UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

FACULTAD DE INGENIERÍA INFORMÁTICA

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENIERIA DEL SOFTWARE

Título de la investigación:
Propuesta para la protección de activos físicos y digitales, basándose en las normas ISO/IEC 27001 y NIST SP 800-53 para la empresa Electric Cars of Costa Rica, ubicada en Heredia.

Nombre del estudiante:
Fernando José Artavia García

Tutor:
Carlos de la O

Sede San José

Septiembre, 2025

CONTENIDO

TABLAS

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del Problema

La empresa Electric Cars of Costa Rica es una entidad enfocada en la venta y mantenimiento de carros eléctricos con más de veinte años de experiencia en el mercado y se encuentra ubicada en Heredia. Esta empresa genera soluciones de movilidad amigables con el ambiente, tomando en cuenta que proporciona la distribución de dichas soluciones, siendo pioneros en este tipo de negocios innovadores para clientes en el área del hotelería, campos de golf y transporte, ya sea de carga o de personas.

Como todo depende del contexto o de la situación de cada cliente, se cuenta con personal altamente capacitado en la materia, para poder generar recomendaciones objetivas y moldeables a las demandas de cada cliente y proveer de esta manera un servicio de primera.

No obstante, la empresa, a pesar de su innovación y liderazgo en este mercado, ha presentado deficiencias en su apartado de seguridad de la información, creando un problema que puede tener afectaciones tanto en el largo como en el corto plazo y puede comprometer la confianza depositada de los clientes, su posicionamiento en el mercado y las respuestas ante incidentes de este tipo. Esto se ve reflejado en la actual gestión de sus activos físicos y digitales y en la falta de procedimientos y políticas que se encarguen de asegurar la información que maneja en sus operaciones y negocio.

Descripción del Problema

Acceso no controlado a la sala de equipos críticos: en esta sala están alojados equipos críticos de la empresa, es reconocible a simple vista y no cuenta con controles de acceso adecuados.

Uso inadecuado de protocolos de comunicación: los datos de los clientes viajan por protocolos no seguros.

Falta de procedimientos de respaldos y plan de restauración de los datos: los respaldos se realizan en lapsos semanales, lo que puede ser insuficiente en caso de un incidente grave, además de no contar con un plan de estructurado para la verificación de la integridad de las copias de seguridad ni un plan de restauración de los datos en caso de un incidente.

Accesos no autorizados a la infraestructura crítica: la infraestructura crítica de la empresa está expuesta a accesos no autorizados por falta de controles y la conexión interna y externa a dicha red, esto puede provocar exposición de los datos, posibilidad de ataques, interrupción de alguna operación crítica, entre otros problemas.

Falta de políticas de seguridad de la información: no existen políticas claras que regulen cómo se debe manejar y proteger la información de los clientes.

Objetivo General

Elaborar una propuesta de políticas y procedimientos de seguridad de la información para Electric Cars of Costa Rica, basada en las normas NIST SP 800-53 e ISO/IEC 27001, que permita la mitigación de vulnerabilidades, la protección de activos físicos y digitales y el establecimiento de controles de acceso y respuesta ante incidentes.

Objetivos Específicos

Crear un protocolo de seguridad física para la sala de equipos críticos, sustentado en un análisis de riesgos y que incluya controles de acceso físico conforme lo que dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.11.1.

Elaborar políticas y procedimientos de cifrado de comunicaciones que integren el uso de TLS, claves digitales y buenas prácticas de protección de los datos, conforme lo que dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.10.1.

Crear un plan de respaldos y recuperación de los datos, que incluya lineamientos de verificación e integridad según las normas NIST SP 800-53 e ISO/IEC 27001 A.12.3.

Elaborar documentos de gestión correcta de los activos críticos de la empresa, en los que se describa la segmentación y configuración de *firewall* y la política para el correcto acceso, con base en las normas NIST SP 800-53 e ISO/IEC 27001 A.8.1 y A.12.6.

Crear políticas de seguridad de la información según lo dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.5.1.

Justificación

La seguridad de la información en el entorno empresarial es uno de los aspectos más relevantes hoy en día en cualquier entidad, ya que las amenazas pueden perjudicar no solo sus servicios, sino también la confianza de sus clientes actuales e impedir la atracción de nuevos clientes. En un contexto donde dichos casos cada vez son más frecuentes y difíciles de predecir, es indispensable contar con medidas de seguridad de última generación para poder contrarrestarlos y asimismo responder de manera eficaz cuando se presenten.

En una actualidad, cuando los incidentes en materia de seguridad de la información son tan frecuentes, se requiere respuestas inmediatas, basadas en esquemas actualizados y con una funcionalidad pensada a largo plazo, a fin de que, en caso de presentarse algún acontecimiento, el equipo de trabajo de la empresa cuente con el plan, el conocimiento y la confianza para generar una respuesta eficaz sin comprometer su seguridad de la información.

Los resultados de esta investigación tienen una gran variedad de beneficios a corto y largo plazo para la empresa, entre ellos están: mayor seguridad, construcción de la confianza de los clientes, aumento del prestigio de la empresa, capacidad de respuesta ante accidentes informativos, entre otros. Lo anterior, además de ser beneficioso para la empresa, puede fomentar un impacto en la cultura empresarial del mercado laboral, de su apartado social y ético.

Viabilidad Técnica

La empresa posee una infraestructura técnica con la cual se puede trabajar esta propuesta. Se cuenta con servidores, red interna y externa, equipos para cada colaborador, base de datos, entre otros.

Esta estructura presenta una base sólida para implementar políticas y procedimientos de la seguridad de la información basados en marcos internacionales y altamente reconocidos como lo son las normas NIST SP 800-53 e ISO/IEC 27001. De esta manera, se trata de una implementación que potencia dicha infraestructura ya instalada y se beneficia de ella para poder incluir los políticas y procedimientos planteados en el estudio.

Viabilidad Operativa

Para la correcta realización de este proyecto se requiere un amplio conocimiento sobre la seguridad de la información, incluyendo elementos como las buenas prácticas, la identificación y mitigación de amenazas y la comprensión de conceptos y directrices básicas, como las que dictan las normas NIST SP 800-53 e ISO/IEC 27001.

Es de vital importancia la correcta documentación de las políticas y procedimientos expuestos en esta investigación, así como comunicarlos de manera efectiva al personal, para que puedan ser aplicados de manera eficiente y correcta. Para que esto se cumpla, se requerirá capacitar al personal para brindarle el conocimiento necesario para su correcta aplicación, además de proporcionar las soluciones expuestas en la propuesta.

De esta manera se tendría una base para que dichos colaboradores no solo entiendan de manera correcta las soluciones propuestas en este estudio, sino que también están informados de la importancia de aplicarlas en caso de ser necesario, saber en qué contextos un apartado puede ser más útil que otro, interiorizando el conocimiento y haciéndolo más robusto a la hora de ponerlo en práctica.

Viabilidad Económica

Costos de *software*: en este apartado se incluye la adquisición principalmente de *software* para la realización de análisis de riesgo y un reporte de postura sobre el sitio web para la detección de brechas de seguridad que expongan datos de los clientes o de la empresa.

Costos de *hardware*: en este apartado incluye el equipo que se va a utilizar para las evaluaciones de seguridad, creación de procedimientos y políticas de la propuesta.

Conectividad: Se utilizará para la proporción de comunicación a internet, descarga de normativas y trabajo de forma remota de la propuesta.

Documentación: costo de la creación de las políticas y procedimientos relacionados con la propuesta, además de su correcta comunicación al personal sobre su uso e importancia dentro del entorno empresarial, costos que pasan desapercibidos, como la impresión y los materiales necesarios para ello.

