros o procesos no autorizados; ya sea de forma intencional o accidental.

Por otro lado, la confidencialidad de la información según se indica en la Norma ISO/IEC/27000:2014, es la "Propiedad de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados" (p. 2), tal y como lo indica la norma, que la información esté accesible únicamente para las personas autorizadas, ya sea mediante sistemas o por medio de empleados, que estos tengan acceso únicamente a lo que necesiten para cumplir con

sus funciones. Se puede garantizar por medio de control de acceso, credenciales de acceso o cifrado de información.

Asimismo, la empresa debe garantizar lo indicado en la Norma ISO/IEC/27000:2014, en cuanto a que "la información sea accesible y utilizable a pedido por una entidad autorizada" (p. 2); según lo indicado por la norma, se refiere a que la información esté disponible cuando el personal o el negocio autorizado lo requiera. Si se cuenta con integridad y confidencialidad de la información, pero al tratar de tener acceso a un sistema o a la información se tiene problema de acceso, no será útil para la empresa. La información para que sea rentable y valiosa debe estar disponible para quien la requiera.

Como lo indica la Norma ISO/IEC/27000 (2014), "Un conjunto de medidas para preservar la confidencialidad, integridad y disponibilidad de la información, es la seguridad de la información" (p. 4); tal y como lo indica la norma, se debe contar con medidas preventivas y reactivas para resguardar la información sin importar si corresponde a información física o digital de aquí la diferencia del término *Seguridad Informática,* la cual se encarga únicamente de proteger la información digital.

Según Rodríguez (1995), "La seguridad de la información tiene como meta proteger los activos o recursos de las organizaciones de pérdida y asegurar la viabilidad de las operaciones de la organización si ésta llegara a ocurrir" (p.12), de ahí la importancia de contar con un sistema de gestión de seguridad de la información, para tener identificados los activos de información de la empresa, donde se definen: responsables, riesgos, impactos (financiero, legal, daño de imagen), valor y clasificación del activo, tiempo en custodia y áreas que posean copia de dicho activo; con el fin de resguardar la información y tener mapeada su ubicación dentro de la organización. Se tendrá un control clasificado de información de valor para el negocio y ayudará para la toma de decisiones en cuanto a controles de seguridad y planes de acción para asegurarla.

Según Rodríguez (1995), "Clasificar la información de acuerdo a su importancia para la empresa para saber qué tanta seguridad se necesita para cada tipo de información, cuánto tiempo necesita ser retenida, a quién se le dará acceso, si se requieren duplicados de la información o no,

etc.” (p.14); según lo expuesto por el autor, es indispensable darle trazabilidad a la información del negocio, para poder asegurarla ante posibles amenazas y vulnerabilidades asociadas.

CAPÍTULO III: MARCO METODOLÓGICO

Para el propósito de esta investigación se iniciará diagnosticando el estado actual del negocio. Para ello se realizará una serie de preguntas con base en los 14 dominios de la norma ISO/IEC 27001:2013, que evidenciará el estado de la empresa y su madurez en cuanto al cumplimiento de cada apartado, algunos aspectos por considerar de la Norma ISO 27001 (2014) son los siguientes:

- Políticas de Seguridad de la Información: apartado que se basa específicamente, en si la organización cuenta con una política de seguridad de la información y si tiene alcance con el sistema de gestión, tanto para personal interno como externo al negocio.

- Organización de la Seguridad de la Información: verificación de normas, directrices o políticas, relacionadas con la segregación de funciones dentro de la organización, contactos con autoridades y grupos de interés especiales en cuanto a seguridad de la información.

- Seguridad ligada a los recursos humanos: cultura en los empleados en temas de seguridad de la información, al inicio de la contratación y durante el empleo; periodicidad con que los empleados son capacitados en temas de seguridad de la información.

- Gestión de activos: existencia de un inventario de activos, orientado en activos de información, que especifique roles de los propietarios, responsables, custodios y la clasificación de la información (confidencial, uso interno o uso público).

- Control de acceso: accesos a los sistemas de información de la organización, privilegios que tienen los usuarios en cuanto a las aplicaciones y a la información, controles que regulen el riesgo sobre la incorrecta asignación de privilegios de los usuarios.

- Criptografía: normativa que regule el tránsito de la información de manera cifrada ya sea de forma interna o externa.

- Seguridad física y ambiental: lineamientos establecidos para el acceso a zonas críticas dentro de la institución y sobre la protección ante amenazas externas y ambientales.

- Seguridad de las operaciones: directrices en cuanto a la gestión de cambios en los sistemas, como lo son las bases de datos, registros de ingresos y cambios; revisión a los usuarios privilegiados en los sistemas.

- Seguridad de las comunicaciones: normas para controlar la red, responsabilidades y gestiones para asegurar la red, con el fin de asegurar de forma razonable el tránsito interno o externo de la información.

- Adquisición, desarrollo y mantenimiento de sistemas: asegurar los servicios de aplicaciones en las redes, lineamientos para la gestión de cambios en desarrollo para la puesta en producción de aplicaciones, con el objetivo de proteger los datos sin importar el ambiente donde se desarrolle.

- Relación con proveedores: directrices para el tratamiento, manejo y tránsito de la información de la organización con los proveedores; el deber de los proveedores al estar en contacto con información sensible.

- Gestión de incidentes de seguridad de la información: plan de tratamientos de incidentes dentro de la organización, desde su clasificación hasta el proceso de comunicación para la atención.

- Aspectos de seguridad de la información en la gestión de la continuidad del negocio: normas que definan un plan de recuperación ante desastres y la continuidad del negocio.

- Cumplimiento: identificación de leyes y normas que aplican a la organización con el fin de cumplir con los requisitos establecidos; en este apartado se aplicarán específicamente, las leyes y/o reglamentos que se basan en la administración de la información de los afiliados. (pp.16-32)

Enfoques de investigación

El enfoque de una investigación es una guía para resolver el problema de la investigación; nos ayuda a plantear y a elaborar la estrategia para llevar a cabo el estudio de la investigación. Según Hernández, R.; Fernández, C.; Baptista, P. (2014) citando a Grinnell (1997), los enfoques:

1. Llevan a cabo la observación y evaluación de fenómenos.
2. Establecen suposiciones o ideas como consecuencia de la observación y evaluación realizadas.
3. Demuestran el grado en que las suposiciones o ideas tienen fundamento.
4. Revisan tales suposiciones o ideas sobre la base de las pruebas o del análisis.
5. Proponen nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar las suposiciones e ideas o incluso para generar otras. (p.4)

Según lo expuesto, los enfoques ayudan a establecer la estructura, métodos, procesos y supuestos para evaluar los problemas planteados en la investigación, con el fin de analizar los datos mediante la observación, descripción, cuestionarios y evaluaciones, para obtener el conocimiento adecuado y sustentar la investigación. El cómo obtener los datos, es donde se orientan los tipos de enfoques de la investigación; asimismo, da apoyo al proceso del diseño y elección de los instrumentos a utilizar para recolectar la información.

Según Cauas (2015), en los enfoques metodológicos se distinguen dos tipos:

- Enfoque cuantitativo: aquel que utiliza preferentemente información cuantificable (medible), sigue una estructura o proceso; debido a su estructura, los datos son fáciles de medir.

- Enfoque cualitativo: explora para encontrar respuesta de la investigación, cuyo análisis se dirige a lograr descripciones detalladas de los fenómenos estudiados. Son investigaciones participativas y cuentan con puntos de vistas, entre otras características. (p. 2)

Enfoque cuantitativo

El enfoque cuantitativo sigue una estructura, se realiza de forma ordenada para obtener los datos del estudio mediante un cuestionario de preguntas cerradas, con el fin de probar la hipótesis de la investigación, establece con exactitud los datos, son confiables para el estudio.

En dicho enfoque es más fácil medir los resultados, ya que sigue una estructura y mediante la recolección y análisis de datos se prueban las hipótesis planteadas. Los datos se analizan de forma numérica y objetiva a través de una muestra de la población por investigar. Cabe indicar que la medición y planeación de los datos son puntuales; asimismo, es importante destacar que el investigador debe contar con una postura de neutralidad, pues se requiere que los datos obtenidos sean íntegros para su medición.

Hernández et al. (2014) indican “La investigación cuantitativa ofrece la posibilidad de generalizar los resultados más ampliamente, otorga control sobre los fenómenos, así como un punto de vista basado en conteos y magnitudes.” (p.15). Tal y como lo establecen, se debe ser objetivo, con el fin de no alterar los resultados, no ser condescendientes y obtener los resultados de forma transparente, para definir el estado actual del objeto por investigar.

Enfoque cualitativo

Este enfoque se caracteriza por recolectar la información y analizar los datos para establecer las preguntas durante la investigación o generar nuevas interrogantes. Los datos se pueden recolectar en campo, observando el entorno, por medio de interpretación. Es un estudio basado en la subjetividad, no generaliza los resultados, utiliza cuestionarios abiertos y explora en el campo para encontrar las respuestas. Según Hernández, C. (2014) “este tipo de investigación no tiene en un principio un concepto claro de lo que se estudia ni una hipótesis que después se pueda validar. Los conceptos y las hipótesis se van formulando a lo largo de la propia investigación” (p.189).

Enfoque de la investigación seleccionado

La norma ISO/IEC 27001:2013 posee 14 dominios de diferentes ámbitos, comprenderá desde seguridad física del negocio hasta sistemas de información y se debe abarcar de forma holística con el fin de analizar las respuestas y evidenciar el grado de consecución de cada uno. Para ello se aplicará una serie de cuestionarios, que deben continuar una estructura para obtener resultados concretos del cumplimiento de la norma y comprobar la hipótesis.

Por tales motivos, el enfoque de la investigación seleccionado es el enfoque *Cuantitativo*. Dicho enfoque se utilizará para tener una visión clara de cumplimiento del negocio en cuanto a la norma y de este modo, poder establecer el plan de acción que será una guía para gestionar la certificación en la empresa. Bajo este concepto se darán a conocer las oportunidades de mejora y acciones que se entregarán a la institución para que les permita optar por la certificación en la norma ISO/IEC 27001:2013.

Tipos de investigación

Según el alcance de la investigación y el problema que se requiera resolver, existen distintos tipos de investigación que se pueden aplicar al estudio, el alcance depende de la estrategia de la investigación; los más utilizados se clasifican en:

- Investigación Descriptiva.
- Investigación Exploratoria.
- Investigación Explicativa.

El definir el tipo de investigación depende de dos factores principales, según Hernández et al. (2014):

> a) El conocimiento actual del tema de investigación que nos revele la revisión de la bibliografía
>
> b) La perspectiva que el investigador pretenda dar a su estudio (p.98).

En la etapa de obtención de los datos, se definirá el tipo de estudio que se ejecutará, con el fin de identificar los métodos para obtener los resultados, por ejemplo, si la estrategia por utilizar será descriptiva, exploratoria o explicativa.

Investigación descriptiva

Se define por especificar las propiedades y características importantes del objeto que se analice. Se utiliza en tipos de estudio que involucren: casos, encuestas, desarrollo, entre otros. Describe tendencias de un grupo o población. Según Cauas (2015) "Este tipo de estudios buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que se sometido [sic] a análisis." (p.6). Implica mostrar con precisión los datos y características del objeto en estudio.

Es importante señalar que la investigación descriptiva se enfoca en caracterizar los objetos de la investigación, con el fin de que cada ente pueda ser medible en el análisis y poder describir las variables del estudio.

Investigación exploratoria

El alcance de la investigación aborda estudios pocos conocidos, pretende aclarar y delimitar el problema, se basa en extensas revisiones de libros, reportajes y consultas con expertos en la materia. Se aplica a estudios que no utilizan instrumentos de recolección de datos, solo para identificar las variables. Según Sáez (2017) "tiene la ventaja de aproximar y familiarizar al investigar con un objeto de estudio que era desconocido".

Este tipo de investigación es funcional en estudios de campos poco conocidos, requiere mucha investigación, con la finalidad de contar con un primer conocimiento (primeras instancias) de manera superficial, por ser tan poco conocido el objeto por investigar.

Investigación explicativa

Los estudios explicativos buscan explicar por qué ocurren las causas y cómo se revelan; es el tipo de investigación más estructurada y brinda el sentido de comprender las causas por investigar. Según Cauas, D. (2015), “tienen como fin el explicar la causa de un fenómeno, y/o insertar el fenómeno en un contexto teórico, de modo que permita incluirlo en una determinada generalización” (p. 10).

Tipo de investigación seleccionada

La investigación mostrará con precisión la situación actual de la empresa con base en el cumplimiento de la norma ISO/IEC 27001:2013, con el fin de realizar una propuesta para que puedan gestionar la certificación en dicha norma. Hernández et al. (2014) señala que “los estudios descriptivos son útiles para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación” (p.92).

De acuerdo con las categorías anteriormente descritas de los 14 dominios de la norma, se llevará a cabo el diagnóstico basado en el análisis de cumplimiento por medio de cuestionarios para cada categoría, con el fin de especificar las propiedades y características de los dominios con base en el cumplimiento de la norma; de ahí la importancia de recolectar la información para poder medir el grado de consecución de cada dominio.

Por tales motivos, el tipo de investigación seleccionado es la *Investigación Descriptiva*, con el fin de medir con precisión los datos para determinar el grado de cumplimiento de la norma. La presente investigación tiene como objetivo describir los procesos de la Dirección de Tecnología de Información en la institución, para gestionar la certificación en la norma ISO/IEC 27001:2013, con base en los 14 dominios de la norma; durante el transcurso de la investigación, se podrán añadir otras áreas de la institución que están asociadas con los dominios, por ejemplo, el área de recursos humanos.

Hipótesis de la investigación

¿La no existencia de un sistema de gestión en seguridad de la información en Popular Pensiones puede provocar un mal uso de la información de los afiliados y de la Operadora por parte de terceros, debido a incumplimientos de las buenas prácticas internacionales en esta materia, como las contenidas en la norma ISO/IEC 27001:2013?

La hipótesis de la investigación se basa en demostrar si la organización está preparada o no para un proceso de certificación en la norma ISO/IEC 27001:2013, tomando en cuenta los riesgos asociados al incumplimiento de las buenas prácticas establecidas en dicha norma; Hernández et al. (2014) explican que "en una investigación de enfoque cuantitativo, la hipótesis puede surgir del planteamiento del problema" (p.105) y en efecto, la hipótesis de la investigación, se basa en el problema planteado, con los riesgos asociados a los que está expuesta la empresa, si no cuentan con un sistema de gestión de seguridad de la información robusto.

Fuentes de información

Las fuentes de información nos proporcionan mecanismos para la revisión de la literatura de la investigación. Son distintos documentos que poseen información y datos útiles; asimismo, son soporte para fortalecer el conocimiento y llevar a cabo el estudio.

Para la presente investigación, se utilizarán distintos documentos con los cuales se podrán obtener los resultados deseados, con el fin de diagnosticar el estado actual del negocio en cuanto al cumplimiento de la norma ISO/IEC 27001:2013. Con el resultado del diagnóstico, se procederá a determinar las brechas existentes e identificar las acciones para la gestión y cierre de las brechas; estableciendo las actividades, recomendaciones y recursos necesarios.

Primaria

Son fuentes de información que brindan datos de primera instancia, cuya información es original, se componen principalmente de libros, obras literarias, trabajos de investigación, revistas, entre otros.

La principal fuente de información para la investigación es la norma ISO/IEC 27001:2013, con ella se abarca el estudio de los 14 dominios de la norma y se aplicará un cuestionario por cada dominio para evidenciar el cumplimiento; asimismo, se aplicará el cuestionario mediante entrevista con la Dirección de Tecnología de Información de Popular Pensiones y otras áreas involucradas en el proceso.

Secundaria

Se basa en la fuente de información primaria, reúne listado de resúmenes y referencias, sobre un tema ya conocido. Proporciona acceso a las fuentes primarias, confirma los descubrimientos y el contenido de la investigación.

Para el presente estudio, se basa en los archivos, procesos e información documentada por la empresa Popular Pensiones, para evidenciar el cumplimiento de la norma, producto del cuestionario para determinar el diagnóstico del negocio. Asimismo, se obtendrá soporte en documentos relacionados con la investigación, a saber: normativa ISO/IEC 27002:2013 “Mejores prácticas en la gestión de seguridad de la información”, normativa ISO/IEC 27003 “Guía para la implementación de un sistema de seguridad de la información”, normativa ISO/IEC 27004 “Evaluación para la seguridad de la información” y la normativa ISO/IEC 27000 “Información general y vocabulario del sistema de gestión de seguridad de la información”.

Terciarias

Se componen de bibliografías de las fuentes de información secundarias, una desventaja es que pueden ser datos desactualizados, se pueden utilizar para conocer antecedentes de la investigación.

Se tendrá soporte en las bibliografías, artículos de la norma ISO/IEC 27001:2013 y en la biblioteca virtual de la universidad.

Descripción de variables

Hernández et al. (2014) explican que una variable es "una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse" (p.105); tal y como lo indican, la investigación se basa en medir el cumplimiento de la empresa con base en la norma ISO/IEC 27001:2013, con el fin de diagnosticar al negocio; posterior al diagnóstico, se determinarán las brechas y plan de acción.

Conceptual

Definen las características de la variable mediante la descripción, "se enumeran las propiedades de interés inmediato para la investigación y se postulan las relaciones entre ellas" (Cauas, 2015, p.6).

Operacional

Según Hernández et al. (2014), citando a Hernández Sampieri et al. (2013) "Especifica qué actividades u operaciones deben realizarse para medir una variable e interpretar los datos obtenidos" (p.120); variable que mostrará lo que se debe realizar, para la recolección de los datos y las correlaciones entre variables.

Instrumental

Se indicarán los instrumentos de medición, con el cual se va a obtener los datos de la investigación, es importante definir las variables operacionales para organizar los instrumentos por utilizar.

Cuadro de variables

En el siguiente cuadro, se detallarán las variables por utilizar en la investigación.

Tabla 1. Cuadro de Variables

Objetivos Específicos	Variables	Variable Conceptual	Variable Operacional	Variable Instrumental
Diagnosticar el estado actual del negocio; basado en las mejores prácticas establecidas en la norma ISO/IEC 27001:2013, detallando el grado de madurez, valorando lineamientos existentes de seguridad de la información para identificar puntos de mejora y el nivel de cumplimiento.	Diagnóstico del negocio (indicador).	Según la norma ISO/IEC 27000, corresponde a "medida que proporciona una estimación o evaluación de atributos específicos derivados de un modelo analítico con respecto a las necesidades de información definidas".	Entrevistas Cuestionarios	Guía de Entrevista Guía de Cuestionario
Determinar las brechas existentes según lo estipulado en la norma ISO/IEC 27001:2013; donde se identificará las acciones para la gestión y cierre de brechas entre el estado actual y el requerido.	Brechas existentes de la norma.	Falencias en la organización en cuanto al cumplimiento de la norma.	Análisis del resultado del cuestionario	Guía de Cuestionario
Elaborar una propuesta para la atención de las brechas encontradas; estableciendo las actividades, recomendaciones y recursos necesarios para atender el cierre de brechas encontradas.	Propuesta para la atención de brechas.	Según el diccionario de la RAE, una propuesta es una "Proposición o idea que se manifiesta y ofrece a alguien para un fin" (Recuperado de: https://dle.rae.es/?id=UOsGs7G)	Plan para atender las brechas encontradas.	Cuadro donde se identifiquen: actividades, recomendaciones y recursos necesarios para atender las brechas.

Objetivos Específicos	Variables	Variable Conceptual	Variable Operacional	Variable Instrumental
Analizar el costo/beneficio donde se reflejen las ventajas de aplicar las buenas prácticas establecidas en la norma ISO/IEC 27001:2013, así como el costo asociado correspondiente a la implementación, para la empresa, determinando los recursos necesarios para llevar a cabo el plan de acción.	Costo/beneficio	Estudio de costos y beneficios asociados a la implementación de la propuesta de la investigación; en el cual determinará si es rentable o no para la empresa.	Análisis del costo/beneficio, identificando las ventajas, desventajas y costo de implementación.	Establecer los beneficios, costos de implementación y recursos necesarios para llevar a cabo la propuesta, asimismo, el lapso de tiempo para implementar cada actividad (corto, mediano o largo plazo)

Fuente: Elaboración propia.

Población

La empresa Popular Pensiones cuenta con distintas direcciones dentro de la organización, a saber: Gerencia General, Dirección de Negocios, Dirección de Administración, Dirección de Inversiones y la Dirección de Tecnología de Información; la presente investigación se enfocará en el proceso de la Dirección de Tecnología del negocio. Cabe indicar, que la norma ISO/IEC 27001:2013, no obliga a las organizaciones en aplicar lo establecido en todos sus procesos, pero sí se debe indicar el alcance durante la evaluación. En la siguiente ilustración, se muestra la estructura orgánica de la empresa Popular Pensiones.

Ilustración 1. Estructura Orgánica Estructura Orgánica

Fuente: https://www.bancopopular.fi.cr/Sociedades/Paginas/Popular-Pensiones.aspx

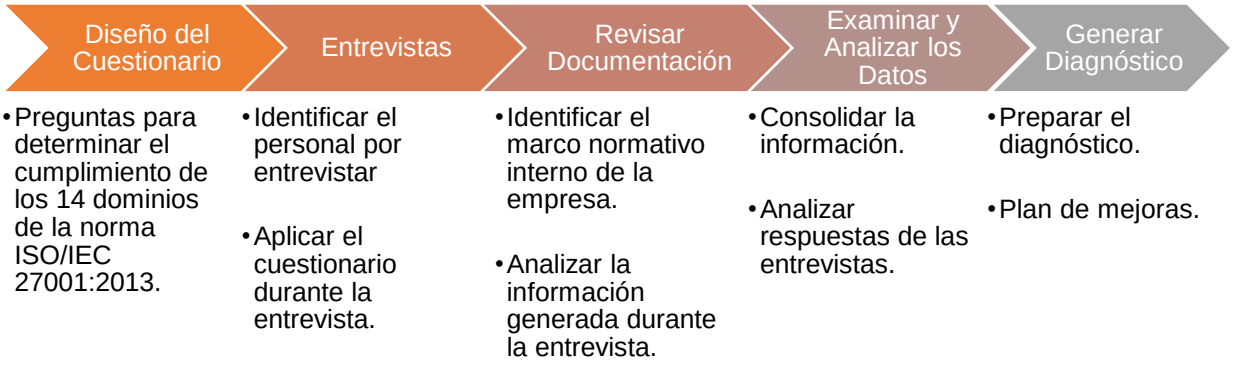
Muestra

Según lo visto en el punto anterior -Población-, Popular Pensiones cuenta con cuatro Direcciones, la aplicación de la norma se desarrollará directamente a la Dirección de Tecnología de Información de la empresa Popular Pensiones y se aplicará una entrevista a la Directora de Tecnología de Información; personal que se identificó como requerido para obtener la información, asimismo, la que tiene relación con cada dominio establecido en la norma ISO/IEC 27001:2013. Cabe indicar que, durante la entrevista, la Directora se podrá apoyar en otro recurso de la organización en caso de necesitarlo.

Instrumentos de recolección de datos

Se utilizarán dos tipos de instrumentos para la recolección de datos de la investigación, a saber: entrevista y cuestionarios. El enfoque que se utilizará se muestra en la ilustración 2.

Ilustración 2. Instrumentos de Recolección de Datos

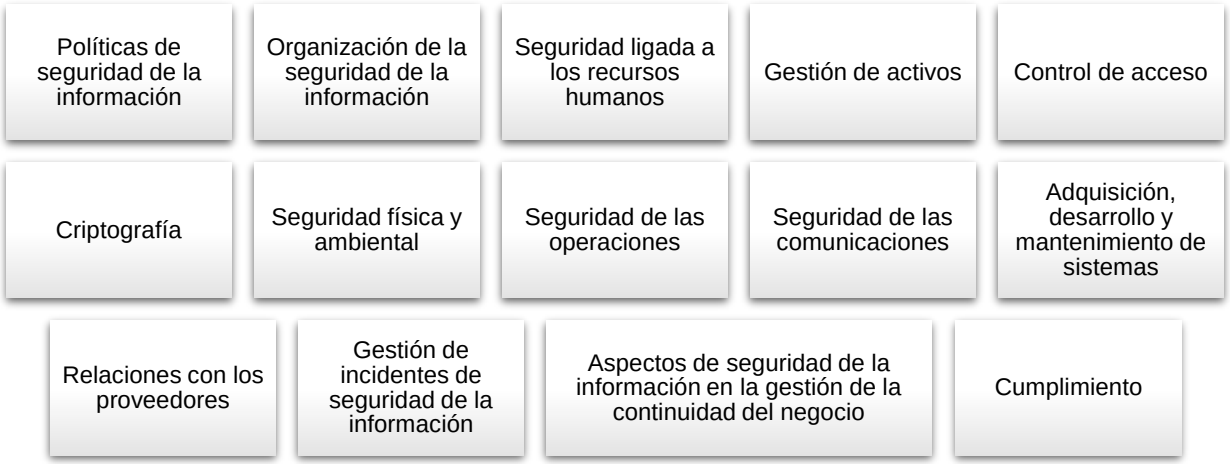


Fuente: Elaboración propia.

Cuestionario

El primer paso del diagnóstico es diseñar las plantillas por utilizar para la recolección de información; se basan en una serie de preguntas que están alineadas a los requerimientos de la norma ISO/IEC 27001:2013, de los dominios que se muestran en la Ilustración 3:

Ilustración 3. Dominios de la Norma ISO/IEC 27001:2013



Fuente: Elaboración propia con insumos de la Norma ISO/IEC 27001:2013.

Cabe indicar que dichas plantillas, ayudarán a identificar los niveles de madurez de los requerimientos y controles de la norma ISO/IEC 27001:2013.

Entrevista

Se procedió a identificar al personal requerido para obtener la información; para la selección, se consideró su relación con cada dominio de la norma. El personal seleccionado fue la Directora de Tecnología de Información de Popular Pensiones. Cabe indicar que, durante la entrevista, se le aplicará el cuestionario con el fin de recolectar la información necesaria para realizar el diagnóstico.

Revisión de documentación

Como parte del análisis, se revisará la documentación proporcionada por el personal entrevistado y los requerimientos según la norma. Esta información incluye, entre otros:

- Políticas.
- Directrices.
- Estudios preliminares.
- Reporte de sistemas.
- Procedimientos.
- Manuales.
- Registros.

Análisis FODA

Es una herramienta que puede ser aplicada en cualquier empresa, situación, persona, área o sistema de trabajo. Permite obtener un diagnóstico preciso y esencial para la toma de decisiones acorde a los objetivos y metas planteados. Reconoce el perfil o el estado actual en el que se encuentra la organización o sistema por evaluar.

Para la presente investigación, el análisis del FODA ayuda a identificar las fortalezas, oportunidades, debilidades y amenazas aplicado a la empresa correspondiente a la implementación del Sistema de Gestión de Seguridad de la Información; con el fin de obtener conclusiones sobre la forma en que el objeto en sí estudiado, podrá afrontar los cambios (oportunidades y amenazas) a partir de sus fortalezas y debilidades internas.

Según Riquelme (2016), los objetivos de la matriz FODA son:

Fortalezas: los atributos o destrezas que una industria o empresa contiene para alcanzar los objetivos.

Debilidades: lo que es perjudicial o factores desfavorables para la ejecución del objetivo.

Oportunidades: las condiciones externas, lo que está a la vista por todos o la popularidad y competitividad que tenga la industria u organización útiles para alcanzar el objetivo

Amenazas: lo perjudicial, lo que amenaza la supervivencia de la industria o empresa que se encuentran externamente, las cuales, pudieran convertirse en oportunidades, para alcanzar el objetivo. (párr.14).

Análisis GAP

Es un método para evaluar a la empresa y definir el estado actual del negocio respecto a los sistemas de información correspondiente al cumplimiento de la norma ISO/IEC 27001:2013. El resultado indica el nivel de madurez en el cual se encuentra la empresa, con el fin de definir las metas a corto, mediano o largo plazo para establecer los planes de acción.

Según Catoria F. (noviembre, 2013) “es un servicio que permite identificar la distancia existente entre la organización actual de la seguridad de la información en la empresa y las buenas prácticas más reconocidas en la industria” (párr.3), el análisis hará posible identificar

las brechas existentes y diseñar un plan de acción que permita minimizar los riesgos o falencias halladas.

Dicho análisis se utilizará en la investigación para identificar las brechas del negocio en cuanto al cumplimiento de la norma ISO/IEC 27001:2013, específicamente a los 14 dominios de la norma y poder establecer un plan de acción para minimizar los riesgos asociados al no cumplimiento de los dominios y gestionar la certificación de la norma. Para ello, se utilizará una serie de cuestionarios, con el fin de identificar el nivel de madurez en el cual se encuentra la organización.

Proceso para la recolección y análisis de datos

Dentro de las actividades de evaluación de cumplimiento, se revisarán las siguientes categorías principales de la norma: Políticas de Seguridad, Organización de la Seguridad de la Información, Seguridad en los Recursos Humanos, Gestión de Activos, Control de Acceso, Criptografía, Seguridad Física y del Entorno, Seguridad en las Operaciones, Seguridad en las Comunicaciones, Adquisición, Desarrollo y Mantenimiento de Sistemas, Relaciones con Proveedores, Gestión de Incidentes de Seguridad de la Información, Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio y Cumplimiento.

De acuerdo con las categorías anteriormente descritas, se llevará a cabo el diagnóstico basado en el análisis de la documentación de la seguridad de la información existente y del resultado de la entrevista con la representante de Tecnología de Información de la institución, se analizará la implementación y gestión de controles de seguridad de la información, con sus respectivos procesos, personas y tecnologías que dan apoyo a los controles sugeridos para el cumplimiento acorde a lo que establece un Sistema de Gestión de Seguridad de la Información bajo el estándar ISO/IEC 27001:2013.

Recolección de datos

Cuestionarios:

El primer paso del análisis de la situación actual es diseñar los cuestionarios por utilizar para la recolección y análisis de la información. Para esto se definió una plantilla que abarca los requerimientos y objetivos de control establecidos en la norma ISO/IEC 27001:2013.

La plantilla desarrollada está basada en preguntas abiertas y cerradas alineadas a los requerimientos de la ISO/IEC 27001:2013 y a identificar los niveles de madurez de los requerimientos y controles de la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2009 respectivamente.

Plantilla Análisis Objetivos de Control – ISO/IEC 27001:2013: esta plantilla recolecta la situación actual y nivel de madurez de los siguientes dominios:

- A.5 Políticas de Seguridad.
- A.6 Organización de la Seguridad de la Información
- A.7 Seguridad ligada a los recursos humanos.
- A.8 Gestión de Activos.
- A.9 Control de Acceso.
- A.10 Criptografía.
- A.11 Seguridad Física y del Entorno.
- A.12 Seguridad de las Operaciones.
- A.13 Seguridad en las Comunicaciones.
- A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas.
- A.15 Relaciones con Proveedores.
- A.16 Gestión de Incidentes de Seguridad de la Información.
- A.17 Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio.
- A.18 Cumplimiento.

<u>Entrevista con el personal</u>

Diseñada la plantilla de recolección de información, se procede a identificar el personal requerido para obtener la información y programar la entrevista con este. Para definir el personal a participar en la sesión, se consideró la relación con cada ítem por evaluar y el alcance de la

investigación. El personal elegido para la entrevista es la Directora de Tecnología de Información de la empresa.

Adicional a la ejecución de la entrevista, se considera las solicitudes de información adicional por medio de correo electrónico o telefónico, con el objetivo de aclarar puntos relacionados con el análisis, en caso de surgir alguna duda, respecto a la información brindada.

Análisis de datos

Como parte del análisis, se revisará la documentación proporcionada por el personal por entrevistar. Una vez ejecutada la entrevista, se consolidará la información en las plantillas respectivas y se procede a analizar la información recopilada, asignando a cada ítem de la plantilla el grado de satisfacción de cumplimiento y el correspondiente nivel de madurez, con el fin de brindar las recomendaciones y el plan de acción pertinente.

Nivel de madurez

Se utilizará el modelo *Information Security Management Maturity Model*, el cual define los grados de madurez según las buenas prácticas internacionales de seguridad de la información. Dicho modelo establece un nivel de 1 a 5 de acuerdo con los siguientes criterios:

Tabla 2. Descripción Nivel de Madurez

Nivel	Nombre	Descripción
1	Inicial	Existe evidencia de que la organización ha reconocido las problemáticas y acepta que deben ser corregidas. Sin embargo, no existen procesos formales.
2	Repetible	Los procesos se han desarrollado hasta el punto donde se siguen procedimientos similares por las personas que realizan tareas similares. La responsabilidad es recargada de forma individual.

3	Definido	Los procesos han sido estandarizados, documentados y comunicados mediante capacitaciones. Representan la formalización de las prácticas existentes.
4	Gestionado	La gerencia monitorea y mide el cumplimiento de los procedimientos y toma acciones en aquellos casos que se identifique que los procesos no funcionan de forma efectiva. Los procesos se encuentran en constante mejora y proveen buenas prácticas.
5	Optimizado	Los procesos han sido mejorados hasta llegar a ser buenas prácticas mediante resultados de la mejora continua y modelos de madurez con otras organizaciones. Herramientas integradas para automatizar el flujo de trabajo, promoviendo la efectividad y calidad.

Fuente: Elaboración propia con insumos de la Norma *Information Security Management Maturity Model (ISM³).*

Asimismo, se evalúa la madurez de requisitos y dominios del estándar ISO/IEC 27001:2013 mediante el análisis de tres atributos, cada uno de los cuales se valora en una escala de 1 a 5, la cual corresponde a los niveles de madurez detallados anteriormente.

Tabla 3. Evaluación nivel de madurez

	Personas	**Procesos**	**Tecnología**
Inicial	No existen recursos para atender las actividades de Seguridad de la Información.	Los procesos no están alineados.	Tecnologías de seguridad seleccionadas son compradas, pero no implementadas o configuradas apropiadamente.
Repetible	Existen roles dedicados de seguridad con un enfoque limitado.	Algunas actividades están incompletas o inconsistentes	Tecnologías de seguridad son implementadas y configuradas.
Definido	Existe un equipo centralizado y gobierno de seguridad de la información.	Las políticas y procesos están bien documentados y comprendidos.	Se implementan tecnologías de seguridad, pero con poca integración.
Gestionado	Las rendiciones de cuentas residen en un nivel ejecutivo.	Los procesos están bajo mejora continua.	Tecnologías de seguridad son entregadas y configuradas de forma efectiva.

Optimizado	Los ejecutivos asocian los indicadores de seguridad al desempeño operacional y financiero de la Institución.	Existe un vínculo directo entre las políticas de TI y la organización.	TI es utilizado en forma integral para automatizar el flujo de trabajo y mejorar la calidad.

Fuente: Elaboración propia con insumos de la Norma *Information Security Management Maturity Model (ISM³).*

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

El presente análisis consiste en la explicación de los resultados obtenidos producto de la aplicación del cuestionario a la Directora de Tecnología de Información de la empresa Popular Pensiones. La base para el análisis correspondiente toma en cuenta los datos procesados, el enfoque y el diseño de la investigación; explicará la calificación y el nivel de madurez obtenido por cada dominio establecido en el alcance de la investigación. Se identifican mejoras de cada dominio con el fin de continuar mejorando el sistema de gestión de seguridad de la información del negocio.

Resultado de la evaluación

Para cada uno de los dominios establecidos en el alcance de la investigación, se analiza la gestión desarrollada por la empresa Popular Pensiones, lo cual permite ubicar el estado de la seguridad de la información de la organización en un porcentaje de cumplimiento según lo establecido en la norma ISO/IEC 27001:2013 y un nivel de madurez según el estándar ISM^3. Se describirá el estado de preparación en seguridad de la información, incluyendo porcentaje de cumplimiento de los requisitos y controles, así como las brechas existentes.

Situación actual

A5 Políticas de Seguridad de la Información

Porcentaje de Cumplimiento	100%
Nivel de Madurez	Gestionado

Observaciones

-La empresa cuenta con varias políticas aprobadas y publicadas en la intranet, estas apoyan la gestión de seguridad de la información en el negocio.