Tabla 1

Costos de la Investigación.

Nombre	Precio en colones
Software de Apoyo (Virus Total, CISCO talos, Qualys SSL, IBM X-forcé labs)	0
Normas (NIST SP 800-53 e ISO/IEC 27001)	75.000
Hardware	500.000
Conectividad	50.000
Documentación	10.000 (aproximado)

Fuente: elaboración propia, 2026.

Los montos mencionados muestran un esquema de la inversión que se realizaría en caso de adquirir los beneficios que se presentan en este estudio, siendo una inversión en una solución pensada para el largo plazo.

Viabilidad Legal

El desarrollo de esta investigación destinada para la empresa Electric Cars of Costa Rica debe cumplir ciertas directrices de acuerdo con la normativa costarricense vigente correspondiente a la materia de seguridad informática, a saber:

Ley n.° 8148 y adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal, donde tipifican y sancionan delitos informáticos en Costa Rica (2001).

Se relaciona con el proyecto ya que se busca el fomento de controles que prevengan accesos no autorizados, manipulación indebida de la información y ataques a los sistemas informáticos de la empresa en estudio, teniendo de esta manera una viabilidad legal para la realización de la propuesta.

Ley n.° 4573 (2001), la cual sanciona y reprime los delitos informáticos en ámbitos como la confidencialidad, la integridad y la disponibilidad de la información. Se determina que la investigación no infringe ninguno de estos principios ya que no participa ni fomenta dichas

conductas en el apartado de seguridad informática, teniendo de esta manera una viabilidad legal para su realización.

Ley n.° 6683 (1982), la cual se encarga de la protección de los datos y derechos de autor en la utilización de apartados bibliográficos, marcos internacionales y normativas de este tipo. Con respecto a la investigación por realizar se determina que no infringe dicha ley ya que las herramientas usadas serán de tipo *open source* y gratuitas, confirmando de esta manera la viabilidad legal de la investigación.

Ley n.° 8968 (2011), la cual se encarga de los apartados correspondientes a los datos personales y su tratamiento, garantizando de esta manera la privacidad de los ciudadanos de Costa Rica y sus datos. Se determina que esta investigación no infringe dicha ley ya que la información proporcionada por Electric Cars of Costa Rica se utilizará únicamente con fines de realización de este proyecto, garantizando de esta manera su protección y uso exclusivo para la investigación.

Proyecciones

La investigación tiene como objetivo la creación de políticas y procedimientos para la seguridad de la información de la empresa Electric Cars of Costa Rica y por medio de estos asegurar la seguridad informática, tanto de su infraestructura tecnológica presente como de la información de sus clientes, creando de esta manera una mayor confianza y aportando y mejorando la imagen de la empresa en general, gracias a la implementación de estándares internacionales en la seguridad de la información como las directrices NIST SP 800-53 e ISO/IEC 27001.

Alcance Funcional

El alcance funcional del proyecto define las acciones, procesos y componentes relevantes para su elaboración, en este caso se mencionan de manera específica los aspectos de la seguridad de la información relevante a los activos críticos de la empresa Electric Cars of Costa Rica y cómo se propone solucionar y delimitar el alcance propio de cada sección.

Nombre del apartado	Descripción del Apartado
Creación de protocolo de seguridad física (NIST SP 800-53 y ISO/IEC 27001 A.11.1)	1. Realizar un análisis de riesgos para identificar posibles vulnerabilidades en la seguridad física. 2. Elaborar un documento que establezca controles de acceso físico a la sala donde se instalan los equipos críticos de la empresa.
Elaboración de políticas y procedimientos para el cifrado correcto de las comunicaciones (NIST SP 800-53 y ISO/IEC 27001 A.10.1)	1. Generar un reporte de postura de seguridad del sitio web oficial de la empresa, con el fin de identificar posibles brechas de seguridad que expongan al cliente o su información (VirusTotal, IBM X Force, CISCO Talos, Qualys SSL labs). 2. Elaborar un procedimiento para la adopción de estándares como TLS y AES-256 para cifrar las transferencias de datos. 3. Crear una guía sobre buenas prácticas para el manejo de certificados digitales, gestión de claves y correcta rotación de estas.
Creación de protocolo de respaldo de los datos (NIST SP 800-53 y ISO/IEC 27001 A.12.3)	1. Definir un procedimiento para la generación de respaldos. 2. Crear un procedimiento de verificación periódica de la integridad de las copias de seguridad. 3. Crear un plan de restauración de datos en caso de incidentes.
Elaboración de documentos de gestión correcta de los activos críticos de la empresa (NIST SP 800-53 y ISO/IEC 27001 A.8.1 y A.12.6)	1. Crear una política donde se establezca el debido proceso para solicitar acceso a la red interna y su infraestructura. 2. Elaborar un procedimiento para la correcta configuración de un *firewall* que monitore y

	filtre el tráfico hacia el servidor para mayor seguridad.
Creación de políticas de seguridad de la Información (NIST SP 800-53 e ISO/IEC 27001 A.5.1)	1. Crear las políticas y procedimientos para asegurar la seguridad de la información de los activos críticos de la empresa basado en las normas NIST SP 800-53 e ISO/IEC 27001. 2. Desarrollar un manual de clasificación de datos según su nivel de confidencialidad. 3. Definir un protocolo de respuesta a incidentes y directrices para el uso de dispositivos personales.

Fuente: elaboración propia, 2026.

Este alcance se centra en una guía y resumen de los apartados de la propuesta, donde por medio de puntos específicos se dicta el proceder y cómo se propondrá solución paso a paso.

Alcance Metodológico

Realizar un análisis de riesgos a la infraestructura física de la empresa para detectar brechas de seguridad, más un reporte de postura de seguridad de su sitio web, además de los procedimientos de respaldo y restauración en caso de algún incidente, de esta manera se podrán mapear posibles riesgos informáticos y sus causas, así como señalar el impacto de que estos riesgos están presentes y sin solución. Partiendo de este punto se establecen propuestas de solución y maneras de atacarlos sin comprometer la seguridad informática de la empresa y de sus clientes.

Elaboración de políticas y procedimientos para la seguridad de los activos físicos y digitales de la empresa partiendo del estudio anteriormente mencionado, de esta manera, teniendo claros los riesgos, problemas y causas de las deficiencias de la seguridad de la información presentes en la empresa, se procede a la creación de las políticas y procedimientos, que serán concebidos de manera que se adapten exclusivamente a las necesidades de la empresa, para la mejora de su seguridad informática, partiendo de la guía y tutela de estándares internacionales como NIST SP 800-53 e ISO/IEC 27001.

Alcance Tecnológico

Para el fortalecimiento de la seguridad se utilizarán *softwares* de antivirus, encriptación de los datos y sus estándares (TLS y AES-256) y herramientas de tecnología con fines de seguridad informática (VirusTotal, IBM X Force, CISCO Talos, Qualys SSLlabs).

CAPÍTULO II: MARCO REFERENCIAL

La empresa Electric Cars of Costa Rica es una entidad que se dedica a la venta y mantenimiento de vehículos eléctricos, con servicios de renta de carros eléctricos, reacondicionados, venta de partes y accesorios. Es una empresa completamente de origen costarricense, la cual busca un enfoque completamente nuevo e innovador en la región, como se indica en la página web de la empresa (2025):

> En Electric Cars, nos enfocamos en ofrecer a nuestros clientes una amplia gama de opciones en vehículos eléctricos tipo golf, versátiles para utilizar en las diferentes áreas que requieren un alto rendimiento y para tan diversas tareas: hotelería, residenciales, industria, renta en playas, campos de golf, utilitarios para transporte de personas y de carga, entre otros. Somos representante y distribuidor de las marcas más reconocidas como lo son E-Z-GO y Cushman siendo las más prestigiosas del mercado mundial pertenecientes al conglomerado industrial estadounidense Textron. (párr.1).