-Se evidencia el historial de revisión de cada uno de ellos.

A6 Organización de la Seguridad de la Información

Porcentaje de Cumplimiento	71%
Nivel de Madurez	Definido

Observaciones

-Establecer, dentro de su normativa, procedimientos que especifiquen cuándo y qué autoridades o grupos de interés especiales deberían contactarse.

-Establecer formalmente normas relacionadas con la gestión del teletrabajo.

A7 Seguridad Ligada a los Recursos Humanos

Porcentaje de Cumplimiento	100%
Nivel de Madurez	Definido

Observaciones

-La empresa cuenta con varias políticas aprobadas en cuanto a la gestión de los recursos humanos, se establece periodicidad y mejora continua en cuanto a los procesos del área.

A8 Gestión de Activos

Porcentaje de Cumplimiento	80%
Nivel de Madurez	Gestionado

Observaciones

-La empresa cuenta con normativa relacionada con la gestión de activos; sin embargo, se debe definir directrices para el cumplimiento de la gestión de medios removibles.

A9 Control de Acceso

Porcentaje de Cumplimiento	100%
Nivel de Madurez	Gestionado

Observaciones

- La empresa cuenta con la normativa demandada para el cumplimiento del dominio, gestiona de forma adecuada los accesos de los usuarios.

- Crea cultura en la organización, referente a la responsabilidad de los usuarios con el uso de los sistemas.

A10 Criptografía

Porcentaje de Cumplimiento	100%
Nivel de Madurez	Definido
Observaciones	

- Establecen las pautas y métodos de controles criptográficos y sobre la gestión de llaves.

A11 Seguridad Física y Ambiental

Porcentaje de Cumplimiento	87%
Nivel de Madurez	Definido
Observaciones	

-En cuanto a la información obtenida, no se evidencian lineamientos que indiquen las directrices, procedimientos y controles para las áreas de entrega y carga.

-Existen métodos y buenas prácticas, pero no se evidencia documentación formal que defina la protección física contra las amenazas externas y ambientales.

A12 Seguridad de las Operaciones

Porcentaje de Cumplimiento	93%
Nivel de Madurez	Gestionado
Observaciones	

- La empresa cuenta con normativa relacionada con la seguridad de las operaciones; sin embargo, no se cuenta documentado un proceso formal para la gestión de cambios.

A13 Seguridad en las Comunicaciones

Porcentaje de Cumplimiento	86%
Nivel de Madurez	Gestionado
Observaciones	

- La empresa cuenta con normativa relacionada con la seguridad en las comunicaciones, tomando en cuenta controles de red, seguridad en los servicios de red transferencia de información, mensajería electrónica y acuerdos de confidencialidad.

-Se puede mejorar las directrices, estableciendo lineamientos del esquema topológicos de red, según lo establecido en la norma.

A14 Adquisición, Desarrollo y Mantenimiento de Sistemas

Porcentaje de Cumplimiento	100%
Nivel de Madurez	Gestionado

Observaciones

- La implementación del dominio por parte de Popular Pensiones se encuentra 100% realizada y alineada con lo establecido en la norma ISO/IEC 27001:2013.

A15 Relaciones con los Proveedores

Porcentaje de Cumplimiento	80%
Nivel de Madurez	Definido

Observaciones

-Con base en la documentación suministrada, se puede establecer lineamientos relacionados con la cadena de suministros de tecnología de información y comunicaciones, demandados por la norma ISO/IEC 27001:2013.

A16 Gestión de Incidentes de Seguridad de la Información

Porcentaje de Cumplimiento	100%
Nivel de Madurez	Gestionado

Observaciones

-La implementación del dominio por parte de Popular Pensiones, se encuentra 100% realizada y alineada con lo establecido en la norma ISO/IEC 27001:2013.

A17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Porcentaje de Cumplimiento	75%
Nivel de Madurez	Definido

Observaciones

- La empresa cuenta con la normativa demandada para el cumplimiento del dominio. Realizan buenas prácticas respecto a las redundancias.

-Se puede mejorar las directrices, estableciendo lineamientos de control para los diferentes ambientes.

A18 Cumplimiento

Porcentaje de Cumplimiento	88%
Nivel de Madurez	Gestionado
Observaciones	

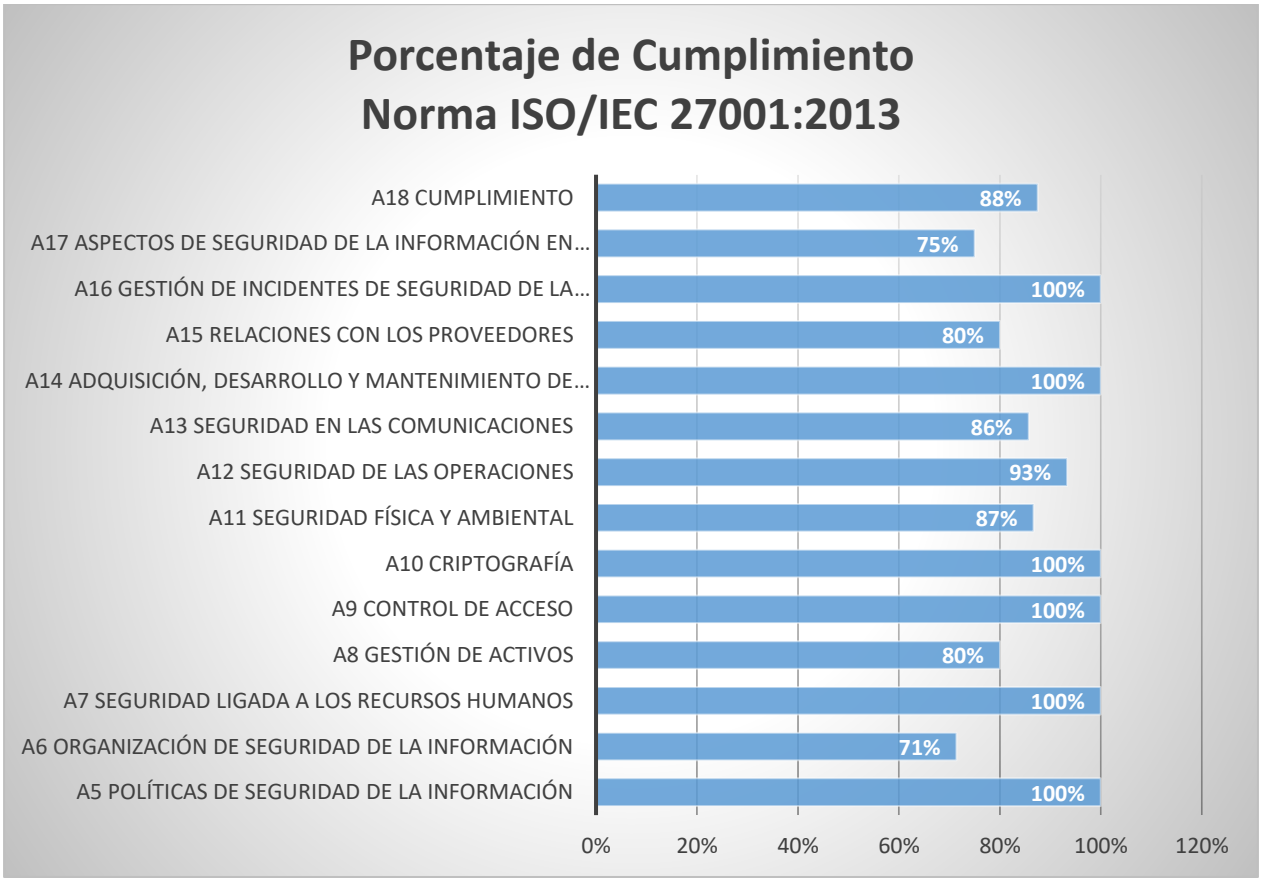
- La empresa cuenta con la normativa demandada para el cumplimiento del dominio, respecto a la norma.

-Se puede mejorar las directrices, estableciendo lineamientos formales como políticas con directrices y controles relacionados con la propiedad intelectual.

Porcentaje de cumplimiento

El porcentaje según el cumplimiento actual de la empresa con los requisitos establecidos en la norma ISO/IEC 27001:2013, es de un 90%.

Ilustración 4. Porcentaje de cumplimiento

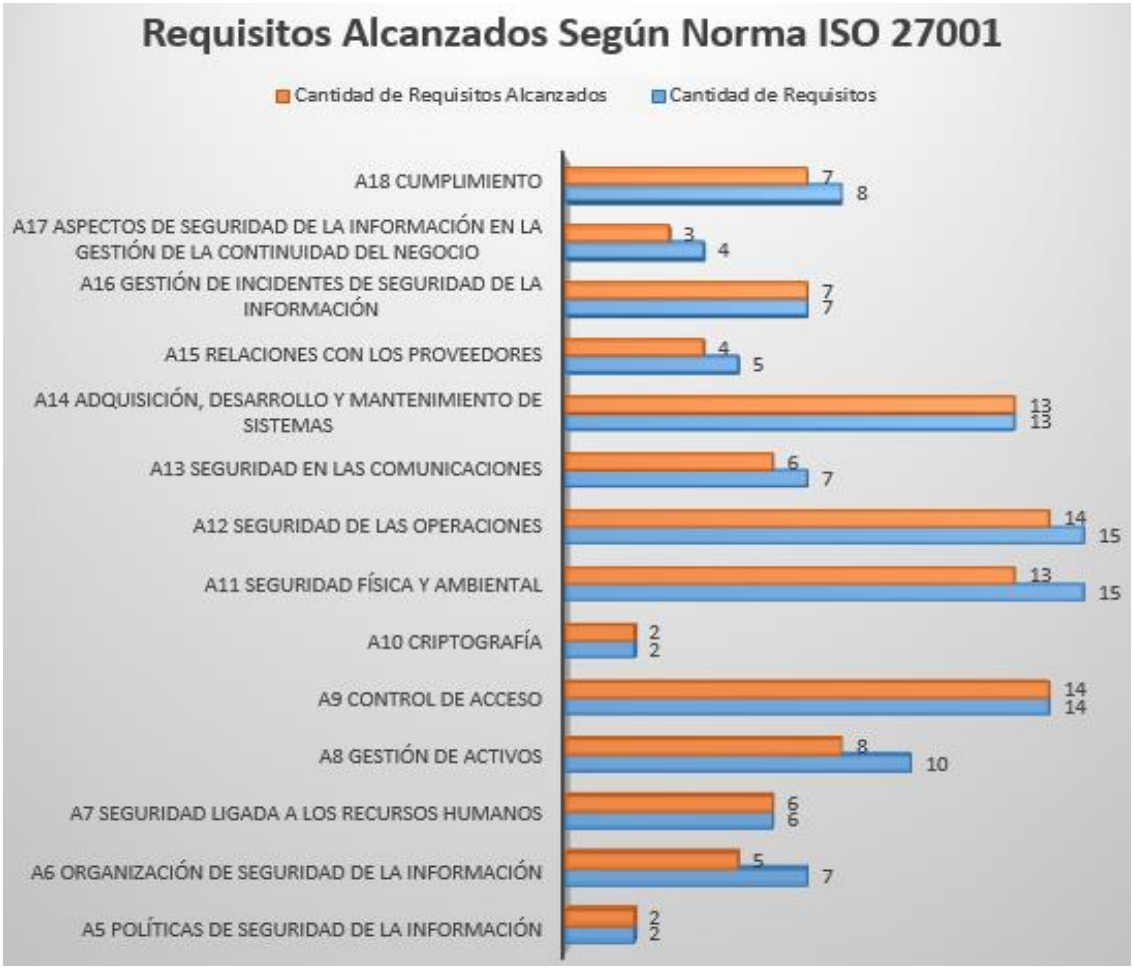


Fuente: Elaboración propia.

En la Ilustración 4 se muestra el porcentaje de cumplimiento de cada dominio de control establecido en la norma ISO/IEC 27001:2013 en la empresa Popular Pensiones. Es importante destacar que seis de los catorce dominios, tienen una calificación del 100% y no es necesaria una intervención. La calificación más baja corresponde al dominio "A6. Organización de la Seguridad de la Información" con un 71% y requiere una intervención de mejora al igual para los dominios: A18. Cumplimiento, A17. Aspectos de Seguridad de la Información, A15. Relaciones con los Proveedores, A13. Seguridad en las Comunicaciones, A12. Seguridad de las Operaciones, A11. Seguridad Física y Ambiental y A8. Gestión de Activos.

En cuanto a los requisitos alcanzados, la empresa cumple con los siguientes, basados en la norma ISO/IEC 27001:2013:

Ilustración 5. Requisitos alcanzados según norma



Fuente: Elaboración propia.

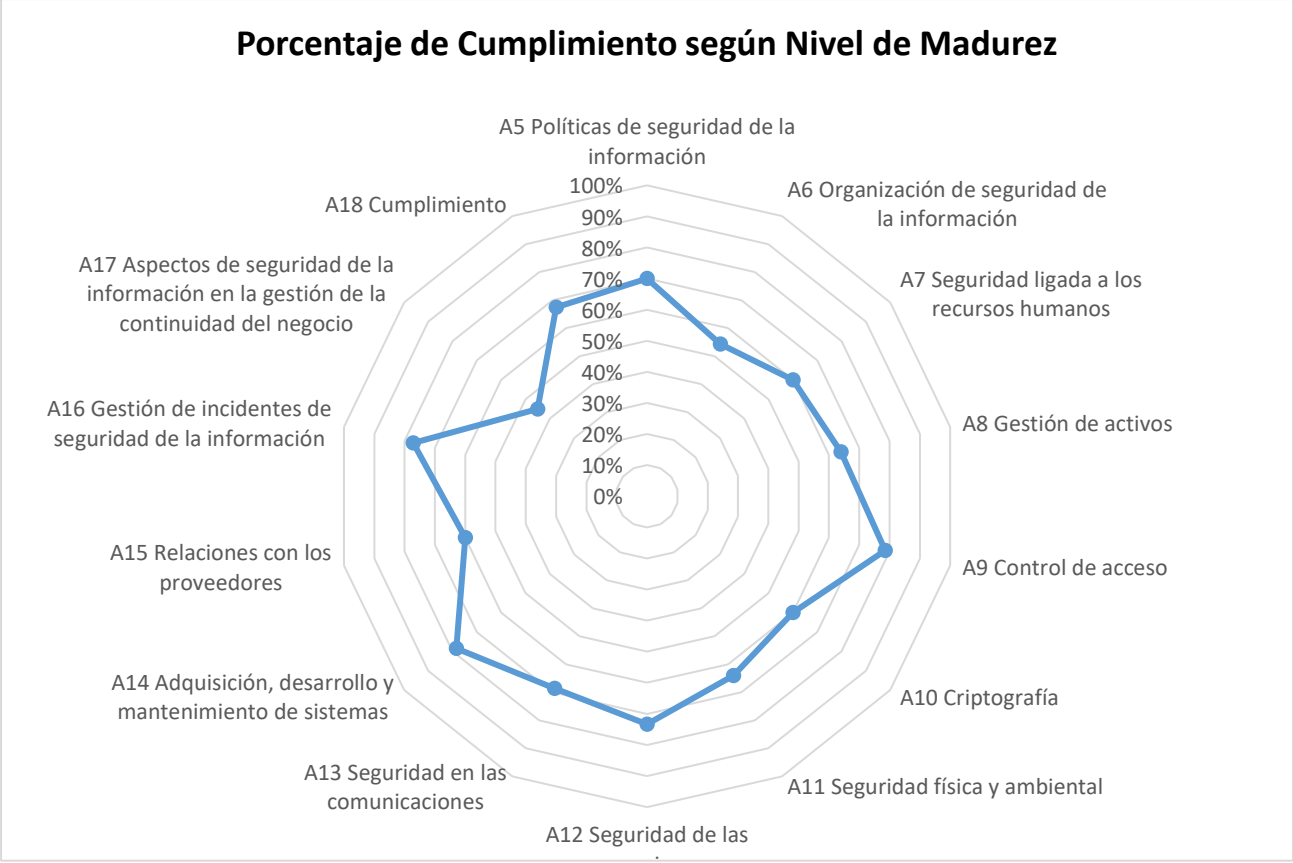
En la Ilustración 5 se muestra la cantidad de requisitos establecidos en cada dominio y su cumplimiento por parte de la empresa Popular Pensiones: un total de 115 requisitos definidos en la norma por cada dominio de control y los requisitos alcanzados por parte de la empresa con un total de 104.

Popular Pensiones cumple a cabalidad con los requisitos de los siguientes dominios: A5 Políticas de seguridad de la información, A7 Seguridad ligada a los recursos humanos, A9 Control de acceso, A10 Criptografía, A14 Adquisición, desarrollo y mantenimiento de sistemas, A16 Gestión de incidentes de seguridad de la información; no obstante, los requisitos que requieren mejoras y cuentan con debilidad son: A6 Organización de seguridad de la información, A8 Gestión de activos, A11 Seguridad física y ambiental, A12 Seguridad de las operaciones, A13 Seguridad en las comunicaciones, A15 Relaciones con los proveedores, A17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio y A18 Cumplimiento.

El porcentaje de los niveles de madurez de la empresa, según los requisitos establecidos en la norma ISO/IEC 27001:2013, es de un 68%. Dicho resultado se obtuvo mediante el análisis de tres atributos (personas – procesos – tecnología), cada uno de los cuales se valora en una escala del 1 al 5, la cual corresponde a los niveles de madurez a calificar: inicial, repetible, definido, gestionado y optimizado.

En la Ilustración 6 se muestra, por cada dominio de control, el porcentaje obtenido en la empresa Popular Pensiones respecto al nivel de madurez. El porcentaje más bajo corresponde al dominio A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio con un 45% y el dominio A6. Organización de seguridad de la información, con un 54%.

Ilustración 6. Porcentaje de cumplimiento según nivel de madurez



Fuente: Elaboración propia.

Respecto al nivel de madurez, tomando en cuenta los requisitos y dominios establecidos en el alcance de la investigación, se muestra en la Ilustración 7 el nivel de madurez por cada dominio y requisito alcanzado por la empresa Popular Pensiones; cabe indicar que se utilizó una escala del 1 al 5 del modelo *Information Security Management Maturity Model*, siendo 5 el logro más alto en cuanto al nivel de madurez del negocio.