Partiendo de este contexto, este marco referencial busca fundamentar la propuesta para la empresa Electric Cars of Costa Rica, dividiéndola en secciones que abordan apartados importantes, se define primero conceptos clave relacionados con la seguridad de la información y la correcta gestión de riesgos, los marcos normativos NIST SP 800-53 e ISO/IEC 27001 y el motivo por el cual fueron elegidos para esta investigación, además de su aporte, prácticas saludables en el ámbito de seguridad de la información, buenas prácticas entre los propios colaboradores en la empresa y la importancia de tener un plan de acción ante incidentes informáticos.

Finalmente, gracias a todos los elementos anteriormente expuestos, se ofrece una integración que conecta los conceptos, marcos y estudios mencionados con la problemática planteada en la empresa seleccionada para esta investigación.

Seguridad de la Información como Factor Determinante en la Actualidad

Al tratarse de un término tan amplio como la seguridad de la información, primero se debe hacer una distinción vital, este estudio se centra en el apartado de seguridad de la información y no de seguridad informática, ambos temas, aunque guardan similitudes y pueden llegar a entrelazarse, no son los mismos, según Villalón-Fonseca (2022: “La seguridad de la información cubre un

entorno más amplio, llevando a los requisitos del campo no solo el ámbito digital sino también el factor humano y físico del objeto de estudio" (p.5).

Este comentario destaca que la seguridad de la información es un tema de vital importancia para la empresa de estudio ya que esta posee problemas de activos físicos (equipos críticos, sala de servidores) y de activos digitales (operaciones, base de datos), siendo vulnerabilidades que deben ser gestionadas de una manera conjunta para su correcta corrección e implementación y así hacerlas efectivas.

Además, está el factor humano, que generalmente puede llegar a ser un tema ignorado cuando se incluye, pero es común que por errores de esta índole se den fugas de información sin intención, malas prácticas por parte de colaboradores de la empresa, malos respaldos o hechos en fechas muy distantes unas de otras, entre otros.

Según la International Organization for Standardization (ISO, 2022) se define el concepto como la "tríada CIA, que sus siglas corresponde a: Confidencialidad, Integridad y Disponibilidad" siendo estos tres términos los principales pilares donde se debe construir, basar los controles y lineamientos de seguridad de la información de cada organización (párr.1).

De igual manera, el National Institute for Standards and Technology (NIST, 2020) establece que la seguridad de la información de cada empresa debe poder garantizar la protección de activos críticos, ya sean físicos o digitales de amenazas tanto internas como externas de la organización, por medio de implementaciones de controles administrativos dentro de la empresa, ya sean técnicos o administrativos (párr.5).

Ampliando un poco la anterior cita, esto deja ver que la seguridad no solo depende de herramientas digitales, sino que también acoge en su término aspectos como la cultura organizacional de la empresa, más las políticas y procedimientos ante incidentes de esta índole.

Activos de Información

Los activos de información comprenden todos los recursos de la organización correspondiente a este apartado, para la empresa electa estos incluyen el total de activos físicos, digitales y humanos que tengan un rol de desarrollo, en sus operaciones y en la continuidad del negocio, según la International Organization for Standardization (ISO, 2022). Estos, para efectos

del estudio, cubren apartados mencionados presentes en la empresa como lo son base de datos, las redes internas y externas, la documentación y el propio conocimiento de los colaboradores de la empresa.

Según menciona el National Institute for Standards and Technology (NIST, 2020), la correcta gestión de los activos de una empresa requiere el establecimiento de todos los activos que se consideren críticos de manera documentada, para que de esta manera se asegure la adecuada protección en su ciclo de vida participe en la entidad (p.63).

Este apartado nos recalca no solo la necesidad de saber cuáles son los activos críticos, sino también quienes son los responsables de ellos, qué controles se aplican, si son efectivos ante incidentes comunes y de alta complejidad que garanticen su seguridad, dependiendo de si son de carácter físico o digital.

En el caso de Electric Cars Of Costa Rica, los activos de información se pueden dividir en las dos categorías:

Activos Digitales: base de datos de los clientes, ventas, respaldos, red interna y externa de la empresa.

Activos Físicos: salas críticas de servidores, dispositivos de red del complejo, documentación empresarial y portátiles de los colaboradores.

Una vez mencionados estos activos y definidos sus conceptos e importancia, se denota que la no presencia de controles adecuados de estos activos de información genera riesgos directos respecto al CIA (Confidencialidad, Integridad y Disponibilidad). Un ataque informático, por ejemplo, al apartado de servidores, y la pérdida de respaldos, por mencionar algunos posibles incidentes, pueden comprometer de manera grave la confianza del cliente y la propia operatividad de la empresa en el largo plazo.

Por ello, la gestión de activos requiere implementar políticas que aseguren su uso responsable y que estén alineadas con estándares internacionales como los de la International Organization for Standardization y el National Institute for Standards and Technology.

Gestión de Riesgos de Seguridad de la Información en Ambientes Empresariales

La gestión de riesgos en la seguridad de la información es un método generalmente sistemático para evaluar y tratar amenazas que pueden afectar la confidencialidad, la integridad y la disponibilidad de los activos. Según el National Institute for Standards and Technology (NIST, 2020):

> … esto complementa lo que sería un marco de riesgos convencional, pero con una integración más técnica, siendo más participe en la toma decisiones estratégicas dentro de la organización, gracias a esto, los riesgos se pueden asimilar más allá de un simple fallo técnico sino también su impacto en los apartados financieros, legales y de reputación en la empresa (p.4).

Una correcta gestión de los riesgos de la seguridad de la información permitirá el establecimiento de prioridades en la entidad, dando paso de esta manera a una estructura más lineal y ejecutable en un plan de acción contra incidentes, siendo un método de mitigación, prevención de amenazas y respuestas rápidas, pero sobre todo efectivas, ante incidentes de este tipo. Algunos ejemplos de protocolos posibles gracias a una correcta gestión son los protocolos de accesos, las políticas de respaldo o los cifrados.

En conclusión, la gestión de riesgos permite establecer un punto de partida para la correcta elaboración de políticas y procedimientos de la seguridad de la información, permitiendo identificar dónde está el problema, por qué se da y las maneras de mitigarlo, además de clasificar y definir un orden de cuáles serían los activos críticos de mayor prioridad con su correcta protección.

Controles de Seguridad como Herramienta de Mitigación

Una vez definida la gestión de riesgos de la seguridad de la información, corresponde referirse a los controles de seguridad, según Villalón-Fonseca (2022):

> Un control de seguridad es un método, herramienta o procedimiento para hacer cumplir un requisito de seguridad. Para definir e implementar controles de seguridad, cada requisito de seguridad debe considerarse al menos una vez. Es común que varios requisitos se apliquen

> con un solo mecanismo, pero también se pueden utilizar múltiples mecanismos para aplicar un requisito de forma multicapa.
>
> Hemos descrito el tipo de modelo para un proceso de seguridad que puede aplicarse a una amplia variedad de entornos de TI. (p.15).

Estos controles sirven principalmente como método para poder hacer o definir la implementación correspondiente en el apartado, esto para que no se vea afectado u opacado por alguna otra deficiencia que no se haya tomado en cuenta previo a una gestión de riesgo, sino que sea el mejor candidato para mitigar la deficiencia seleccionada. Una expansión sobre este apartado y algunos de sus beneficios los menciona el National Institute for Standards and Technology (NIST, 2020).

Para comprender las políticas, tecnologías y sectores, es necesario que los controles sean relevantes al implementarse. Emplear un catálogo de controles neutral en cuanto a políticas, tecnologías y sectores ofrece numerosos beneficios y anima a las organizaciones a:

• Centrarse en las funciones, capacidades de seguridad y privacidad necesarias para el éxito de la misión y el negocio, así como en la protección de la información y la privacidad de las personas, independientemente de las tecnologías empleadas en los sistemas organizacionales.

• Analizar cada control de seguridad y privacidad, para determinar su aplicabilidad a tecnologías, entornos operativos, funciones empresariales y comunidades de interés específicos.

• Especificar políticas de seguridad y privacidad como parte del proceso de adaptación para controles con parámetros variables.

Políticas y Procedimientos de Seguridad en la Protección de los Datos

Una vez hecha una gestión de los riesgos e identificación de los controles más adecuados para la protección de los activos de la organización, se procede con la elaboración de políticas de seguridad, según Sepúlveda, Cravero (2021), “Una política incluye diferentes componentes de gestión, entre los cuales están la gestión de activos, de usuarios, la infraestructura computacional, disposición adecuada de servicios de información y la gestión de acceso, entre otros” (p.2).

Partiendo de ese punto, se establecen también procedimientos dentro de estas mismas políticas, que son los que los definirán su uso dentro de la organización. Cabe recalcar que dichas políticas y procedimientos tendrán que pasar por un proceso de prueba y evaluación para poder lograr un refinamiento después de cierto periodo ya en uso.

Según el National Institute for Standards and Technology (NIST, 2020) se puede dividir en el siguiente procedimiento:

- Identificación de controles necesarios para la correcta elaboración de las políticas y procedimientos por ejecutar dentro de la organización.
- Documentación de estas y su orden de ejecución precisamente planeado por la organización, basándose en estándares internacionales.
- Implementación dentro de la organización y análisis para buscar defectos o mejoras puntuales a dichas políticas y procedimientos.
- Monitoreo continuo sobre la evolución dentro de la organización, para hacer un registro de su efectividad en la seguridad de la información y prevención de incidentes.
- Refinamiento para lograr una vida útil más longeva sin perder la calidad y efectividad de dichas políticas y procedimientos ante la detección, prevención y accionar de incidentes.

Este método permite que las políticas y procedimientos elegidos no sean permanentes, sino que estén en constante monitoreo y evolución dependiendo de las necesidades y nuevas amenazas. Tiene como objetivo alargar su vida útil dentro de la organización y sobre todo su efectividad e importancia dentro de ello. Esto conforme pase el tiempo necesario, hasta que necesiten un desarrollo total y desde cero por ya ser métodos obsoletos.

Normativas y Regulaciones Internacionales

En el mundo actual, marcado por la transformación digital, la dependencia en los diferentes sistemas de información y sus propósitos ha dejado de ser una novedad o añadidura en cualquier organización, para pasar a ser uno de sus mayores pilares y diferenciadores con respecto a la competencia, marca y reputación de cada empresa que los posee, esta dependencia no es algo malo a nivel operativo siempre y cuando se administre de una manera responsable y las implementaciones nacidas de ella estén construidas mediante procedimientos, marcos estudiados

y efectivos. Para el éxito no solo basta con generar dichas implementaciones, sino también mantenerlas seguras de todas amenazas cibernéticas y saber cómo detectarlas.

Según Villalón-Fonseca (2022):

> La parte más técnica de un proceso de seguridad se ocupa de la detección de vulnerabilidades y amenazas para los componentes objetivo del sistema, en el contexto de los objetivos de seguridad. Las amenazas y vulnerabilidades técnicas pueden obtenerse de bases de datos de vulnerabilidades en línea, sistemas de soporte de proveedores, comunidades en línea, foros digitales, etc. Una vulnerabilidad sin amenazas asociadas puede no considerarse en el proceso de seguridad, pero sí puede identificarse y monitorearse para detectar cambios. (p.15).

Como se ha indicado en los conceptos clave del estudio, esta cita recalca que la detección de las vulnerabilidades, principalmente las presentes en un sistema, pero no limitándose solo al apartado digital, es vital para la seguridad de la información de todas las organizaciones en la actualidad.

Ante esta realidad, se han desarrollado normativas, estándares y marcos de referencia que tienen como misión la incorporación de políticas, procedimientos y controles que ayuden a mitigar amenazas de todo tipo e índole, ya sean protección de activos, fraudes cibernéticos, accesos no autorizados, pérdida de datos por mala gestión de copias de seguridad y demás que pueden afectar las operaciones de la organización en temas de seguridad de la información.

Siendo dos de los marcos con más estudios y viabilidad aplicativa destacan la International Organization for Standardization (ISO) y el National Institute for Standards and Technology (NIST), siendo los electos para el estudio en cuestión con su diferente enfoque y misma misión, guiando a las organizaciones en la elaboración de estrategias efectivas en la seguridad de la información.

International Organization for Standardization

La norma ISO es un marco internacional principal para este estudio, es uno de los referentes como más historia y trayectoria en la época moderna, acumula ya varias versiones desde su creación, cada una refinada y adaptada a las nuevas problemáticas y amenazas de la actualidad,

siendo una de las más influyentes en el ámbito de la seguridad de la información a nivel mundial. Según la propia ISO (2022), este documento se ha elaborado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información de una organización se ve influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados, y el tamaño y la estructura de esta. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y brinda a las partes interesadas la confianza de que los riesgos se gestionan adecuadamente, siendo un pilar en la actualidad.

Esta norma es la base de varias políticas y procedimientos de empresas de renombre las cuales también fueron objeto de estudio para pulir sus ya presentes modelos y de esta manera adaptarse a las nuevas amenazas para la seguridad de la información de las empresas y seguir siendo un referente a nivel mundial por las organizaciones en este ámbito.

En términos prácticos y de manera resumida, algunos de los tópicos principales que acoge esta norma son los siguientes (ISO, 2022):

- Políticas de Seguridad
- Controles de Seguridad
- Factor Humano
- Protección Física y de Operaciones
- Respuesta ante Incidentes
- Cumplimiento Normativo

Los anteriores puntos son solo algunos de los más relevantes dentro de la norma, pero no necesariamente todos deben ser utilizados en cada organización, esta norma plantea un esquema o esqueleto bastante flexible, para que de esta manera sea aplicable a varias empresas y sus

necesidades específicas, sin sacrificar la calidad de sus metodologías implementadas dentro de la misma norma.

Esto pasa por cuanto el porqué se quiere aplicar la norma en cada organización puede variar su enfoque, y con eso se refiere a que se requiera solo una parte para que la empresa asegure su apartado de seguridad de la información con éxito.

En el caso de estudio actual en Electric Cars of Costa Rica, esta norma puede aplicarse de esta manera en aspectos como el reforzamiento de la seguridad de sus activos físicos, basados en los principios y metodología que la norma expone, siendo una opción bastante viable, confiable e internacionalmente reconocida para aportar de manera sólida a su seguridad de la información.

Su implementación, además, puede también respaldar y beneficiar en un futuro a la organización en temas como auditorías, correctos respaldos de los datos o bien clientes exigentes que busquen un factor definitivo de que sus datos -ya sean personales o empresariales- estén siendo tratados bajo marcos estrictos y actualizados.