El nivel más bajo obtenido por la empresa es un 3, para los dominios de control: A6. Organización de seguridad de la información, A7. Seguridad ligada a los recursos humanos, A10. Criptografía, A11. Seguridad física y ambiental, A15. Relaciones con los proveedores y A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Ilustración 7. Nivel de madurez por requisito y dominios

Fuente: Elaboración propia.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

El presente capítulo contiene las principales conclusiones y recomendaciones a las que se llegó tras el desarrollo de la investigación correspondiente al estudio y gestión de la norma ISO/IEC 27001:2013 en la empresa Popular Pensiones. La metodología planteada fue con base en la descripción, con el fin de medir con precisión los datos para determinar el grado de cumplimiento de la norma. La herramienta principal para la consecución de los resultados fue el cuestionario, con el cual se entrevistó al personal involucrado con los dominios por evaluar.

Conclusiones

Durante y posterior a las fases de análisis y tabulación de datos correspondientes a la evaluación de la situación actual de Popular Pensiones, respecto al cumplimiento de los dominios de la norma ISO/IEC 27001:2013 y del Sistema de Gestión de Seguridad de la Información, se detallan las siguientes conclusiones:

1. La empresa Popular Pensiones presenta una gestión de la seguridad de la información alineada a las directrices, políticas, normas, procedimientos y buenas prácticas; con un enfoque global de la seguridad de la información a nivel organizacional, sin embargo, no hace énfasis a algún proceso específico de su cadena de valor o procesos críticos. Por lo tanto, la gestión de la seguridad de la información y su orientación al cumplimiento de la norma ISO/IEC 27001:2013 no se encuentra alineada, al no tener delimitado su alcance.

2. Si bien la empresa cumple en un 90% en la cantidad de requisitos alcanzados correspondientes a la norma ISO/IEC 27001:2013, su nivel de madurez es de un 68%, lo que significa que existen normativas, directrices y controles que no están siendo aplicados y comunicados a nivel de la organización; proporcionando una falta de mejora continua y revisión de controles, con el fin de identificar las falencias.

3. Las diferentes áreas operativas de la empresa, se encuentran enteradas de las responsabilidades sujetas a la seguridad de la información; sin embargo, es importante

reforzar la capacitación, sensibilización y la divulgación de la seguridad, mejorando la cultura en la organización. Es importante recalcar a todas las áreas la concientización sobre todos los lineamientos existentes, con el fin de alinear al negocio con el Sistema de Gestión de Seguridad de la Información, ya que este debe convertirse en un tema institucional prioritario, para gestionar la norma.

4. El diagnóstico realizado corresponde al cumplimiento de los catorce dominios (controles) establecidos en la norma ISO/IEC 27001:2013 y al alcance de la presente investigación, si bien la norma también cuenta con los apartados de:

    - Contexto de la organización.
    - Liderazgo.
    - Planificación.
    - Soporte.
    - Operaciones.
    - Evaluación del desempeño.
    - Mejoras.

    La investigación se concentró en los controles de la norma, con el objetivo de evaluar inicialmente el estado actual de cada uno y así poder demostrar a la empresa, el nivel de cumplimiento y su estado de madurez. Cabe indicar que los apartados mencionados anteriormente involucran a la alta gerencia de la organización y la factibilidad para una evaluación y entrevista es muy compleja. Sin embargo, el valor agregado es exteriorizar los beneficios de gestionar el cumplimiento de la norma, el diagnóstico de los controles y el plan de acción; y así poder mostrar a la Gerencia el estado actual de su negocio.

5. Mediante el plan de acción definido para los dominios evaluados, la empresa tendrá identificados los recursos, tiempo, plantillas y responsables para la aplicación de mejoras en el sistema de gestión de seguridad de la información y atención de las brechas halladas. Asimismo, los costos asociados en la implementación de los controles faltantes o mejoras asociadas a ellos.

Recomendaciones

Las recomendaciones se basan en las brechas encontradas durante la evaluación de los 14 dominios de la norma ISO/IEC 27001:2013 y en cómo mejorar los procesos asociados a cada control de la norma, con el fin de gestionar el Sistema de Gestión de Seguridad de la Información.

1. Se recomienda definir el Sistema de Gestión de Seguridad de la Información en Popular Pensiones tomando en cuenta los procesos críticos de la cadena de valor y la visión de convertirse en la primera operadora de pensiones costarricense con certificación ISO/IEC 27001:2013 y ofrecer a sus afiliados la garantía del manejo seguro de su información. Cabe destacar que esta recomendación debe ser el punto de partida esencial para alcanzar la certificación correspondiente. Si bien la presente investigación tuvo como alcance la evaluación de los controles (dominios) de la norma, la implementación de un sistema de gestión requiere el apoyo de la alta gerencia para inculcar en la empresa el cumplimiento de dicho sistema.

2. Aunado al punto anterior, se recomienda continuar con la evaluación de la norma, específicamente con los apartados:

    - Contexto de la organización.
    - Liderazgo.
    - Planificación.
    - Soporte.
    - Operaciones.
    - Evaluación del desempeño.
    - Mejoras.

    Lo anterior, creando una política especifica que regule la gestión de la seguridad de la información en el negocio y analizar su efectividad, definiendo: qué hacer (objetivo),

cuándo (periodicidad), quiénes (responsables), dónde (contexto) y registro (almacenamiento de la evaluación).

3. Aplicar la propuesta del plan de acción de las brechas encontradas en la evaluación de los catorce dominios establecidos en el alcance de la investigación. Esto con el fin de subsanar lo hallado y mejorar los procesos asociados a los controles determinados.

   En virtud de lo anterior, se recomienda que el responsable de implementar el plan de acción, sea la Directora de Tecnología de Información del negocio, a partir del momento de entrega de la propuesta; asimismo se indica que, el tiempo estimado de dicha implementación es de 8 días hábiles.

4. Concientizar a toda la organización sobre los lineamientos existentes con el fin de alinear al negocio con el sistema de gestión de seguridad de la información, preparar al personal para cumplir con los controles establecidos en la norma ISO/IEC 27001:2013, con el objetivo de garantizar el cumplimiento; previamente, durante y posterior a la auditoría que realice el ente certificador y estar enfocados en conseguir los objetivos planteados y lo más importante, crear conciencia sobre la protección y manejo de la información en el Sistema de Gestión de Seguridad de la Información.

5. Es importante recalcar que la norma no indica que toda la organización o todos los procesos deben cumplir con los lineamientos establecidos en dicha norma, por lo que su aplicación puede estar delimitada en el alcance; al tener identificado el proceso del negocio en el alcance es sobre el proceso indicado que se efectúa la evaluación, por lo que se recomienda a la empresa Popular Pensiones, delimitar sus procesos del negocio, para centralizar la evaluación.

CAPÍTULO VI: PROPUESTA

Introducción

Las amenazas en los activos de información de las empresas van creciendo día a día, cada vez son más atractivos para las personas maliciosas, con el fin de obtener información sensible y confidencial; el objetivo de apoderarse de dicha información va desde dañar la imagen de la empresa hasta sustraer potencialmente dinero. La tecnología avanza y con ella los ataques, se presentan distintos tipos de fraude, ya sea interno o externo, por ello se debe tomar conciencia sobre cómo abarcar de forma holística la seguridad de la información en el negocio.

La institución, al gestionar de una forma eficaz la seguridad de la información, evita las inversiones mal dirigidas o desproporcionadas que se producen por: contrarrestar amenazas sin una evaluación previa, desestimar riesgos, falta de contramedidas, implantar controles desproporcionados y de un coste más elevado del necesario, falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, entre otros.

En virtud de lo anterior, es importante contar con un Sistema de Gestión de la Información en la entidad, para identificar los riesgos, amenazas y vulnerabilidades a que puedan estar expuestos los activos de información de la organización y así contar con un nivel de madurez adecuado de seguridad de la información.

Propósito

Al implementar un Sistema de Gestión de Seguridad de la Información en la empresa, que mitigue riesgos tecnológicos y de la información del negocio, considerando aspectos de amenazas, riesgos y vulnerabilidades que puedan poner en peligro la confidencialidad, integridad y

disponibilidad de la información durante todo su ciclo de vida, se pretende asegurar de forma razonable la protección de los activos de información del negocio y de los afiliados, así como garantizar el cumplimiento regulatorio en el marco normativo ISO/IEC 27001:2013.

Beneficios

- Oportunidad de lograr la certificación en la norma ISO/IEC 27001:2013, para distinguirse en el mercado (siendo la primera operadora de pensiones complementarias del país en obtener la certificación).

- Dar seguridad a los afiliados de que la información que administra la organización está siendo gestionada de forma segura, aplicando los controles establecidos en la norma.

- Contar con un inventario de activos de información en la Dirección de Tecnología de Información, en el cual se tendrán identificados los responsables, exposición de riesgos, formato del activo de información (digital – físico), tiempo en custodia, impactos (financiero, legal, entre otros).

Objetivo general

Elaborar una propuesta para la gestión de la certificación en la norma ISO/IEC 27001:2013 de la empresa Popular Pensiones.

Objetivos específicos

1. Diagnosticar el estado actual del negocio, basado en las mejores prácticas establecidas en la norma ISO/IEC 27001:2013, detallando el grado de madurez y valorando lineamientos existentes de seguridad de la información, identificando puntos de mejora y el nivel de cumplimiento.

2. Determinar las brechas existentes según lo estipulado en la norma ISO/IEC 27001:2013; identificando las acciones para la gestión y cierre de brechas entre el estado actual y el requerido.

3. Elaborar una propuesta para la atención de las brechas encontradas, estableciendo las actividades, recomendaciones y recursos necesarios para la atención del cierre de brechas.

4. Analizar el costo/beneficio en el cual se reflejen las ventajas de la aplicación de las buenas prácticas establecidas en la norma ISO/IEC 27001:2013, así como el costo asociado correspondiente a la implementación para la empresa, determinando los recursos necesarios para la ejecución del plan de acción.

Proyecciones

Producto del análisis efectuado en cuanto al cumplimiento de cada dominio de la norma ISO/IEC 27001:2013, se establecerá el plan de acción, que constituirá controles para mitigar y reducir los riesgos que puedan materializarse, provocando pérdidas financieras o daño de imagen a la institución.

Cabe indicar que la documentación de activos y revisión de cumplimiento de la norma mediante el cuestionario, así como los controles establecidos de dicha investigación, facilitará la mejora continua en materia de Seguridad de la Información y de la norma ISO/IEC 27001:2013 en la empresa; al efectuar el seguimiento de cumplimiento de los controles de forma periódica, se tiene la oportunidad de alcanzar y mantener la certificación de dicha norma.

Dominios de la norma ISO/IEC 27001:2013 evaluados

Se iniciará diagnosticando el estado actual del negocio. Para ello se realiza una serie de preguntas con base en los 14 dominios de la norma ISO/IEC 27001:2013, que evidencian el estado

de la empresa y su madurez en cuanto al cumplimiento de cada apartado, algunos aspectos por considerar de la Norma ISO/IEC 27001:2013 son los siguientes:

- Políticas de Seguridad de la Información: apartado que se basa, específicamente, en si la organización cuenta con una política de seguridad de la información y si tiene alcance con el sistema de gestión, tanto para personal interno como externo al negocio.

- Organización de la Seguridad de la Información: verificación de normas, directrices o políticas, relacionadas con la segregación de funciones dentro de la organización, contactos con autoridades y grupos de interés especiales en cuanto a seguridad de la información.

- Seguridad ligada a los recursos humanos: cultura en los empleados en temas de seguridad de la información, al inicio de la contratación y durante el empleo; periodicidad en que los empleados son capacitados en temas de seguridad de la información.

- Gestión de activos: existencia de un inventario de activos, orientado en activos de información, que especifique roles de los propietarios, responsables, custodios y la clasificación de la información (confidencial, uso interno o uso público).

- Control de acceso: accesos a los sistemas de información de la organización, privilegios que tienen los usuarios en cuanto a las aplicaciones y a la información, controles que regulen el riesgo sobre la incorrecta asignación de privilegios de los usuarios.

- Criptografía: normativa que regule el tránsito de la información de forma cifrada, ya sea de forma interna o externa.

- Seguridad física y ambiental: lineamientos establecidos para el acceso a zonas críticas dentro de la institución y sobre la protección ante amenazas externas y ambientales.

- Seguridad de las operaciones: directrices en cuanto a la gestión de cambios en los sistemas, como lo son las bases de datos, registros de ingresos y cambios en esta; revisión a los usuarios privilegiados en los sistemas.

- Seguridad de las comunicaciones: normas para controlar la red, responsabilidades y gestiones para asegurar la red, con el fin de asegurar de forma razonable el tránsito interno o externo de la información.

- Adquisición, desarrollo y mantenimiento de sistemas: asegurar los servicios de aplicaciones en las redes, lineamientos para la gestión de cambios en desarrollo para la puesta en producción de aplicaciones, con el objetivo de proteger los datos sin importar el ambiente en el cual se desarrolle.

- Relación con proveedores: directrices para el tratamiento, manejo y tránsito de la información de la organización con los proveedores, el deber de los proveedores al estar en contacto con información sensible.

- Gestión de incidentes de seguridad de la información: plan de tratamientos de incidentes dentro de la organización, desde su clasificación hasta el proceso de comunicación para su atención.

- Aspectos de seguridad de la información en la gestión de la continuidad del negocio: normas que definan un plan de recuperación ante desastres y la continuidad del negocio.

- Cumplimiento: identificación de leyes y normas que aplican a la organización con el fin de cumplir con los requisitos establecidos; en este apartado se aplicarán

específicamente, las leyes o reglamentos que se basan en la administración de la información de los afiliados.

Análisis FODA

Para la presente investigación, el análisis del FODA ayuda a identificar las fortalezas, oportunidades, debilidades y amenazas aplicado a la empresa correspondiente a la implementación del Sistema de Gestión de Seguridad de la Información, con el fin de obtener conclusiones sobre la forma en que el objeto en sí estudiado podrá afrontar los cambios (oportunidades y amenazas) a partir de sus fortalezas y debilidades internas, con las siguientes estrategias a favor de su crecimiento:

Tabla 4. Matriz FODA

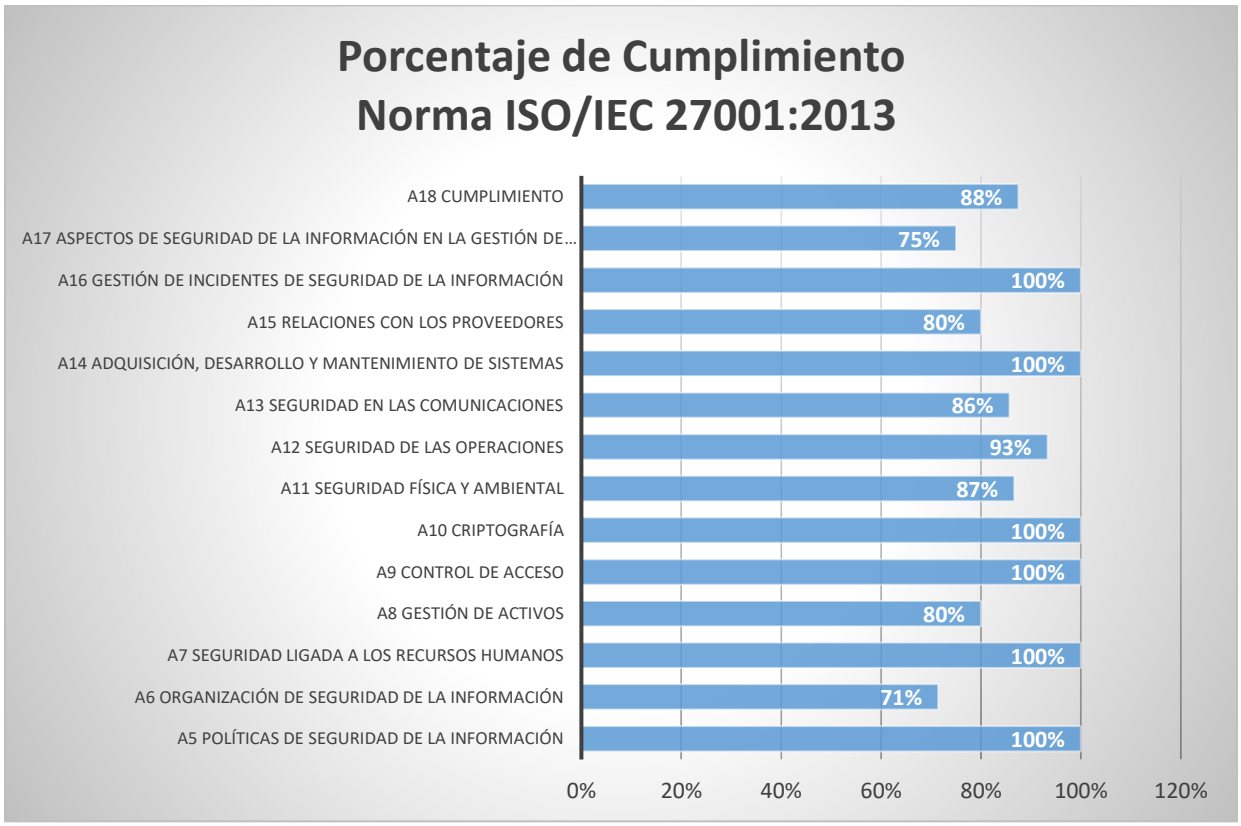
FORTALEZAS	Uso adecuado de los recursos informáticos.	**DEBILIDADES**	Ausencia de cumplimiento del marco normativo ISO/IEC 27001:2013 en el negocio.
	Apoyo de la alta gerencia, para implementar el sistema de gestión en el negocio.		Costos derivados a la implementación del Sistema de Gestión de Seguridad de la Información.
	Disminución de riesgos que afecten los principales pilares de seguridad de la información: disponibilidad, integridad y confidencialidad de la información.		Resultados de mediano a largo plazo, según disponibilidad de recursos.
OPORTUNIDADES	Establecer un Sistema de Gestión de Seguridad de la Información en el negocio, logrando el cumplimiento de las regulaciones vigentes.	**AMENAZAS**	Oposición al cambio.
	Obtener la certificación en la norma ISO/IEC 27001:2013.		Nuevos riesgos de seguridad asociados a tecnologías emergentes.
	Estrategia de mercado (ventaja competitiva), siendo la primera operadora de pensiones en el país en obtener la certificación.		
	Contar con un inventario de activos de información en la Dirección de Tecnología de Información, donde se tendrán identificados los responsables, exposición de riesgos, formato del activo de información (digital – físico), entre otros.		

Resultado de la evaluación

Para cada uno de los dominios establecidos en el alcance de la investigación se analizó la gestión desarrollada por la empresa Popular Pensiones, lo cual permite ubicar el estado de la seguridad de la información de la organización en un porcentaje de cumplimiento según lo establecido en la norma ISO/IEC 27001:2013 y un nivel de madurez según el estándar ISM[3] (*Information Security Management Maturity Model*, el cual define los grados de madurez según las buenas prácticas internacionales de seguridad de la información). Se describirá el estado de preparación en seguridad de la información, incluyendo porcentaje de cumplimiento de los requisitos y controles, así como las brechas existentes.

El porcentaje según el cumplimiento actual de la empresa con los requisitos establecidos en la norma ISO/IEC 27001:2013, es de un 90%.

Porcentaje de Cumplimiento

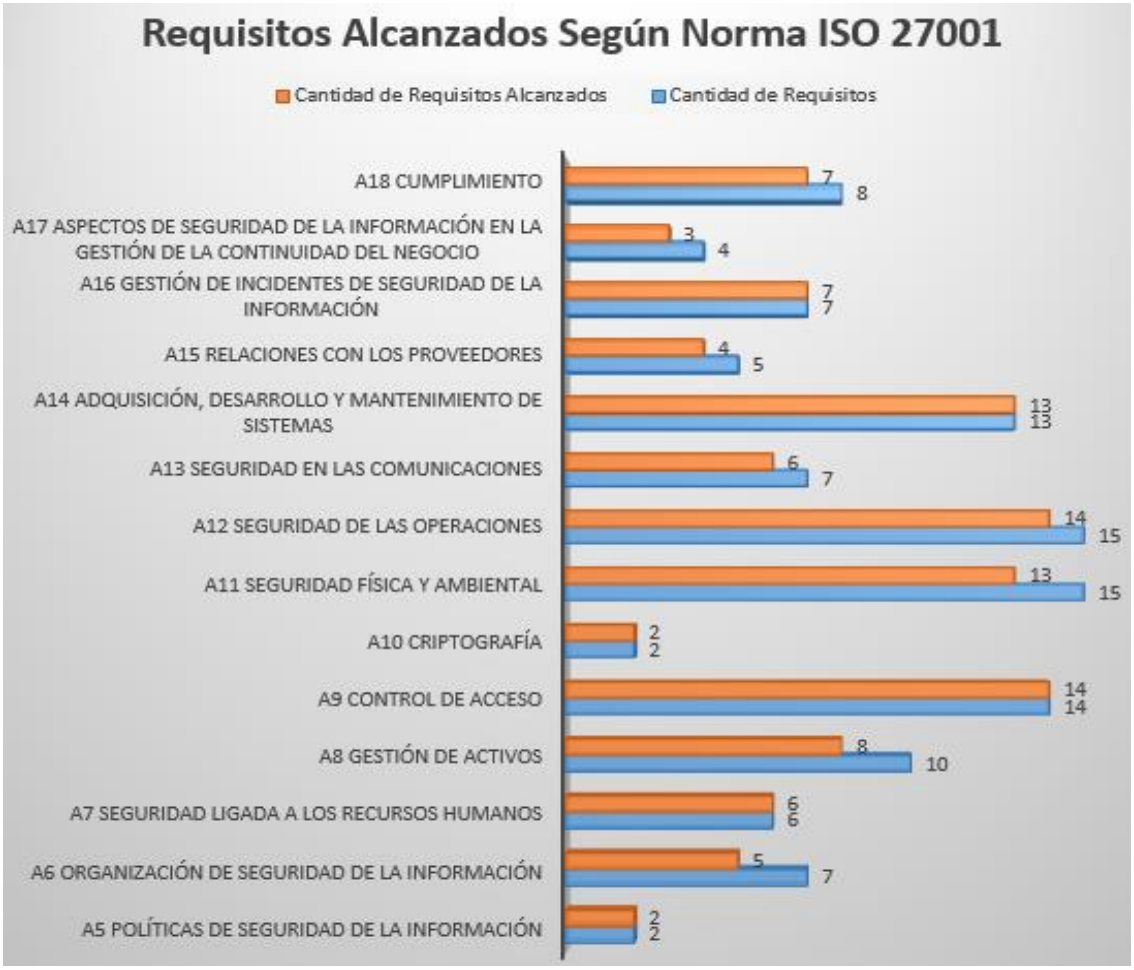


Fuente: Elaboración propia.

En el gráfico *Porcentaje de Cumplimiento* se muestra el porcentaje de cumplimiento de cada dominio de control establecido en la norma ISO/IEC 27001:2013 en la empresa Popular Pensiones, es importante destacar que seis de los catorce dominios tienen una calificación del 100% y no es necesaria una intervención. La calificación más baja corresponde al dominio A6. Organización de la Seguridad de la Información con un 71% y requiere una intervención de mejora al igual para los dominios: A18. Cumplimiento, A17. Aspectos de Seguridad de la Información, A15. Relaciones con los Proveedores, A13. Seguridad en las Comunicaciones, A12. Seguridad de las Operaciones, A11. Seguridad Física y Ambiental y A8. Gestión de Activos.

En cuanto a los requisitos alcanzados, la empresa cumple con los siguientes, basados en la norma ISO/IEC 27001:2013:

Requisitos alcanzados según norma



Fuente: Elaboración propia.

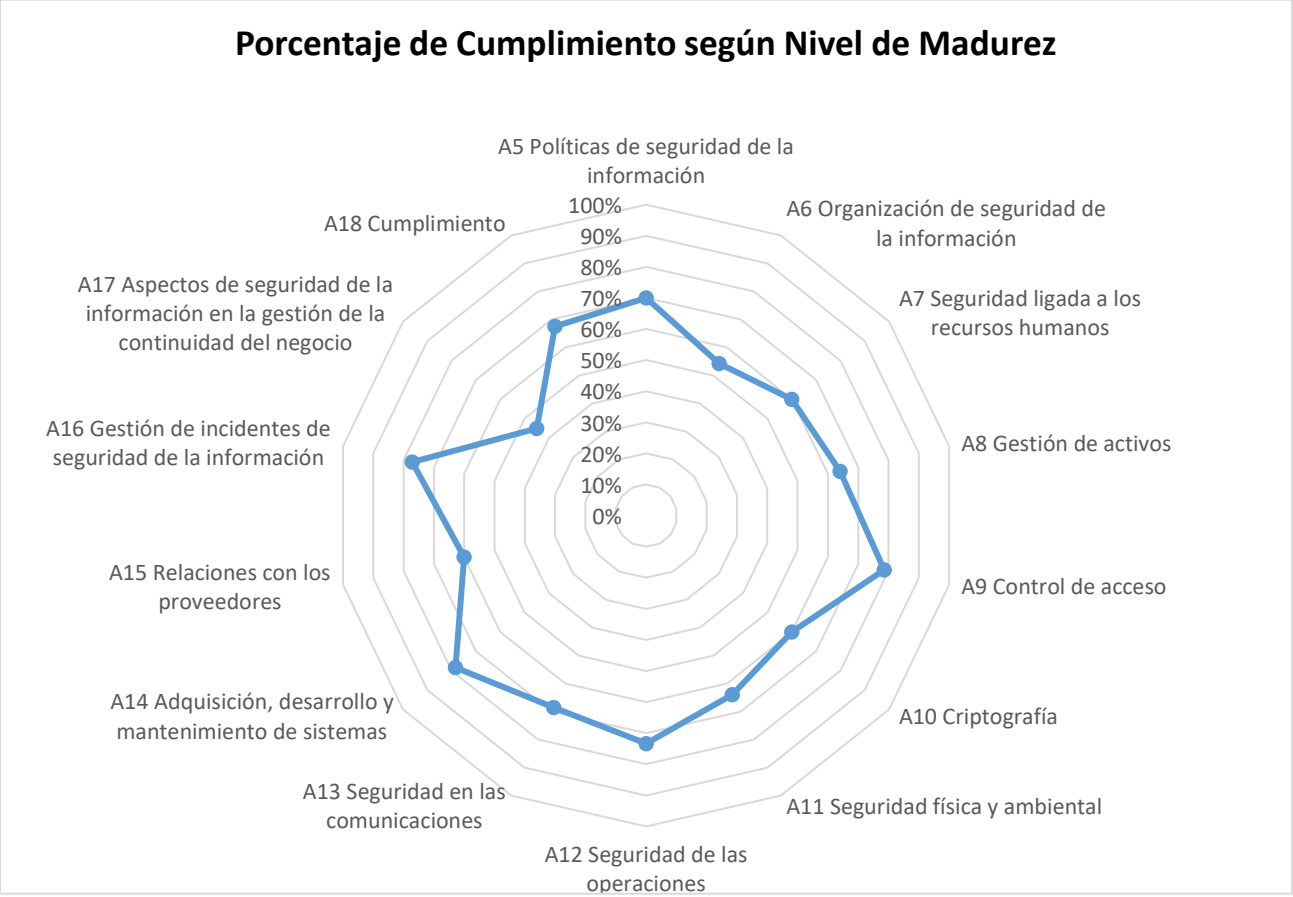
En el gráfico *Requisitos Alcanzados Según Norma* se muestra la cantidad de requisitos establecidos en cada dominio y su cumplimiento por parte de la empresa Popular Pensiones, para un total de 115 requisitos definidos en la norma por cada dominio de control y los requisitos alcanzados por parte de la empresa con un total de 104.

Popular Pensiones cumple a cabalidad con los requisitos de los siguientes dominios: A5 Políticas de seguridad de la información, A7 Seguridad ligada a los recursos humanos, A9 Control de acceso, A10 Criptografía, A14 Adquisición, desarrollo y mantenimiento de sistemas, A16 Gestión de incidentes de seguridad de la información; no obstante, los requisitos que requieren mejoras y cuentan con debilidad son: A6 Organización de seguridad de la información, A8 Gestión de activos, A11 Seguridad física y ambiental, A12 Seguridad de las operaciones, A13 Seguridad en las comunicaciones, A15 Relaciones con los proveedores, A17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio y A18 Cumplimiento.

El porcentaje de los niveles de madurez de la empresa, según los requisitos establecidos en la norma ISO/IEC 27001:2013, es de un 68%. Dicho resultado se obtuvo mediante el análisis de tres atributos (personas – procesos – tecnología), cada uno de los cuales se valora en una escala del 1 al 5, la cual corresponde a los niveles de madurez a calificar: inicial, repetible, definido, gestionado y optimizado.

En el siguiente gráfico se muestra, por cada dominio de control, el porcentaje obtenido en la empresa Popular Pensiones respecto al nivel de madurez. El porcentaje más bajo corresponde al dominio A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio con un 45% y el dominio A6. Organización de seguridad de la información con un 54%.

Porcentaje de cumplimiento según nivel de madurez

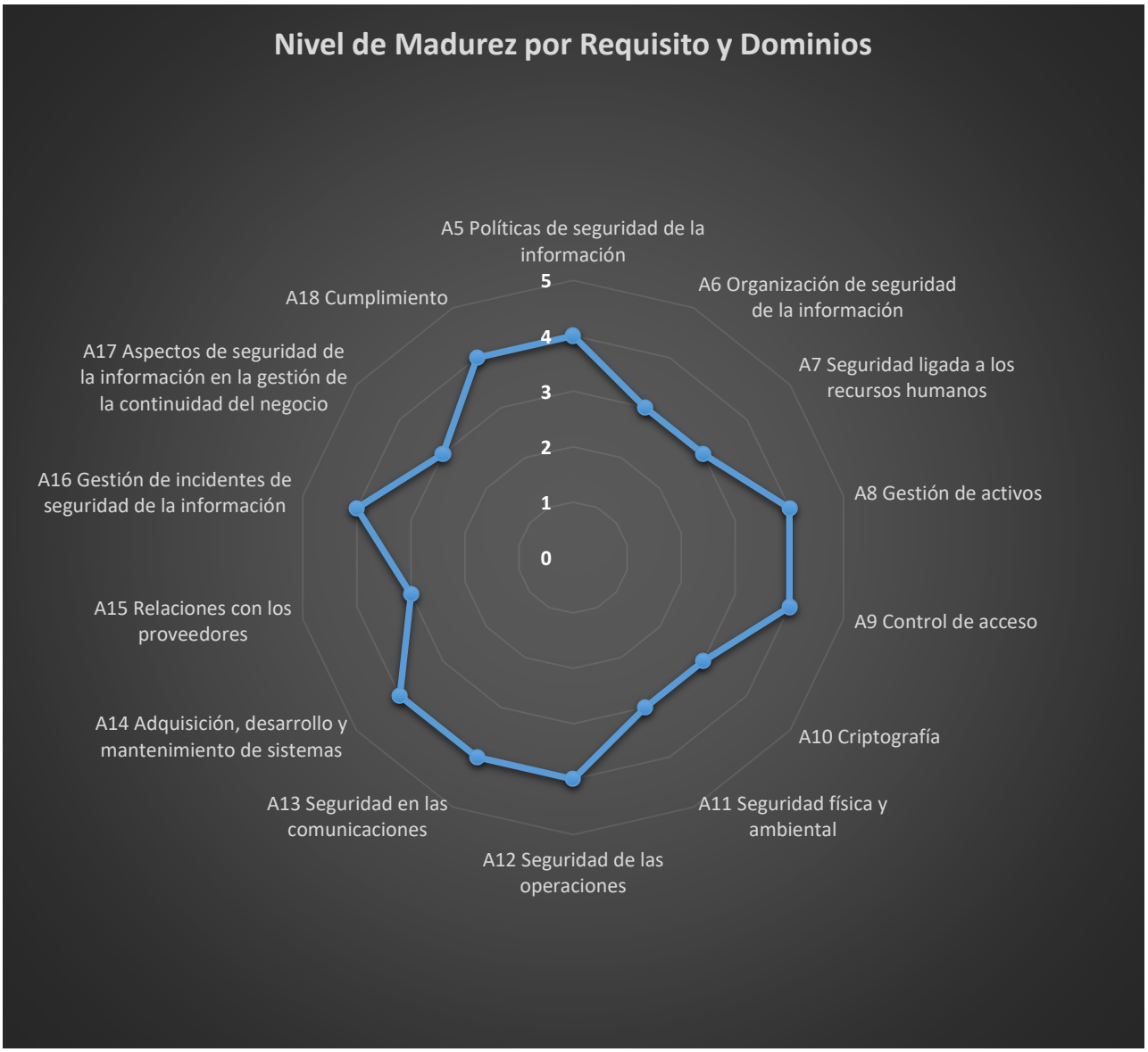


Fuente: Elaboración propia.

Respecto al nivel de madurez, tomando en cuenta los requisitos y dominios establecidos en el alcance de la investigación; se muestra en la ilustración 7 el nivel de madurez por cada dominio y requisito alcanzado por la empresa Popular Pensiones; cabe indicar que se utilizó una escala del 1 al 5 del modelo *Information Security Management Maturity Model*, siendo 5 el logro más alto en cuanto al nivel de madurez del negocio.

El nivel más bajo obtenido por la empresa es un 3, para los dominios de control: A6. Organización de seguridad de la información, A7. Seguridad ligada a los recursos humanos, A10. Criptografía, A11. Seguridad física y ambiental, A15. Relaciones con los proveedores y A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Nivel de madurez por requisito y dominios



Fuente: Elaboración propia.

Plan de Acción

Un plan de acción de seguridad de la información, ofrece a las empresas un medio para mitigar los riesgos y un método para alcanzar metas y objetivos organizacionales que estén relacionados con la seguridad de la información. En el presente plan, se define el propósito y los objetivos que se apremian en la organización en relación a la norma ISO/IEC 27001:2013,

asegurando que las inversiones dedicadas a los proyectos sean de apoyo para la mejora continua del Sistema de Gestión de Seguridad de la Información y gestionar así la certificación.

Objetivo

Elaborar un Plan de Acción de Seguridad de la Información, según el estándar internacional ISO/IEC 27001:2013, para mejorar el Sistema de Gestión de Seguridad de la Información. En dicho plan se deben establecer las actividades generales de implementación de los controles faltantes según lo establecido en la norma.