El uso de esta norma no solo ayuda a la organización a ser mejor en temas tan relevantes como la seguridad de la información, sino que la propia implementación puede fomentar una mejor cultura laboral, una competencia más sana, que busque también el funcionamiento bajo las metodologías de esta norma, beneficiando al mercado costarricense en general en apartados de seguridad de la información y sobre todo en un mejor trato de los datos de clientes y colaboradores.

National Institute for Standards and Technology

El NIST es otro de los marcos internacionales más importantes de nuestra actualidad, aunque con un enfoque en el apartado práctico con respecto al ISO, esto no es para nada un problema, simplemente es otro punto de vista que puede resultar más útil o conveniente dependiendo de la organización que lo desee aplicar.

Para fines de este estudio se busca apoyarse en ambas para elaborar políticas y procedimientos con lo mejor que pueden ofrecer estos dos marcos, siendo que el NIST se centra más en los controles de seguridad y la importancia de la privacidad que sean aplicables a sistemas de información dentro de cada organización.

Este catálogo de controles de seguridad y privacidad proporciona medidas de protección para sistemas, organizaciones e individuos. Los controles están diseñados para facilitar la gestión de riesgos y el cumplimiento de las leyes federales, órdenes ejecutivas, directivas, regulaciones, políticas y estándares aplicables.

Con pocas excepciones, los controles de seguridad y privacidad del catálogo son neutrales en cuanto a políticas, tecnología y sector, lo que significa que se centran en las medidas fundamentales necesarias para proteger la información y la privacidad de las personas a lo largo de su ciclo de vida.

Si bien los controles de seguridad y privacidad son en gran medida neutrales en cuanto a políticas, tecnología y sector, esto no implica que sean ajenos a ellas. Comprender las políticas, tecnologías y sectores es necesario para que los controles sean relevantes al implementarse (p.16.).

Estos controles de seguridad están estructurados de una manera que sean aplicables para organizaciones de todos los tipos y con contextos diferentes, pero también llamando y dando especial importancia ciertos puntos (NIST, 2020):

- Centrarse en las funciones y capacidades de seguridad y privacidad necesarias para el éxito de la misión y el negocio, así como para la protección de la información y la privacidad de las personas, independientemente de las tecnologías empleadas en los sistemas organizacionales.
- Analizar cada control de seguridad y privacidad para determinar su aplicabilidad a tecnologías específicas, entornos operativos, funciones de la misión y el negocio, y comunidades de interés.
- Especificar las políticas de seguridad y privacidad como parte del proceso de adaptación para los controles con parámetros variables. (p.16.)

Esta norma también tiene un factor de escalabilidad y flexibilidad importante, permitiendo que la organización clasifique el nivel de riesgo de cada deficiencia y tenga la libertad de implementar controles de acuerdo con sus necesidades, que estas vayan evolucionando y adaptándose con la salida de nuevas publicaciones de la misma norma sin perder las sólidas bases y educación instruida por anteriores versiones.

Esta norma, mediante la adopción de controles para Electric Cars of Costa Rica, puede aportar un enfoque más complejo en sus medidas de seguridad de la información, así como una capa de profundidad, contando también con un apartado más práctico que complementa los ideales de gestión planteados en el apartado de la ISO.

ISO 27001 y NIST SP 800-53 como una Solución

Las normas ISO/IEC 27001 y NIST SP 800-53 son de los mayores referentes a nivel internacional en materia de seguridad de la información, siendo ambas mundialmente reconocidas como el estándar por varias empresas de renombre. Aunque ambas persiguen la meta de mantener y garantizar la confidencialidad, integridad y disponibilidad (CIA) de los activos de la información de las organizaciones que las implementan, presentan unas diferencias que merecen mención, ya que estas pueden variar el enfoque, la aplicabilidad y los objetivos a largo plazo de cada organización que las implementa.

El enfoque de elaborar una propuesta que incluya ambas se está volviendo más frecuente ya que las posibilidades que brindan para aportar a la seguridad de la información son más robustas, actualizadas y difíciles de contrarrestar para los atacantes que buscan beneficiarse de la falta de estas en su totalidad, o de las deficiencias que uno u otro marco puede tener.

Al tener ambos marcos el mismo propósito es difícil imaginar que su metodología sea diferente, esto se denota bastante en su aplicabilidad y a la hora de poner ambos marcos en práctica en caso de que se usen específicamente en la misma acción, de acuerdo con ISO (2022).

La ISO busca la implementación y manutención de la gestión de la seguridad de la información (SGSI), basándose principalmente en un proceso de adaptación continuo y con posibilidades de una certificación oficial. Siendo un esto un sello de garantía internacional que además de respaldar a la entidad, protege sus activos bajo estándares internacionales que están en la actualidad globalmente aceptados y son de la más alta calidad.

Además, busca la implementación de una cultura empresarial más preocupada por la seguridad de la información, informándola por medio de capacitaciones y entrenamiento de su personal para la respuesta ante incidentes y el proceder en caso de uno, priorizando de esta manera

apartados como los activos críticos de la empresa, el proceso que se deberá a llevar a cabo y los roles de cada colaborador, así como los lineamientos o políticas que van atados a ese proceder.

Esto significa que, además de indagar un apartado técnico puro, también busca que colaboradores de todas las ramas de la empresa comprendan la gravedad de un tema como la seguridad de la información y tengan la capacidad de detectar situaciones potenciales que pueden desembocar en un incidente que afecta a los activos y los datos tanto propios de la empresa como de los clientes, y así tener, en caso de ser necesario, respaldo de datos actualizados para no intervenir en las operaciones de la empresa.

Por su parte, el National Institute of Standards and Technology (NIST) posee un enfoque más directo y técnico a la hora de resolver estas problemáticas, en este estudio se destaca su publicación SP 800-53, que además de generar una introducción sólida y mantener la metodología de la propia NIST, proporciona un catálogo detallado de controles de seguridad y privacidad, siendo el pilar de dicha publicación. Esta información la amplía el NIST (2020):

> Los controles de seguridad son las salvaguardas o contramedidas empleadas dentro de un sistema u organización para proteger la confidencialidad, integridad y disponibilidad del sistema y su información, así como para gestionar los riesgos de seguridad de la información. Los controles de privacidad son las salvaguardas administrativas, técnicas y físicas empleadas dentro de un sistema u organización para gestionar los riesgos de privacidad y garantizar el cumplimiento de los requisitos de privacidad aplicables.
>
> Los controles de seguridad y privacidad se seleccionan e implementan para satisfacer los requisitos de seguridad y privacidad impuestos a un sistema u organización. Los requisitos de seguridad y privacidad se derivan de las leyes, decretos, directivas, regulaciones, políticas, estándares y necesidades de la misión aplicables para garantizar la confidencialidad, integridad y disponibilidad de la información procesada, almacenada o transmitida, y para gestionar los riesgos a la privacidad individual. (p.1).

Esta definición muestra que el NIST se centra en proveer mecanismos prácticos y de fácil medición para garantizar la protección de los activos críticos, pero su principal diferenciador con el marco de la ISO/IEC 27001 es la neutralidad y la aplicabilidad, como se comentó anteriormente.

Se centra en la defensa de la propia privacidad de la empresa y sus datos, brindando controles robustos que faciliten este procedimiento de acuerdo con las necesidades, método o interacción que se esté dando para la correcta transmisión de la información, más una capa de protección que permita que este procedimiento tenga control y privacidad.

El NIST (2020) amplía al respecto:

> Los programas de privacidad son responsables de gestionar los riesgos para las personas asociados con la creación, recopilación, uso, procesamiento, almacenamiento, mantenimiento, difusión, divulgación o eliminación (denominados colectivamente "procesamiento") de información de identificación personal (PII) y de garantizar el cumplimiento de los requisitos de privacidad aplicables. (p.13).