Alcance

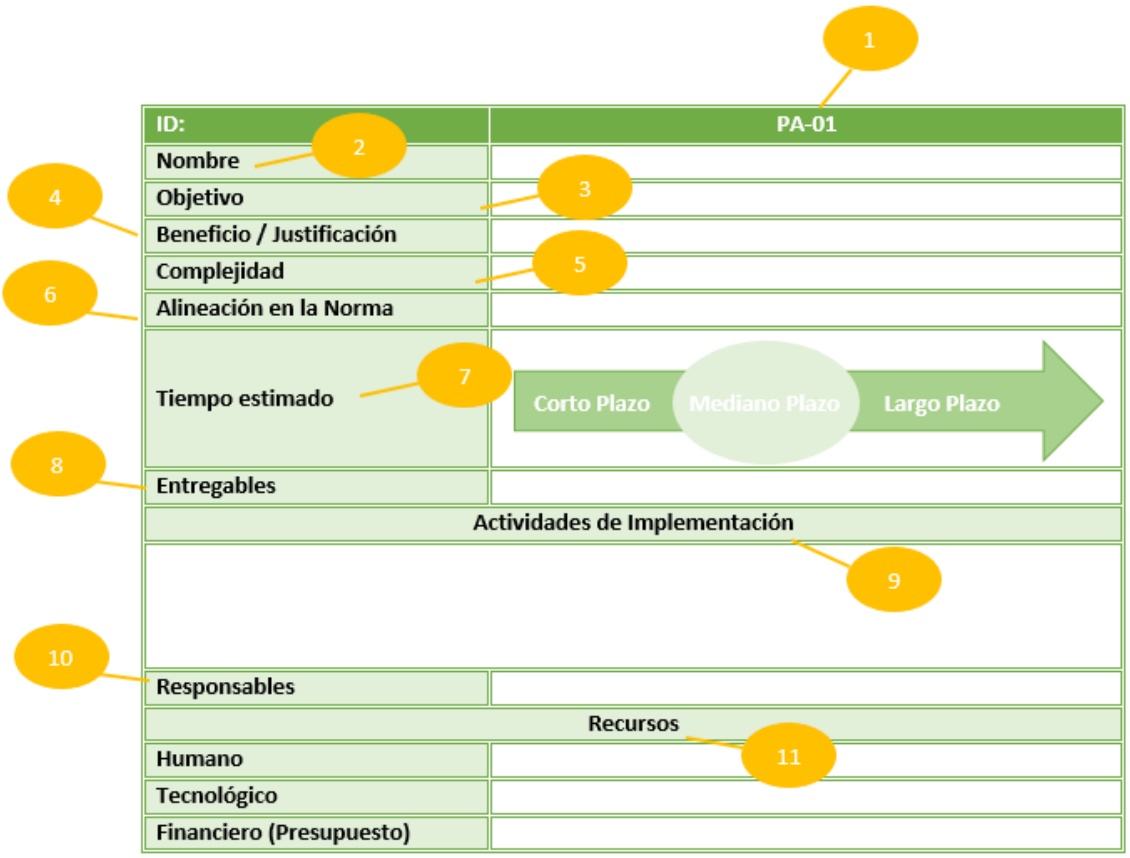
El presente plan fue desarrollado considerando como alcance las actividades para obtener el cumplimiento de los objetivos de control (dominios) detallados en el estándar de seguridad ISO/IEC 27001:2013, según las brechas de seguridad identificadas. Dentro de las actividades se consideran las siguientes categorías principales: Organización de seguridad de la información, Gestión de activos, Seguridad física y ambiental, Seguridad de las operaciones, Seguridad en las comunicaciones, Adquisición, desarrollo y mantenimiento de sistemas, Relaciones con los proveedores, Aspectos de seguridad de la información en la gestión de la continuidad del negocio y Cumplimiento.

Diseño de atención de brechas

Se procedió a identificar las estrategias o programas para cubrir las brechas identificadas durante la fase del diagnóstico de la situación actual. Cada estrategia se identifica con el requisito faltante o que se debe mejorar en la institución, para dar cumplimiento a los requerimientos establecidos de cada dominio.

Cada estrategia o programa cuenta con un identificador único, el cual está compuesto por la palabra “PA”, la cual significa (Plan de Acción) y un identificador numérico. En la Ilustración 8 se muestran los criterios que componen cada estrategia.

Ilustración 8. Plantilla plan de acción



Fuente: Elaboración Propia

Donde:

1. **ID**: se asigna un identificar único al plan de acción para poder distinguirlos, utilizando la nomenclatura PA, seguida de un consecutivo numérico.

2. **Nombre**: en esta sección se le asigna un nombre corto al plan de acción.

3. **Objetivo**: se describe la finalidad que tiene el plan de acción.

4. **Beneficio / Justificación**: se describe la justificación de la implementación del plan de acción, así como los beneficios directos de su implementación.

5. **Complejidad**: se le asigna un valor (alto, medio o bajo) a la complejidad de la implementación.

6. **Alineación en la norma**: se especifica la alineación que tiene el plan de acción con la norma ISO/IEC 27001:2013.

7. **Tiempo estimado**: en esta sección se indica el periodo en el cual se estima que debe ser implementado el plan de acción. Se establecieron tres plazos:
    - Corto plazo: Menor a un año.
    - Mediano plazo: Mayor a un año y menor a 3 años.
    - Largo plazo: Mayor a 3 años.

8. **Entregables**: se listan los entregables principales que deben ser productos de la implementación del plan de acción.

9. **Actividades de implementación**: se especifican las actividades que se deben ejecutar para implementar el proyecto.

10. **Responsables**: en este apartado se debe especificar los puestos o áreas responsables de implementar el plan de acción.

11. **Recursos**: en esta sección, se detallan los recursos que deben considerarse para ejecutar el plan de acción. El recurso financiero corresponde a una estimación del salario por horario de un funcionario de la institución, que labora específicamente en la Dirección de Tecnología de Información, para desarrollar la implementación; este costo puede variar según la estrategia de implementación seleccionada u otros factores en el momento de implementar el plan.

Propuesta del plan de acción

La presente propuesta corresponde al plan de remediación de brechas encontradas en el diagnóstico de la situación actual de la empresa Popular Pensiones. En la Tabla 5. *Propuesta del Plan de Acción*; se muestra un resumen del plan de acción, recursos necesarios para atender el plan y los responsables en la institución. Asimismo, en el anexo de la propuesta se encuentran los documentos a que hace mención cada plan de acción.

Tabla 5. Propuesta del plan de acción

Plan de Acción		Recursos			Responsabilidades	
Nombre	**Objetivo**	**Inversión**	**Humano**	**Tecnológico**	**Responsables**	**Roles**
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A6. Organización de seguridad de la información.	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A8. Gestión de activos	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A11.	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.

Seguridad física y ambiental

Plan de Acción		Recursos			Responsabilidades	
Nombre	**Objetivo**	**Inversión**	**Humano**	**Tecnológico**	**Responsables**	**Roles**
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A12. Seguridad de las operaciones	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A13. Seguridad en las comunicaciones	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013para el cumplimiento del dominio de control A15. Relaciones con los proveedores	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos

						para que se encuentren adaptados a la organización.

Plan de Acción		Recursos			Responsabilidades	
Nombre	**Objetivo**	**Inversión**	**Humano**	**Tecnológico**	**Responsables**	**Roles**
Implementación de políticas, procedimientos y/o documentación requerida por la Norma ISO/IEC 27001:2013 para el cumplimiento del dominio de control A18 Cumplimiento	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación	Horas: 5 Costo por hora: ¢5000 Inversión: ¢25.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la documentación realizada por el Asesor. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación de los documentos para que se encuentren adaptados a la organización.
Creación de Plantilla de Inventario de Activos de Información.	Crear la plantilla inicial para identificar los activos de información de la Dirección de Tecnología de Información.	Horas: 24 Costo por hora: ¢5000 Inversión: ¢120.000	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.	N.A.	*Asesor *Directora de Tecnología de Información *Personal Asignado de Tecnología de Información	**Asesor:** Creación de los documentos listados en la sesión de actividades de implementación. **Directora de Tecnología de Información:** Revisar la plantilla realizada por el Asesor y el trabajo que realice el Personal de Apoyo. **Personal de Apoyo de Tecnología de Información:** Realizar el acompañamiento en la creación del inventario de activo de información, identificar los activos de información en la Dirección de Tecnología de Información y categorizar según plantilla.

Descripción del plan de acción

En este apartado se detalla cada uno de los planes de acción para la implementación de lo requerido, con el fin de gestionar la certificación de la norma ISO/IEC 27001:2013. Está compuesto de ocho (8) planes de acción para el cumplimiento de los dominios por mejorar y controles faltantes en la organización. Cabe indicar que la inversión en implementar cada plan es un valor estimado tomando en cuenta el salario promedio del personal de Tecnología de Información; asimismo, el costo puede variar según la estrategia por seguir de la empresa, recurso humano que considere además del sugerido y el tiempo para ejecutar cada plan de acción.

Tabla 6. Plan de Acción 1

ID:	PA-01
Nombre	Creación, revisión y actualización de políticas y/o documentación requerida por ISO/IEC 27001:2013.
Objetivo	Crear el documento y procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A6. Organización de seguridad de la información.
Complejidad	Media
Alineación en la Norma	A6.1.3 Contacto con Autoridades Y A6.2.2 Teletrabajo
Tiempo estimado	
Entregables	
Actividades de Implementación	
-Creación de la plantilla Contacto con Autoridades, en la cual se debe incluir las autoridades competentes con el Sistema de Gestión de Seguridad de la Información. -Propuesta de mejora política Teletrabajo.	
Responsables	Asesor: Creación de la documentación listada en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: Completar la plantilla con los entes relacionados.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢25.000 colones

Tabla 7. Plan de Acción 2

ID:	PA-02
Nombre	Creación, revisión y actualización de políticas y/o documentación requerida por ISO/IEC 27001:2013.
Objetivo	Crear el procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A8. Gestión de Activos
Complejidad	Media
Alineación en la Norma	A8.1.1 Inventario de Activos, A8.3.1 Gestión de medios removibles y A8.3.2 Eliminación de medios
Tiempo estimado	
Entregables	
Actividades de Implementación	
-Creación del procedimiento para la gestión de medios removibles, el cual contempla también la eliminación de medios. -Creación de la plantilla "Inventario de Activos de Información Tecnología de Información".	
Responsables	Asesor: Creación de la documentación listada en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del documento y plantilla, con el fin de adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢120.000 colones

Tabla 8. Plan de Acción 3

ID:	PA-03
Nombre	Creación, revisión y actualización de políticas y/o documentación requerida por ISO/IEC 27001:2013.
Objetivo	Crear el procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A11. Seguridad Física y Ambiental
Complejidad	Media
Alineación en la Norma	A11.1.4 Protección contra amenazas externas y ambientales, A11.1.6 Áreas de entrega y carga
Tiempo estimado	
Entregables	
Actividades de Implementación	
Creación de la política/directriz Seguridad Física y Ambiental. Si bien la empresa cuenta con la seguridad necesaria según la norma, está pendiente establecerla como una directriz o política en la institución.	
Responsables	Asesor: Creación de la documentación listada en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del documento y adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢25.000 colones

Tabla 9. Plan de Acción 4

ID:	**PA-04**
Nombre	Creación, revisión y actualización de políticas y/o documentación requerida por ISO/IEC 27001:2013.
Objetivo	Crear el procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A12. Seguridad de las Operaciones.
Complejidad	Media
Alineación en la Norma	A12.1.2 Gestión de cambios
Tiempo estimado	
Entregables	
Actividades de Implementación	
Creación de la directriz Seguridad de las Operaciones, específicamente al proceso *Gestión de Cambios*.	
Responsables	Asesor: Creación de la documentación listada en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del documento y adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢25.000 colones

Tabla 10. Plan de Acción 5

ID:	**PA-05**
Nombre	Creación, revisión y actualización de políticas y/o documentación requerida por ISO/IEC 27001:2013.
Objetivo	Crear el procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A13. Seguridad en las Comunicaciones.
Complejidad	Alta
Alineación en la Norma	A13.1.3 Segregación en las redes
Tiempo estimado	
Entregables	
Actividades de Implementación	
Creación de la directriz Seguridad en las Comunicaciones, específicamente al proceso *Segregación en las Redes*.	
Responsables	Asesor: Creación de la documentación listada en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del documento y adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢50.000 colones

Tabla 11. Plan de Acción 6

ID:	PA-06
Nombre	Creación, revisión y actualización de políticas y/o documentación requerida por ISO/IEC 27001:2013.
Objetivo	Crear el procedimiento inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A15. Relación con los proveedores.
Complejidad	Baja
Alineación en la Norma	A15.1.3 Cadena de suministro de tecnologías de información y comunicaciones
Tiempo estimado	
Entregables	
Actividades de Implementación	
Creación de un apartado, el cual especifique la seguridad de la información con el proveedor y subcontratos por este.	
Responsables	Asesor: Creación de la documentación listada en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del documento y adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢25.000 colones

Tabla 12. Plan de Acción 7

ID:	**PA-07**
Nombre	Plan de Continuidad de negocio adaptado a lo requerido por la norma ISO/IEC 27001:2013.
Objetivo	Crear el apartado inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A17 Aspectos de seguridad de la información en la gestión de continuidad del negocio.
Complejidad	Baja
Alineación en la Norma	A17.2.1 Disponibilidad de recursos de procesamiento de información
Tiempo estimado	
Entregables	
Actividades de Implementación	
Creación de un apartado, el cual especifique la disponibilidad de recursos de procesamiento de información iniciales en la organización.	
Responsables	Asesor: Creación del apartado listado en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del apartado y adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢25.000 colones

Tabla 13. Plan de Acción 8

ID:	PA-08
Nombre	Plan de Continuidad de negocio adaptado a lo requerido por la norma ISO/IEC 27001:2013.
Objetivo	Crear el apartado inicial requeridos por la norma, para el cumplimiento de la certificación.
Beneficio / Justificación	Cumplimiento del dominio de control A18 Cumplimiento
Complejidad	Baja
Alineación en la Norma	A18.1.2 Derechos de propiedad intelectual
Tiempo estimado	
Entregables	
Actividades de Implementación	
Creación de un apartado, el cual especifique los derechos de propiedad intelectual de la empresa.	
Responsables	Asesor: Creación del apartado listado en la sección de actividades de implementación. Directora de Tecnología de Información: Revisar la documentación realizada por el Asesor y el Personal de Apoyo. Personal de Apoyo de Tecnología de Información: verificar la creación del apartado y adaptarlos a la organización.
Recursos	
Humano	Asesor, Directora de Tecnología de Información, Personal asignado de Tecnología de Información.
Tecnológico	N.A.
Financiero (Presupuesto)	¢25.000 colones

Conclusiones

Durante y posterior a las fases de análisis y tabulación de datos correspondientes a la evaluación de la situación actual de Popular Pensiones, respecto al cumplimiento de los dominios de la norma ISO/IEC 27001:2013 y del Sistema de Gestión de Seguridad de la Información, se detallan las siguientes conclusiones:

1. La empresa Popular Pensiones presenta una gestión de la seguridad de la información alineada a las directrices, políticas, normas, procedimientos y buenas prácticas, con un enfoque global de la seguridad de la información a nivel organizacional; sin embargo, no hace énfasis a algún proceso específico de su cadena de valor o procesos críticos. Por lo tanto, la gestión de la seguridad de la información y su orientación al cumplimiento de la norma ISO/IEC 27001:2013, no se encuentra alineada al no tener delimitado su alcance.

2. Si bien la empresa cumple en un 90% en la cantidad de requisitos alcanzados, correspondientes a la norma ISO/IEC 27001:2013; su nivel de madurez es de un 68%, lo que significa que existen normativas, directrices y controles que no están siendo aplicados y comunicados a nivel de la organización; proporcionando una falta de mejora continua y revisión de controles, con el fin de identificar sus falencias.

3. Las diferentes áreas operativas de la empresa se encuentran enteradas sobre las responsabilidades sujetas a la seguridad de la información; sin embargo, es importante reforzar la capacitación, sensibilización y la divulgación de la seguridad, mejorando la cultura en la organización. Es importante recalcar la concientización a todas las áreas sobre todos los lineamientos existentes, con el fin de alinear al negocio con el Sistema de Gestión de Seguridad de la Información, ya que este debe convertirse en un tema institucional prioritario, para gestionar la norma.

4. El diagnóstico realizado corresponde al cumplimiento de los catorce dominios (controles) establecidos en la norma ISO/IEC 27001:2013 y al alcance de la presente investigación, si bien la norma también cuenta con los apartados de:

- Contexto de la organización.
- Liderazgo.
- Planificación.
- Soporte.
- Operaciones.
- Evaluación del desempeño.
- Mejoras.

La investigación se concentró en los controles de la norma, con el objetivo de evaluar inicialmente el estado actual de cada uno y así poder demostrar a la empresa, el nivel de cumplimiento y su estado de madurez. Cabe indicar que los apartados mencionados anteriormente involucran a la alta gerencia de la organización y la factibilidad para una evaluación y entrevista es muy compleja. Sin embargo, el valor agregado es exteriorizar los beneficios de gestionar el cumplimiento de la norma, el diagnóstico de los controles y el plan de acción, y así poder mostrar a la Gerencia el estado actual de su negocio.

5. Mediante el plan de acción definido para los dominios evaluados, la empresa tendrá identificados los recursos, tiempo, plantillas y responsables para la aplicación de mejoras en el sistema de gestión de seguridad de la información y atención de las brechas halladas. Asimismo, los costos asociados en la implementación de los controles faltantes o mejoras asociadas.

Recomendaciones

Las recomendaciones se basan en las brechas encontradas durante la evaluación de los 14 dominios de la norma ISO/IEC 27001:2013 y en cómo mejorar los procesos asociados a cada control de la norma, con el fin de gestionar el Sistema de Gestión de Seguridad de la Información.

1. Se recomienda definir el Sistema de Gestión de Seguridad de la Información en Popular Pensiones, tomando en cuenta los procesos críticos de la cadena de valor y la visión de convertirse en la primera operadora de pensiones costarricense con certificación ISO/IEC

27001:2013 y ofrecer a sus afiliados la garantía del manejo seguro de su información. Cabe destacar que esta recomendación debe ser el punto de partida esencial para alcanzar la certificación correspondiente. Si bien la presente investigación tuvo como alcance la evaluación de los controles (dominios) de la norma, la implementación de un sistema de gestión requiere el apoyo de la alta gerencia para inculcar en la empresa el cumplimiento de dicho sistema.

2. Aunado al punto anterior, se recomienda continuar con la evaluación de la norma, específicamente con los apartados:

    - Contexto de la organización.
    - Liderazgo.
    - Planificación.
    - Soporte.
    - Operaciones.
    - Evaluación del desempeño.
    - Mejoras.

    Lo anterior, creando una política especifica que regule la gestión de la seguridad de la información en el negocio y analizar su efectividad definiendo: qué hacer (objetivo), cuándo (periodicidad), quiénes (responsables), dónde (contexto) y registro (almacenamiento de la evaluación).

3. Aplicar la propuesta del plan de acción de las brechas encontradas en la evaluación de los catorce dominios establecidos en el alcance de la investigación. Esto con el fin de subsanar lo hallado y mejorar los procesos asociados a los controles determinados.

    En virtud de lo anterior, se recomienda que el responsable de implementar el plan de acción, sea la Directora de Tecnología de Información del negocio, a partir del momento de entrega de la propuesta; asimismo se indica que, el tiempo estimado de dicha implementación es de 8 días hábiles.

4. Concientizar a toda la organización sobre los lineamientos existentes con el fin de alinear al negocio con el sistema de gestión de seguridad de la información, preparar al personal para cumplir con los controles establecidos en la norma ISO/IEC 27001:2013, con el objetivo de garantizar el cumplimiento; previamente, durante y posterior a la auditoría que realice el ente certificador y estar enfocados en conseguir los objetivos planteados y lo más importante, crear conciencia sobre la protección y manejo de la información en el Sistema de Gestión de Seguridad de la Información.