La privacidad en la seguridad de la información es un concepto bastante amplio debido a la gran medida de casos y contextos en que puede ser utilizada, como el NIST la define en su publicación, se centra en el apartado del personal y la información que se le relaciona, siendo otro enfoque principal del marco en esta sección.

En conclusión, más que ser diferentes en el sentido literal, ambas normas resultan ser complementarias siendo la ISO/IEC 27001 un marco que puede aportar una estructura y cultura dentro de la empresa sobre esta problemática, mientras que la NIST puede aportar controles robustos específicos para cada activo, ya sea físico o digital, según sus necesidades actuales y una adaptabilidad garantizada para el futuro. Esto es conveniente para el estudio de Electric Cars of Costa Rica, que carece de estos puntos, a pesar de tener una estructura tecnológica funcional, por tanto, estas normativas brindan refuerzo y certificación internacional en ámbitos de la seguridad de la información.

Además de brindar controles robustos con la posibilidad de moldearse a sus problemáticas empresariales, brindará también privacidad de los datos: cabe destacar que para que estas normas puedan tener un impacto duradero y sólido en cualquier ámbito que se aplique, debe darse la debida capacitación del personal, algo que está fuera del alcance de este estudio, pero sí es una de sus recomendaciones principales para que la propuesta desarrollada pueda ser asimilada con éxito por el personal encargado de la implementación de este estudio.

Riesgos Informáticos y Ciberamenazas

Ni la seguridad de la información, ni los marcos que velan porque se aplique en las diferentes empresas, pueden entenderse de manera correcta sin antes comprender de qué males son los que se están intentando defender, dado que en la seguridad de la información y en la informática en general siempre van a presentarse deficiencias y métodos que tendrán el propósito de afectar tanto de manera física como digital a la empresa. Esto es lo que se le conoce como un ciberataque, según Guaña-Moya (2022):

> El ataque informático o ciberataque se refiere a aquellas acciones deliberadas contra datos, software o hardware en sistemas o redes informáticas, acciones que pueden destruir, interrumpir, degradar o denegar el acceso.
>
> Para detectar o manejar un ataque cibernético, es importante conocer las debilidades de la red, así como también, es necesario que el equipo de seguridad cibernética comprenda el motivo del atacante, a qué datos podrían apuntar y por qué ocurrió el ataque. En consecuencia, es necesaria una planificación adecuada para hacer frente a un ataque cibernético, mediante lo que algunos autores identifican como modelado y análisis de ataques, que permite describir cómo se pueden modelar las amenazas para mitigar los ataques cibernéticos en cualquier organización. (pp. 3-4).

Entre estos modelos para buscar la mitigación de dichos ataques están los marcos que se encargan de defender de un impacto negativo en la confidencialidad, integridad y disponibilidad de la información (CIA), estos riesgos pueden surgir de varias maneras, ya sean por medio de factores internos dentro de la empresa, como lo pueden ser errores humanos, configuraciones que no se realizaron con el debido cuidado en equipos críticos, falta de políticas claras para la seguridad de la información, ausencia de controles, entre otros.

Estos riesgos internos manejan conceptos ya planteados anteriormente y pueden abarcar bastante en una organización, son los que abren las puertas también a los factores externos que son los que generalmente explotan estas vulnerabilidades, siendo principalmente el atacante partícipe de dichos factores externos.

De aquí, la importancia de poder tener la capacidad de identificarlos, clasificarlos y finalmente mitigarlos, estos apartados deben funcionar como un pilar para el desarrollo correcto de

un plan de seguridad, controles y políticas que se deseen implementar, de forma tal que sean sostenibles y también escalables con el tiempo, siendo esto último un punto importante ya que si dicha implementación no puede sufrir adaptaciones, quedaría obsoleta en muy poco tiempo, comprometiendo nuevamente la seguridad de la información de la empresa y exponiéndola a las nuevas amenazas modernas que dicha implementación no valoró al momento de su puesta en operación en la empresa.

Cada ciberataque puede variar su propósito y rol, esto quiere decir que el impacto puede depender de las intenciones del atacante y sus objetivos. Guaña-Moya (2022) define este procedimiento en cinco atributos clave:

Actores: mínimo existen dos actores involucrados en cada ciberataque: el propietario del activo al que se dirige y un adversario, lo cual indica que las definiciones de ciberataque no tienen que ver con la naturaleza de los adversarios, debido que las operaciones, tanto ofensivas como defensivas, pueden ser realizadas por naciones, empresas, grupos, colectivos o individuos.

Activos objetivo: estos activos incluyen redes y sistemas informáticos, información, programas o funciones residentes o en tránsito en sistemas o redes, infraestructura física operada por computadora y objetos físicos extrínsecos a una computadora, sistema informático o red.

Motivación: las motivaciones de los ataques cibernéticos incluyen el acceso a información segura o no autorizada, el espionaje y el robo de datos y dinero, seguridad nacional y causas políticas, así como propaganda o engaño.

Efecto en los activos objetivo: los ataques cibernéticos resultan en la alteración, eliminación, corrupción, engaño, degradación, inhabilitación, interrupción o destrucción de los activos, también en impedir el acceso a los activos.

Duración: Incluye la posibilidad de que un ciberataque se ejecute durante un período prolongado de tiempo.

Las amenazas cibernéticas pueden llegar a ser varias, a tal punto que se imposibilita enumerarlas todas, a modo de entendimiento, se mencionarán las principales amenazas que afectan a usuarios y, principalmente, a empresas.

Esto a debido que dependiendo del tipo de atributos pueden ser varias en un mismo ciberataque, además los objetivos del atacante y sus motivaciones pueden variar. Según Guaña-Moya (2022), las causas más comunes de estos males son las siguientes:

Malware es el nombre común para muchas versiones maliciosas de un programa, suele ser un código informático destinado a destruir datos o procesos, así como adquirir accesos no autorizados a una red, generalmente se proporciona como un enlace o archivo por correo electrónico para que el usuario haga clic en este o abra el archivo de programa maligno.

Los virus informáticos son programas especialmente diseñados para ser plagas, debido que proliferan de forma descontrolada y causan graves daños a los datos electrónicos. Estos programas malignos, que se amplifican entre archivos y computadoras, son sorprendentemente similares en virulencia, modos de propagación y vías evolutivas a lo largo del tiempo a los microbios que causan enfermedades infecciosas, principalmente porque ambos virus se transmiten de un huésped a otro y aunque los virus informáticos son una invención humana, el desarrollo sigue una ruta biológica bien conocida.

Spyware: Se conoce como *spyware* al tipo de *software* que se instala de forma subrepticia en la computadora de un usuario, monitorea la actividad de este e informa a un tercero sobre el comportamiento detectado.

Actualmente, el *spyware* representa una de las amenazas más comunes en Internet para las empresas y los usuarios de manera individual, debido que puede acceder a información confidencial y causar daños en la red. Es un tipo de *malware* que recopila y transmite información personal a empresas de datos, anunciantes o usuarios externos sin el conocimiento y consentimiento de los propietarios de los datos.

Las anteriores problemáticas se orientan más a los apartados puramente digitales de las empresas y usuarios que utilizan un sistema de información, son las más comunes y las que conciernen a este estudio en particular, pero no significa que otras de su mismo tipo no puedan afectar a dicha empresa, además de estos, los ciberataques pueden ser perpetrados de maneras menos directas y más sutiles, como los casos que Guaña-Moya (2022) menciona a continuación.

Phishing: el *phishing* es un método para intentar obtener detalles potencialmente valiosos, como nombres de usuario, contraseñas o datos médicos, por motivos maliciosos, mediante

comunicaciones dirigidas, como correos electrónicos o mensajes, en los que la parte atacante anima a los destinatarios a hacer clic en enlaces a sitios web que ejecutan código malicioso para descargar o instalar *malware.*

Ransomware: corresponde a un modelo de *malware* cuyo objetivo es cifrar información y datos valiosos de las organizaciones con el fin de exigir un pago como condición para permitir el acceso a ellos. Además, con frecuencia es usado para hurtar información delicada de las organizaciones, exigiendo un pago considerable para no hacerla pública a la competencia, autoridades o comunidad en general.

Estas amenazas tienen la capacidad de ser más destructivas, debido a su gran sutileza y dificultad de detección en entidades medianas o grandes, mezclan muchos conceptos y métodos digitales y de ingeniería social en varios casos, hasta llegar a puntos como la definición de *ransomware*, siendo esto específicamente el pináculo de las consecuencias que puede llegar a sufrir tanto un individuo como la propia empresas en general si no se trata estos temas con el debido cuidado y respeto que merecen.

En conclusión, los riesgos informáticos expuestos en esta sección más las ciberamenazas mencionadas representan el porqué de los marcos utilizados en este estudio y la importancia de que una empresa como Electric Cars of Costa Rica posea políticas y procedimientos con estándares internacionales y que cumplan con las necesidades de la empresa.

Buenas Prácticas de la Seguridad de la Información

La correcta gestión de la seguridad de la información no se limita a la implementación de normas internacionales, detección de amenazas o herramientas para mitigarlas. Para poder adquirir un buen desarrollo se necesita contar con buenas prácticas que orienten no solo a colaboradores, sino también a directivos para que apunten a un mismo objetivo. Se le debe dar una importancia clave en la organización y que además se fomente activamente la protección de dichos activos, ya sean de carácter físico o digital.

Estas prácticas no son precisamente rígidas o un esquema que deben seguir las organizaciones estrictamente, ya que cada empresa es diferente y dependerá bastante del contexto de cada una, se debe tener prácticas que impacten positivamente sus activos y que en términos generales aporten a la protección de la confidencialidad, la integridad y la disponibilidad.

Según ambos marcos (NIST e ISO), la aplicación de prácticas consistentes en materia de seguridad puede aportar a reducir apartados como los riesgos informáticos en todas sus formas, la mejora en la calidad y confianza que reciben los clientes, la optimización de procesos internos por medio del establecimiento de protocolos efectivos y actualizados para la prevención y la respuesta en caso de un incidente informático.

Entre las más destacadas según NIST (2020) e ISO (2022) se encuentran las siguientes:

Cultura y concientización del personal: se refiere principalmente a las posibilidades de una deficiencia en la seguridad de la información a causa de un error humano, por ello y como se ha mencionado, un personal capacitado en esta materia es vital para el éxito de una correcta seguridad, la empresa se debe asegurar de que todos los colaboradores que interactúan con los activos que tengan posibilidad de generar una brecha estén capacitados y sepan distinguir dichos riesgos.

Lineamientos: tener políticas estrictas de acuerdo con cada contexto de la empresa y que estas sean de conocimientos de todo el personal, siendo explícitas en apartados como uso, acceso y resguardo de la información y sanciones para aquel que las incumpla.

Buen uso de respaldos: se refiere a la gestión de copias de seguridad, que estas estén actualizadas y verificadas periódicamente, además que estén almacenadas en una ubicación segura, como lo pueden ser las instalaciones principales de la empresa.

Colaboración y cumplimiento normativo: se deber dar un mantenimiento y una alineación con las normativas y estándares internacionales, asegurando de esta manera que cumpla con todos sus requerimientos. La colaboración con organismos internacionales reguladores y la actualización constante frente a nuevas disposiciones legales ayudarán a que las medidas por las que optó la empresa estén alineadas con las mejores prácticas globales, tanto actuales como futuras.

Todas estas prácticas ayudarán a mantener la capacidad de la empresa para responder de manera adecuada a los riesgos específicos que enfrenta. De esta manera se cumple con la trinidad de conceptos (CIA) y ayuda a consolidar una imagen sólida ante los clientes y aliados estratégicos, ya sean nacionales o internacionales, en materia de seguridad de la información.

CAPÍTULO III: MARCO METODOLÓGICO

El marco metodológico representa una parte vital para toda la investigación, este apartado abordará todo lo relacionado con el enfoque y tipo de investigación que se utilizarán para este estudio, de esta manera se podrán definir métodos, técnicas y procedimientos para alcanzar los objetivos propuestos en el mismo estudio, también tocará temáticas como las características de los enfoques y tipos de investigación.

Hay varias maneras en loa que una investigación puede ser ejecutada, pero eso dependerá de su contexto y tipo, siendo esto un punto importante, ya que partiendo del conocimiento de los tipos de investigación que están presentes en la actualidad se definirán apartados y se seleccionará un tipo específico para la investigación. El porqué de esto es que en este capítulo se busca obtener una coherencia entre el problema que se está atacando, los objetivos propuestos de la investigación y las estrategias por emplear, permitiendo de esta manera que los resultados obtenidos al final del estudio sean basados en argumentaciones confiables, válidos en su tipo y con la capacidad de replicarse.

El correcto entendimiento de los tipos de investigación y su enfoque tiene como objetivo dar un sello de garantía, que estos resultados sean alineados con los objetivos y su problemática, de tal manera que exista una linealidad evidente durante todo el estudio, donde se vea y se entienda el contexto del problema hasta los resultados del estudio en sí, manteniendo un orden en el entendimiento de este y una correcta estructura.

En el caso particular de la empresa a la que se le está haciendo el presente estudio, Electric Cars of Costa Rica, una metodología sólida es un pilar fundamental, ya que lo que se busca es crear soluciones de seguridad de la información para la empresa, elaborando políticas y procedimientos que fortifiquen este apartado dentro de la empresa.

Siendo un tema tan amplio como ya se había mencionado, la seguridad de la información abarca aspectos humanos y organizacionales, por ende, un correcto enfoque metodológico aportará un correcto análisis tecnológico del entorno a disposición de la empresa, la compresión de factores humanos, administrativos y finalmente la elaboración de soluciones viables basado en marcos internacionales como lo son ISO/IEC 27001 y NIST SP 800-53.

Teniendo en claro lo anterior, se comenzará brindando una explicación sobre los enfoques de la investigación, el porqué es importante para la correcta estructura de un marco metodológico y sus diferentes tipos con sus respectivas características y cualidades.

Enfoque de la Investigación

El enfoque de la investigación son los métodos de análisis e interpretación de los datos relevantes en un estudio. Elegir el enfoque implica considerar factores como la naturaleza de la problemática por estudiar, la accesibilidad a datos relevantes para el estudio y si la finalidad de este puede ser práctica. Además, el enfoque comprende todo el proceso que se lleva a cabo durante la investigación, tomando en cuenta sus elementos y las etapas que conforma el estudio.

Este concepto es muy importante debido a que es aquel que le da una linealidad a la investigación, para que la problemática planteada esté alineada con los objetivos propuestos del estudio, su importancia es tal que sin su presencia aspectos como la definición del tema, el planteamiento y desarrollo de cualquier propuesta no podrían ser llevados a cabo con éxito, ya que no habría ningún enfoque en cómo determinar la recolección de los datos, su análisis e interpretación para el estudio por realizar.

Siendo el propósito fundamental de una investigación el difundir conocimiento sobre una problemática específica para luego darle una explicación o solución ya sea teórica, práctica o una mezcla de ambas, es vital que este concepto esté correctamente definido para cualquier propuesta que tenga un ámbito investigativo, como lo es el presente estudio.