5. Es importante recalcar que la norma no indica que toda la organización o todos los procesos deben cumplir con los lineamientos establecidos en dicha norma, por lo que su aplicación puede estar delimitada en el alcance; al tener identificado el proceso del negocio en el alcance es sobre el proceso indicado que se efectúa la evaluación, por lo que se recomienda a la empresa Popular Pensiones, delimitar sus procesos del negocio, para centralizar la evaluación.

ANEXO

PA-01

Plantilla – Contacto con las Autoridades

Lista de Contactos de Autoridades y Grupos de Interés Especial

Las siguientes autoridades y grupos de interés especial serán regularmente contactados y monitoreados como parte del Sistema de Gestión de Seguridad de la Información.

Ref.	Nombre del Grupo	Descripción	Tipo	Propósito de Contacto	Método de Contacto	Frecuencia	Empresa	Nombre del Contacto	Dirección del Contacto	Número de Teléfono	Comentarios
1	(Proveedores / Empresas)	(Detalle)	(Especial, Autoridad)	(Tipo de Servicio)	(Teléfono, Correo)	(Cada cuánto se debe contactar)	(nombre)	(Nombre del responsable por parte del grupo)			
2											
3											
4											
5											
6											

Apartado Teletrabajo

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

PUESTA EN MARCHA DE UN ACUERDO DE TELETRABAJO

Desde el punto de vista de la seguridad de la información, hay varios aspectos que deben tenerse en cuenta en cada acuerdo de teletrabajo y la política de la operadora, en estas áreas se establece en las siguientes secciones.

1. Evaluación Inicial del Riesgo

Antes de que pueda comenzar un acuerdo de teletrabajo, habrá una evaluación inicial del riesgo del entorno propuesto y la naturaleza del trabajo que se llevará a cabo.

2. Naturaleza del Trabajo

Una parte importante de la evaluación de riesgos se refiere al tipo de actividades que se llevarán a cabo como parte del acuerdo. Se debe obtener una comprensión completa de:

•La clasificación de la información que se almacenará y procesará como parte del rol.

•El método de acceso de la información.

•Si el rol requiere que la información clasificada se imprima localmente.

•La criticidad comercial del rol y las consecuencias si no estuviera disponible.

3. Seguridad Física

La evaluación de riesgos también considerará la seguridad física del lugar de trabajo propuesto:

• ¿Hay suficiente espacio para albergar el equipo requerido con seguridad?

• ¿Se puede asegurar el área de trabajo, por ejemplo, a través de una puerta cerrada cuando no está en uso?

• ¿Quién más tiene acceso al área de trabajo?

• ¿Cuál es la probabilidad de robo en el área circundante?

• ¿Hay un suministro de energía adecuado y confiable para el área de trabajo?

4. Instalaciones Proporcionadas

La política de la operadora con respecto a la provisión de instalaciones para permitir el teletrabajo se detalla a continuación.

Se debe tener en cuenta que todas las disposiciones de la Política de Dispositivos Móviles de la operadora también se aplican al entorno de teletrabajo y este documento debe ser leído y comprendido por todas las partes involucradas.

5. Equipo

Solo el equipo del personal provisto por la operadora para fines de teletrabajo debe usarse para acceder a las redes de la compañía. Los dispositivos propios del individuo, tales como computadoras portátiles o PC, no deben usarse para este propósito.

De acuerdo con los requisitos, quien realice teletrabajo puede estar provisto de:

•Una computadora portátil, Tablet o PC de escritorio con teclado y mouse

•Una impresora

•Escritorio y silla

•Almacenamiento seguro

•Otros elementos según se requiera para el rol

Este equipo sigue siendo propiedad de la operadora en todo momento

6. Comunicaciones

Se usará una red privada virtual (VPN) para garantizar que todo el tráfico de la red desde el cliente de quien realiza teletrabajo a los servidores de la operadora esté encriptado según los estándares de la operadora.

7. Protección de Respaldo y Virus

Donde sea posible, no se almacenarán datos en la máquina del colaborador. En caso de que esto sea inevitable, es responsabilidad de quien realice teletrabajo, asegurarse de que esté respaldado en la red corporativa lo antes posible.

Se proporcionará protección contra virus en todos los equipos pertinentes y se configurará para actualizarse automáticamente al conectarse a la red corporativa.

8. Soporte Técnico

El soporte técnico de todos los equipos suministrados será proporcionado por TI.

9. Terminación del Acuerdo

En el caso de que el contrato de teletrabajo termine por cualquier motivo, todos los equipos que se suministraron como parte del acuerdo deben devolverse al centro de soporte de TI lo antes posible.

PA-02

Apartado - Eliminación de Medios

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

1. INTRODUCCIÓN

Puede haber circunstancias donde los medios removibles necesitarán ser utilizados para almacenar información clasificada.

El uso de medios removibles como memorias USB, CD, DVD y tarjetas de almacenamiento para almacenar los datos de Popular Pensiones representa un riesgo significativo para la operadora y está estrictamente controlado por la política de seguridad de la información.

Cuando los medios removibles se estén usando actualmente en un proceso de negocio, se debe considerar el mejor método para lograr ese proceso por otros medios.

2. OBJETIVO

Proporcionar procedimientos sobre cómo se deben evaluar las solicitudes para el uso de medios removibles y las recomendaciones apropiadas que se deben realizar dependiendo de las circunstancias y los requisitos.

3. ALCANCE

Este procedimiento aplica a todos los sistemas, personas y procesos que constituyen los sistemas de información de Popular Pensiones, incluyendo empleados y proveedores con acceso a los sistemas de la operadora.

4. SELECCIÓN DE MEDIOS REMOVIBLES

Cuando se utilicen medios removibles de cualquier formato (CD, DVD, dispositivo de memoria, etc.) para almacenar datos confidenciales, se debe evaluar si se puede usar un método alternativo más seguro y, de no ser así, cuál es la mejor manera de asegurar el método actual para que el riesgo para la operadora se minimice.

Tales métodos existentes pueden incluir:

• Transferencia de datos a terceros.

• Llevar información a casa para trabajarla.

• Respaldos de datos, además de respaldos programados del servidor.

• Transferencia de datos entre dispositivos.

En el caso de que un uso existente no se encuentre en la lista anterior, pero contravenga la política de seguridad de la información, aún debe identificarse un método alternativo para lograr el resultado final deseado.

4.1. Transferir Datos a Terceros

Antes de considerar métodos alternativos para la transferencia de datos, los siguiente debe conocerse:

• ¿Qué datos se están transfiriendo?

• ¿Cuál es el propósito de negocio de la transferencia?

• ¿A quién está siendo transferida?

• ¿Cuáles controles tienen establecidos las terceras partes para garantizar la seguridad de los datos sensibles?

• ¿Se requieren acuerdos de confidencialidad con los terceros para garantizar que nuestros datos serán protegidos?

• ¿Con qué frecuencia se transferirán los datos o se trata de un evento puntual?

Solo en circunstancias extremas, cuando no es posible transferir datos por medios de protocoles seguros de transferencia, una memoria cifrada puede ser lo adecuado, idealmente, llevada al tercero por un miembro de la operadora. De lo contrario, debe enviarse por correo certificado con facilidad de seguimiento y requerir una firma en el otro extremo.

5. ELIMINACIÓN

Los dispositivos o medios se eliminarán utilizando algún método elegido (eliminación local, por medio de un tercero, entre otros). Para su eliminación local, la destrucción debe ser presenciada por más de una persona y los nombres de las personas involucradas deben registrarse.

Para una eliminación segura utilizando un tercero, el contratista emitirá un certificado de eliminación que cumpla con la legislación aplicable. El Centro de Soporte de TI mantendrá un registro de estos certificados.

Cuando corresponda, algunos de los equipos (o componentes de ellos) pueden reciclarse de acuerdo con la legislación aplicable.

5.1. Registros de Eliminación y Cierre de Solicitud

Una vez que se eliminó con éxito, el registro de solicitud debe actualizarse con la fecha, hora y método de eliminación y cerrarse.

El registro de activos de *hardware* también debe actualizarse para reflejar el hecho de que el equipo ha sido destruido de forma segura.

Plantilla – Inventario de Activos de Información

Identificación y Valoración de Activos

Inventario de Activos de Información - Tecnología de Información

ID-Activo	Tipo de Activo	Nombre del Activo	Descripción del Activo	Dueño	Formato		Clasificación	Ubicación del Activo (Físico o Digital)	Impacto de Afectación
					Físico	Digital			
Código del Activo de Información	Servicio - Estrategia - Interés Público - Financiero Datos Personales.			Responsable del activo			Público - Interno - Confidencial		Alto - Medio - Bajo

PA-03

Apartado - Seguridad Física y Ambiental

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

1. Perímetros de Seguridad Física

En todos los puntos de entrada alrededor del perímetro de seguridad física deben evaluarse los riesgos que podrían materializarse, entre ellos: techos y paredes para garantizar que ofrecen un buen grado de protección sin puntos débiles.

Las puertas externas deben estar aseguradas con un nivel de protección adicional adecuado al nivel de seguridad requerido (por ejemplo, barras, cadenas, alarmas y cerraduras múltiples) con la debida consideración de las normas de seguridad contra incendios aplicables.

Las ventanas externas alrededor del perímetro deben estar cerradas con llave y las que se encuentran en la planta baja deben asegurarse con barras cuando sea posible (sujeto a las regulaciones pertinentes).

1.1. Área de Recepción

Debe existir un área de recepción, para controlar el acceso del personal interno y externo.

1.2. Barreras Físicas

Cuando sea apropiado, se deben instalar barreras físicas para evitar el acceso sin el nivel correcto de autorización. Esto debería evitar el seguimiento de personas, es decir, una persona no autorizada que siga a una persona autorizada a través de la barrera. Se puede tomar como referencia el control de acceso con tarjetas de proximidad.

1.3. Puertas contra Incendios

Las puertas contra incendios deben cumplir con los requisitos legales y ser probadas regularmente. Como estándar, estos deben ser alarmados y monitoreados desde un punto de control.

1.4. Sistemas de Detección de Intrusos

Instalar alarmas contra intrusos y un circuito cerrado de televisión (CCTV) para proteger los puntos de entrada y advertir sobre violaciones de seguridad.

2. Entrega y Cargas

2.1. Entregas

Se debe utilizar un área de entrega o de espera por separado para que las entregas se puedan inspeccionar antes de que se acepten en el área segura. Dicha inspección debe realizarse lo antes posible después de la entrega y ser lo suficientemente exhaustiva como para evaluar la probabilidad de que haya alguna amenaza presente.

2.2. Separación de Mercancías Entrantes y Salientes

Las áreas deben diseñarse de modo que las entregas y los artículos salientes no se almacenen o procesen en el mismo lugar.

PA-04

Apartado – Gestión de Cambios

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

1. **OBJETIVO**

Establecer las formas en que se lleva a cabo el registro de Auditoría, monitoreando actividades de usuarios tanto autorizados como no autorizados (Gestión de Cambios).

2. **ALCANCE**

Aplica a todos los sistemas, colaboradores y terceros que constituyen los sistemas de información de la empresa, con acceso a los sistemas.

a. Registros de Auditoría

Todos los equipos de cómputo, servidores y otros equipos de red que participan en el almacenamiento o procesamiento de información clasificada tendrán activadas las funciones de registro de auditoría disponibles para permitir el registro y monitoreo de actividades en las siguientes áreas:

• Fechas y horas de eventos clave, por ejemplo, iniciar / cerrar sesión

• Intentos de acceso a sistemas exitosos y fallidos

• Datos exitosos y rechazados y otros intentos de acceso a los recursos

• Cambios a los parámetros y configuraciones del sistema

• Uso de utilidades y aplicaciones del sistema

Esta información debe brindar información cuando se requiera de lo que sucede en los equipos.

El principio general adoptado es que cuanto mayor sea el nivel de clasificación de la información que se posee o procesa, mayor será el nivel de detalle al que los registros de auditoría registrarán los datos. Se deben considerar servidores, *firewalls*, *switches* y demás.

PA-05

Apartado – Segregación en las redes

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

1. INTRODUCCIÓN

El uso de redes es una parte esencial del negocio diario de la empresa. Las redes no solo conectan internamente muchos de los componentes de los procesos de negocios, sino que también vinculan a la empresa con sus proveedores, clientes y partes interesadas.

En virtud de lo anterior, las redes deben estar protegidas para garantizar que la confidencialidad, integridad y disponibilidad de la información esté asegurada en todo momento.

2. OBJETIVO

Establecer las reglas de segregación de redes de la empresa para la protección de la red y actúa como una guía para quienes crean y mantienen una infraestructura de Tecnología de Información.

3. ALCANCE

Aplica a todos los sistemas, colaboradores y terceros que constituyen los sistemas de información de la empresa, con acceso a los sistemas.

a. Segregación en las redes

Se debe configurar un nivel apropiado de confianza en el nivel de dominio y los perímetros de dominio se deben asegurar usando un *firewall* donde corresponda.

Dentro de las redes, las de área local virtuales (VLAN) se usarán para segregar unidades organizativas, entre las cuales pueden ser: segregación por piso en el edificio, segregación de red por departamento, entre otros. Lo importante es que haya una segregación que se adapte en la organización y proteja la información.

En un ambiente de nube, es importante que se analice y definan los requisitos para segregar redes para lograr el aislamiento del interesado y se verifique la capacidad del proveedor de servicios en la nube para cumplir con estos requisitos.

PA-06

Apartado – Relación con proveedores

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

Asegurar la cadena de suministro

En el caso de que el proveedor haga uso de otras organizaciones subcontratadas dentro de la cadena de suministro, es responsabilidad del proveedor garantizar que estas organizaciones protejan la información de la empresa de acuerdo con los contratos establecidos.

- El proveedor no compartirá información clasificada de la empresa con terceros sin un permiso por escrito.

Establecer en los contratos, cláusulas de Seguridad de la Información que involucren al proveedor y subcontratados de este.

PA-07

Apartado – Disponibilidad de los recursos

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

Diseño de la Disponibilidad

Para los nuevos servicios, los requisitos de disponibilidad serán capturados como entrada a la etapa de diseño y se incorporará una resiliencia (capacidad de retorno o seguimiento) apropiada a los nuevos servicios para cumplir con estos requisitos.

Levar a cabo pruebas de aceptación del servicio para garantizar que se cumplan estos requisitos antes de que el servicio entre en funcionamiento. A partir de esta prueba, se generará un informe completo que indicará en qué medida se lograron los objetivos y qué medidas se deben tomar (si corresponde) para cumplir con los requisitos de disponibilidad.

PA-08

Apartado – Derechos de propiedad intelectual

Considerar el siguiente apartado en la política respectiva de Popular Pensiones:

Proteger la propiedad intelectual

Los problemas de derechos de autor no solo se aplican cuando la empresa hace uso del trabajo de otras personas. Los materiales originales que se producen con Popular Pensiones estarán sujetos a los mismos niveles de protección.

A menudo, el establecimiento de los derechos de propiedad intelectual se llevará a cabo como parte de un proceso de negocios y es importante que todos los empleados sepan qué propiedad intelectual tiene la operadora que debe protegerse de la infracción.

Sin embargo, para aquellos trabajos que se generen fuera de los procesos comerciales formales, deben recordarse las siguientes consideraciones:

- Asegurar que se incluya una reclamación de derechos de autor en todas las obras destinadas a la distribución externa.
- Estar alertas a los casos en que los derechos de autor, patentes, marcas comerciales o diseños industriales de la empresa se utilicen sin permiso.
- Reportar las sospechas sobre posibles infracciones al equipo legal.
- Considerar las cláusulas de la propiedad intelectual al enviar elementos que podrían denominarse propiedad intelectual de la empresa a otros fuera de la operadora.

Concientizar al personal sobre la ley, de lo que está y no está permitido respecto a la propiedad intelectual de la empresa.

REFERENCIAS

Catoria, F. (noviembre, 2013). ESET Intelligence Labs: GAP Analysis para empresas. Recuperado de https://www.welivesecurity.com/la-es/2013/11/13/eset-security-services-gap-analysis/

Cauas, D. (2015). Definición de las variables, enfoque y tipo de investigación. Bogotá: Biblioteca electrónica de la Universidad Nacional de Colombia, 2. Recuperado de https://s3.amazonaws.com/academia.edu.documents/36805674/l-Variables.pdf?response-content-disposition=inline%3B%20filename%3Dvariables_de_Daniel_Cauas.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20200103%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20200103T200430Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=74fdd62a8ecd75a205dcf9e611404af0eb9e50b941eab476f1478a0893d6a416

Hernández, R.; Fernández, C.; Baptista, P. (2014). Metodología de la Investigación. México: McGraw-Hill.

Manuel, S. L. J. (2017). Investigación educativa. Fundamentos teóricos, procesos y elementos prácticos (enfoque práctico con ejemplos. esencial para tfg, tfm y tesis). Editorial UNED. Recuperado de https://books.google.es/books?hl=es&lr=&id=c3CZDgAAQBAJ&oi=fnd&pg=PP1&dq=enfoques+exploratorio+de+una+investigaci%C3%B3n&ots=hIUjDlDYQv&sig=pv7P-8riFVEXIHhOXH7ermXUBqY#v=onepage&q=enfoques%20exploratorio%20de%20una%20investigaci%C3%B3n&f=false

Norma ISO 27001 (2013). Information technology - Security techniques - Information security management systems – Requirements.

Norma ISO 27002 (2013). Information technology - Security techniques - Code of Practice for Information Security Management.

Riquelme L. (diciembre, 2016). FODA: Matriz o Análisis FODA – Una herramienta esencial para el estudio de la empresa. Santiago, Chile. Recuperado de https://www.analisisfoda.com/

Rodríguez, L. (1995). Seguridad de la Información en Sistemas de Cómputo. México: Ventura Ediciones, S.A. de C.V.

APÉNDICE

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
A.5 Políticas de Seguridad de la Información	A.5.1 Dirección de la gestión para la Seguridad de la Información	A.5.1.1 Políticas para la Seguridad de la Información	¿Existe una o varias políticas aprobadas y comunicadas?	✓	**3**	**0,6**	Presenta documentación relacionada	Políticas de la institución
		A.5.1.2 Revisión de las políticas para la Seguridad de la Información.	¿Se revisan regularmente las políticas?	✓	**4**	**0,8**	Presenta documentación relacionada	Historial de revisión en las políticas y procedimientos
		Total		**2**	**4**	**1,4**		
A.6 Organización de la Seguridad de la Información	A.6.1 Organización Interna	A.6.1.1 Roles y responsabilidades de Seguridad de la Información	El personal involucrado en la gestión de TI, ¿tiene claro cuáles son sus responsabilidades en seguridad de la información?	✓	**4**	**0,8**	Brinda documentación. Se puede mejorar con una matriz de segregación de funciones	Normativa de la institución
		A.6.1.2 Segregación de funciones	¿Existe una adecuada segregación de tareas, cuando es apropiado?	✓	**3**	**0,6**	Presenta documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.6.1.3 Contacto con autoridades	¿Hay canales de comunicación abiertos con autoridades relevantes?	✗	**2**	**-**	Falta de documentación relacionada	
		A.6.1.4 Contacto con grupos de interés especial	¿Está la organización conectada con grupos que podrían ser de ayuda?	✓	**4**	**0,8**	Presenta documentación relacionada	Normativa de la institución
		A.6.1.5 Seguridad de la Información en gestión de proyectos	¿Los proyectos consideran la seguridad de la información adecuadamente?	✓	**4**	**0,8**	Presenta documentación relacionada	Normativa de la institución
	A.6.2 Dispositivos móviles y teletrabajo	A.6.2.1 Política de dispositivo móvil	¿Se gestionan los riesgos de dispositivos móviles?	✓	**4**	**0,8**	Presenta documentación relacionada	Normativa de la institución
		A.6.2.2 Teletrabajo	¿Son los sitios de teletrabajo seguros?	✗	**2**	**-**	Brinda documentación. Se puede mejorar documentación relacionada al teletrabajo.	
		Total		**5**	**3**	**3,8**		

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
A.7 Seguridad ligada a los Recursos Humanos	A.7.1 Previo al empleo	A.7.1.1 Investigación	En el proceso de selección de personal, ¿se verifican todos los candidatos para antecedentes laborales de manera apropiada y legal?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.7.1.2 Términos y condiciones de empleo	¿Los contratos de empleo cubren la seguridad de la información?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
	A.7.2 Durante el empleo	A.7.2.1 Responsabilidades de la Dirección	¿La gerencia hace cumplir adecuadamente la seguridad de la información?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.7.2.2 Toma de conciencia, educación y formación en seguridad de la información	¿Todos los empleados reciben entrenamiento de conciencia?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.7.2.3 Proceso disciplinario	¿Existe un proceso para disciplinar a los empleados que no siguen las reglas de seguridad de la información?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
	A.7.3 Finalización o cambio de empleo	A.7.3.1 Finalización o cambio de empleo	Cuando un colaborado cesa su contrato laboral, ¿se ha dejado en claro para todos los controles de seguridad de la información que todavía se aplican a ellos después de que se hayan ido?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		Total		**6**	**3**	**3,6**		
A.8 Gestión de Activos	A.8.1 Responsabilidad por los activos	A.8.1.1 Inventario de activos	¿Existe un inventario preciso de los activos e instalaciones de información?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.8.1.2 Propietarios de los activos	¿Todos los activos tienen un dueño?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.8.1.3 Uso aceptable de los activos	¿Existen reglas documentadas para el uso aceptable de los activos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.8.1.4 Devolución de activos	¿Se devuelven los activos al dejar el empleo?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
	A.8.2 Clasificación de la información	A.8.2.1 Clasificación de la información	¿Existe un esquema de clasificación de información?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.8.2.2 Etiquetado de la información	¿Está la información etiquetada según el esquema de clasificación?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.8.2.3 Manejo de los activos	¿Existen procedimientos de manejo de activos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.8.3 Manejo de los medios	A.8.3.1 Gestión de medios removibles	¿Los medios removibles son manejados de manera segura?	✗	**2**	**-**	Brinda documentación. Se puede mejor estableciendo lineamientos para la gestión de medios	Normativa de la institución
		A.8.3.2 Eliminación de medios	¿Se eliminan los medios de forma segura?	✗	**2**	**-**	Brinda documentación. Se puede mejor estableciendo lineamientos para la gestión de medios	Normativa de la institución
		A.8.3.3 Traslado de medios físicos	¿Están los medios protegidos durante el transporte?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**8**	**4**	**6,4**		

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
A.9 Control de Acceso	A.9.1 Requisitos del negocio para el control de acceso	A.9.1.1 Política de control de acceso	¿Está documentada una política de control de acceso?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.9.1.2 Acceso a redes y servicios de red	¿Hay usuarios restringidos a redes o servicios de red específicos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.9.2 Gestión del acceso de usuarios	A.9.2.1 Registro y cancelación de registro de usuarios	¿Está documentado un proceso formal?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.2.2 Aprovisionamiento de acceso a usuarios	¿Está documentado un proceso formal?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.2.3 Gestión de derechos de acceso privilegiados	¿Los derechos de acceso privilegiados se encuentran restringidos y controlados?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.2.4 Gestión de la información secreta de autenticación de usuarios	¿Se implementa un proceso de gestión formal?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.2.5 Revisión de los derechos de acceso de los usuarios	¿Los derechos de acceso son revisados regularmente por los propietarios de activos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.2.6 Eliminación o ajuste de los derechos de acceso	¿Se eliminan o modifican los derechos de acceso al abandonar o cambiar el rol?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Sub Sección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
	A.9.3 Responsabilidades de los usuarios	A.9.3.1 Uso de la información secreta de autenticación	¿Se han comunicado políticas sobre el uso de información de autenticación secreta, como contraseñas?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.9.4 Control de acceso a sistemas y aplicaciones	A.9.4.1 Restricción de acceso a la información	¿El acceso está restringido de acuerdo con la política?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.4.2 Procedimiento de accesos (log on) seguros	¿Existen procedimientos de inicio de sesión seguros donde sea apropiado?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.4.3 Sistema de gestión de contraseñas	¿Los sistemas de gestión de contraseñas aseguran contraseñas seguras?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.4.4 Uso de programas utilitarios privilegiados	¿Están tales programas restringidos en uso?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.9.4.5 Control de acceso al código fuente de los programas	¿Está protegido el código fuente?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**14**	**4**	**11,0**		
A.10 Criptografía	A.10.1 Controles criptográficos	A.10.1.1 Política sobre el uso de controles criptográficos	¿Hay una política establecida?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.10.1.2 Gestión de llaves	¿Hay una política establecida?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		Total		**2**	**3**	**1,2**		
A.11 Seguridad Física y Ambiental	A.11.1 Áreas seguras	A.11.1.1 Perímetro de seguridad física	¿Están definidos los perímetros de seguridad?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.11.1.2 Controles de entrada física	¿Están los controles de entrada en su lugar cuando sea apropiado?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.11.1.3 Aseguramiento de oficinas, salas e instalaciones	¿Se encuentra la seguridad física establecida? Por ejemplo, cerraduras, rejas	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.11.1.4 Protección contra amenazas externas y ambientales	¿Existe una protección física adecuada contra eventos perturbadores?	✗	**2**	**-**	Brinda documentación. Se puede mejorar con lineamientos ante amenazas externas y ambientales	Normativa de la institución
		A.11.1.5 Trabajando en áreas seguras	¿Existen procedimientos de trabajo seguros?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.11.1.6 Áreas de entrega y carga	¿Las áreas están aisladas y aseguradas?	✗	**2**	**-**	Brinda documentación. Se puede mejorar con lineamientos referente a las áreas de entrega y carga	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
	A.11.2 Equipo	A.11.2.1 Colocación y protección del equipo	¿El equipo está ubicado adecuadamente para la seguridad?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.11.2.2 Servicios de soporte	¿Está el equipo protegido de soportar fallas de servicios públicos cuando sea apropiado?	✓	**4**	**0,8**	Indica controles asociados a las descargas eléctricas. Remite documentación relacionada	Normativa de la institución
		A.11.2.3 Seguridad del cableado	¿Están protegidos los cables?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.11.2.4 Mantenimiento del equipo	¿Se mantiene correctamente todo el equipo?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.11.2.5 Remoción de activos	¿Existen procedimientos para permitir la remoción autorizada de activos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.11.2.6 Seguridad del equipo y los activos fuera de las instalaciones	¿Se aseguran adecuadamente los activos fuera del sitio?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.11.2.7 Seguridad en la eliminación o reutilización del equipo	¿Se limpian los medios de almacenamiento antes de reutilizarlos o desecharlos?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.11.2.8 Equipo desatendido por el usuario	¿Está seguro el equipo mientras está desatendido?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.11.2.9 Política de pantalla y escritorio limpio	¿Se mantienen despejados los escritorios y las pantallas cuando están desatendidos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**13**	**3**	**9,6**		
A.12 Seguridad de las Operaciones	A.12.1 Procedimientos y responsabilidades de los usuarios	A.12.1.1 Procedimientos de operación documentados	¿Se documentan todos los procedimientos operativos relevantes?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.12.1.2 Gestión de cambios	¿Existe un proceso de gestión del cambio?	✗	**1**	**-**	Falta de documentación relacionada	
		A.12.1.3 Gestión de la capacidad	¿Hay un plan de capacidad?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.12.1.4 Separación de ambientes de desarrollo, pruebas y operación	¿Están los ambientes separados en su lugar?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.12.2 Protección contra código malicioso	A.12.2.1 Controles contra malware	¿Hay controles antimalware en su lugar?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.12.3 Respaldo	A.12.3.1 Respaldo de la información	¿Existe una política de copia de seguridad?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
			¿Existe un calendario de pruebas?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.12.4 Registro y seguimiento	A.12.4.1 Registro de eventos	¿Se mantienen y revisan los registros adecuados?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.12.4.2 Protección del registro de información	¿Están protegidos los registros?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.12.4.3 Registros del administrador y operador	¿Las actividades son registradas y revisadas?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.12.4.4 Sincronización de reloj	¿Los relojes están sincronizados?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.12.5 Control de *software* operativo	A.12.5.1 Instalación de *software* en los sistemas de información	¿Se controla la instalación del *software*?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.12.6 Gestión de vulnerabilidades técnicas	A.12.6.1 Gestión de vulnerabilidades técnicas	¿Se identifican y gestionan las vulnerabilidades?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.12.6.2 Restricciones en la instalación de *software*	¿Los usuarios tienen restricciones para instalar *software*?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
	A.12.7 Consideraciones de auditoría de sistemas de información	A.12.7.1 Controles de auditoría de sistemas de información	¿Se planean auditorías para minimizar la interrupción de procesos de negocio?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**14**	**4**	**11,0**		
A.13 Seguridad en las Comunicaciones	A.13.1 Gestión de seguridad de la red	A.13.1.1 Controles de red	¿Se gestiona la seguridad de las redes?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.13.1.2 Seguridad de los servicios de red	¿Los acuerdos de servicios de red incluyen requisitos de seguridad, servicio y gestión?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.13.1.3 Segregación en las redes	¿Está la segregación de red en su lugar?	✗	**2**	**-**	Brinda documentación relacionada. Se puede mejorar estableciendo lineamientos del esquema topológico de la red.	
	A.13.2 Transferencia de información	A.13.2.1 Políticas y procedimientos de transferencia de información	¿Están protegidas las transferencias de información a través de políticas, procedimientos y controles?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.13.2.2 Acuerdos de transferencia de información	¿Está cubierta la seguridad de las transferencias en los acuerdos pertinentes?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.13.2.3 Mensajería electrónica	¿Se protege adecuadamente la mensajería electrónica?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.13.2.4 Acuerdos de confidencialidad y no divulgación	¿Se utilizan acuerdos de no divulgación cuando corresponde?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**6**	**4**	**4,8**		
A.14 Adquisición, desarrollo y mantenimiento de sistemas	A.14.1 Requisitos de seguridad de sistemas de información	A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información	¿Se considera la seguridad de la información al especificar nuevos sistemas?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.1.2 Asegurar los servicios de aplicaciones en las redes públicas	¿Están protegidos adecuadamente los servicios de aplicación a través de redes públicas?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.1.3 Protección de las transacciones de servicio de aplicación	¿Las transacciones de servicios de aplicación a través de redes públicas están protegidas adecuadamente?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
	A.14.2 Seguridad en los procesos de desarrollo y soporte	A.14.2.1 Política de desarrollo seguro	¿Las aplicaciones se desarrollan de forma segura?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.2.2 Procedimiento de control de cambios del sistema	¿Existen procedimientos formales de control de cambios?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.2.3 Revisión técnica de las aplicaciones después de realizar cambios de plataforma de operación	¿Se vuelven a probar las aplicaciones para la seguridad después de los cambios de plataforma?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.2.4 Restricciones en los cambios a los paquetes de *software*	¿Se minimizan los cambios en los paquetes de *software* y se administran con cuidado cuando es necesario?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.2.5 Principios de ingeniería de sistemas seguros	¿Se han establecido principios generales claros para crear sistemas seguros?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.14.2.6 Ambiente de desarrollo seguro	¿Están protegidos los entornos de desarrollo?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.14.2.7 Desarrollo contratado externamente	¿El desarrollo de *software* subcontratado se gestiona de manera efectiva?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.2.8 Pruebas de seguridad de sistemas	¿Se ha probado la seguridad de los desarrollos de *software* antes de la implementación?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.14.2.9 Pruebas de aceptación del sistema	¿Se realizan pruebas de aceptación?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
	A.14.3 Pruebas de datos	A.14.3.1 Protección de los datos prueba	¿Los datos de prueba están protegidos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**13**	**4**	**10,2**		
A.15 Relación con los proveedores	A.15.1 Seguridad de la información en la relación con proveedores	A.15.1.1 Política de seguridad de la información para las relaciones con los proveedores	¿Se evalúan y gestionan los riesgos asociados con el acceso de proveedores?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.15.1.2 Abordar la seguridad dentro de los acuerdos de proveedores	¿Se aborda la seguridad en los acuerdos con los proveedores?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.15.1.3 Cadena de suministro de tecnologías de información y comunicaciones	¿Se acuerda que los proveedores abordarán los riesgos dentro de su cadena de suministro?	✗	**2**	**-**	Con base en la documentación suministrada, se puede establecer lineamientos relacionados con la cadena de suministros de tecnología de información y comunicaciones.	
	A.15.2 Gestión de la entrega de servicios del proveedor	A.15.2.1 Seguimiento y revisión de los servicios de proveedores	¿Se evalúa regularmente la prestación de servicios al proveedor?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.15.2.2 Gestión de cambios en los servicios de proveedores	¿Se gestionan los cambios en los servicios del proveedor?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		Total		**4**	**3**	**3,0**		
A.16 Gestión de incidentes de Seguridad de la Información	A.16.1 Gestión de incidentes y mejoras en seguridad de la información	A.16.1.1 Responsabilidades y procedimientos	¿Existe un procedimiento de respuesta a incidentes de seguridad de la información?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.16.1.2 Reporte de eventos de seguridad de la información	¿Se informan los eventos de seguridad de la información de manera apropiada?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.16.1.3 Reporte de debilidades de seguridad de la información	¿Se identifican las debilidades en la seguridad de la información?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	¿Se evalúan los eventos de manera efectiva para establecer si representan incidentes?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.16.1.5 Respuesta a incidentes de seguridad de la información	¿Todos los incidentes se manejan de acuerdo con los procedimientos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.16.1.6 Aprendiendo de los incidentes de seguridad información	¿Se aprenden lecciones de incidentes pasados de seguridad de la información?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.16.1.7 Recolección de evidencia	¿Está la evidencia protegida apropiadamente?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		Total		**7**	**4**	**5,4**		
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio	A.17.1 Continuidad de seguridad de la información	A.17.1.1 Planificación de la continuidad de seguridad de la información	¿Se ha identificado el nivel de seguridad de la información requerido durante un evento perturbador?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.17.1.2 Implementación de la continuidad de seguridad de la información	¿Se mantiene la seguridad de la información durante un evento perturbador?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
		A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información	¿Los planes son probados y validados?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
	A.17.2 Redundancias	A.17.2.1 Disponibilidad de recursos de procesamiento de información	¿Se implementan niveles apropiados de redundancia para cumplir con los requisitos de disponibilidad?	✗	**2**	**-**	Realizan las buenas prácticas. Se puede mejorar definiendo la documentación para el control.	Normativa de la institución
		Total		**3**	**3**	**1,8**		
A.18 Cumplimiento	A.18.1 Cumplimiento de los requisitos legales y contractuales	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	¿Está claro qué requisitos legales, reglamentarios y contractuales deben cumplirse para cada sistema y en todos los ámbitos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.18.1.2 Derechos de propiedad intelectual	¿Se respetan y protegen los derechos de propiedad intelectual?	✗	**2**	**-**	Documentar propiedad intelectual	Normativa de la institución

Dominio de la Norma	Sección	Subsección	Requisitos - Preguntas	¿Requisito Cumplido?	Nivel de Madurez	Valor por nivel de Madurez	Comentarios	Evidencia
		A.18.1.3 Protección de registros	¿Están protegidos los registros de acuerdo con los requisitos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.18.1.4 Privacidad y protección de datos personales	¿Se cumplen las leyes de protección de datos?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.18.1.5 Regulación de controles criptográficos	¿El uso de la criptografía está en línea con las restricciones relevantes?	✓	**3**	**0,6**	Remite documentación relacionada	Normativa de la institución
	A.18.2 Revisión de seguridad de la información	A.18.2.1 Revisiones independientes de seguridad de la información	¿Se realizan revisiones independientes con regularidad?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.18.2.2 Cumplimiento con las políticas y normas de seguridad	¿La administración local se mantiene al tanto del cumplimiento en su área?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		A.18.2.3 Revisiones de cumplimiento técnico	¿Se revisan periódicamente los sistemas para confirmar que cumplen con las políticas y los estándares?	✓	**4**	**0,8**	Remite documentación relacionada	Normativa de la institución
		Total		**7**	**4**	**5,4**		