Los enfoques pueden llegar a ser varios dependiendo de la problemática planteada, a lo largo de los años se han utilizado varias modalidades que permiten al investigador definir un enfoque correcto a su estudio, pero entre todos destacan dos principales enfoques en una investigación: el cuantitativo y el cualitativo; cabe recalcar que es perfectamente posible -y en algunos casos hasta conveniente- combinar ambas modalidades, lo cual nos deja con un enfoque adicional e independiente, que sería el enfoque mixto.

Cada enfoque tiene su propia manera de concebir y abordar el estudio, lo cual afecta la definición del propio problema, la elección de la teoría que fundamentará la investigación y que tipo de metodología se empleará para la recolección de datos y su posterior análisis e interpretación.

Además, la naturaleza de cada investigación puede demandar un enfoque específico para su realización, por esto se debe tener conocimiento sobre estos enfoques y la propia naturaleza de la investigación, ya que si no se le asigna el enfoque de manera correcta, por más datos y procedimientos que se lleven a cabo durante el estudio, si no se atacó la problemática bajo la tutela de un enfoque correctamente seleccionado, las soluciones pueden resultar defectuosas, invalidando el estudio por un enfoque mal planteado y seleccionado por el investigador. A continuación, se detalla cada enfoque.

Enfoque Cuantitativo

El enfoque cuantitativo, como su nombre lo indica, se basa en una medición numérica, puede incluir los análisis estadísticos de datos relacionados con el estudio presente. Su objetivo principal como enfoque es probar, mediante estas herramientas, la identificación de patrones y establecer relaciones entre variables, lo cual ayuda a obtener resultados objetivos dentro del estudio. Este enfoque amerita un razonamiento deductivo, donde las teorías o problemáticas existentes sirvan para generar una base de los instrumentos de medición que posteriormente serán puestos a prueba para obtener resultados y con base en estos validar o refutar las suposiciones o problemáticas planteadas. Para una definición más formal, Hernández Sampieri (2017) amplía:

> Es el método en el cual los investigadores parten de la proposiciones generales o más universales para llegar a una afirmación particular. Este método se utiliza principalmente en las ciencias formales (como las matemáticas y la lógica) y se fundamenta en el razonamiento. Así, por ejemplo, si se parte de las premisas “todo X es Y” y “A es X” se concluye que “A es Y”. (p.21.)

A este enfoque también se le conoce como método deductivo, ya que invita al investigador a esta misma acción por medio de encuestas, cuestionarios, mediciones de rendimiento o estadísticas que sean de utilidad para el estudio. Todo lo anteriormente mencionado puede medirse usando números y con base en ellos, sacar conclusiones que refuten o validen las soluciones propuestas, pueden incluso ayudar a enfocar de manera más específica la investigación y generar conclusiones más acertadas para el objeto de estudio. Algunas de sus características más relevantes, según Hernández Sampieri (2017) son las siguientes:

> Refleja la necesidad de medir y estimar magnitudes de los fenómenos o problemas de investigación. La recolección de los datos se fundamenta en la medición (se miden las variables o conceptos contenidos en la hipótesis). Esta recolección se lleva a cabo al utilizar procedimientos estandarizados y aceptados por una comunidad científica, debido a que los datos son producto de mediciones que se presenta mediante números (cantidades) que se deben analizar con métodos estadísticos (p.40-41).

La investigación debe ser lo más objetiva posible, si se sigue rigurosamente el proceso y de acuerdo con ciertas reglas lógicas, los datos generados poseen validez y confiabilidad, y las conclusiones derivadas contribuirán a la generación de conocimiento.

Estas son algunas de las características más importantes de este enfoque, las cuales también fortalecen y ayudan a asimilar en qué casos utilizar este enfoque investigativo, si es conveniente, o si solo algunos aspectos pueden resultar de utilidad para el estudio, dependiendo del contexto, pero eso sería ya considerado para un enfoque mixto.

Enfoque Cualitativo

El enfoque cualitativo, a diferencia de su contraparte el enfoque cuantitativo, ataca aspectos como la comprensión y descripción del fenómeno en profundidad, tomando en cuenta aspectos más teóricos como percepciones o experiencias de los participantes dentro del contexto de la problemática presentada en el estudio. De esta manera, su punto fuerte es la interpretación y la descripción de las problemáticas, con el fin de construir una hipótesis de la realidad estudiada. Hernández Sampieri (2017) refiere lo siguiente:

> Este es el método en el cual los investigadores parten de hechos particulares o concretos para llegar a conclusiones generales. Este método se utilizará principalmente en ciencias fácticas (naturales o sociales) y se fundamente en la experiencia. En la mayoría de las investigaciones en imposible que todos los casos particulares puedan ser estudiados, lo cual quiere decir que queda la posibilidad de casos en los cuales no se aplica una conclusión definitiva. (p.21).

Este método, a diferencia del otro, puede identificarse como más humano, por la profundidad e importancia que se les da a interpretaciones personales de cada individuo partícipe

del estudio, y por medio de estas prácticas se puede llegar a conclusiones igual de sólidas que su contra parte, ya que puede determinar puntos vitales que el enfoque cuantitativo puede pasar por alto con facilidad. Herramientas como las entrevistas, las observaciones directas y el estudio de casos anteriores pueden ser vitales también para la determinación de patrones que beneficien los propósitos del estudio, siendo un enfoque no tan predefinido o lineal, sino uno que busca ver el panorama completo por medio de experiencias o causas asociadas al comportamiento humano que los preceden. Algunas de sus principales características, según Hernández Sampieri (2014) son las siguientes:

> El enfoque cualitativo también se guía por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven, prime ro, para descubrir cuáles son las preguntas de investigación más importantes; y después, para perfeccionarlas y responderlas (p.7).

Estas características denotan y fortifican lo mencionado anteriormente, el enfoque se especializa en la profundización, tomando en cuenta los comportamientos humanos asociados a la problemática de estudio, pero dependiendo en gran medida del contexto en el que se está planteando dicha problemática y criterio interpretativo del investigador.

Enfoque Mixto

El enfoque mixto es básicamente un enfoque cuantitativo y cualitativo condensados en uno solo, con el propósito de tener lo mejor de ambos enfoques y sus ventajas. Se hace referencia como ventajas, básicamente, que al emplear un enfoque mixto se puede tener una visión más integral, profunda y contextualizada de la problemática del estudio. Por ende, este estudio asimila datos que sean de origen numérico y su recopilación de origen cuantitativo mutuamente con los que son recopilados por medio de testimonio o percepciones humanas de origen cualitativo. Una definición más formal la da Hernández Sampieri (2017):

> El avance de la ciencia se ha debido en parte, a la complementariedad de los métodos cuantitativo y cualitativo, pues las conclusiones generales que se derivan utilizando el primer método, pueden ser puestas aprueba utilizando el segundo.
>
> Por eso los métodos mixtos se han consolidado en la comunidad científica. También se les llama investigación integrativa, multi métodos, métodos múltiples entre otros, y representan procesos sistemáticos, empíricos y críticos de la investigación, que implican la recolección y el análisis integrado de datos de ambos tipos, para realizar inferencias y entender mejor el fenómeno que se estudia. (p.22.).

Lo que destaca esta cita es cómo se pueden abordar datos por medios cuantitativos, como la medición de datos por medio de la estadística y la recolección datos por medio de la experiencia humana, y pueden presentar resultados que aporten de manera positiva y más acertada que trabajando con ambos por aparte, siendo ahora un método único e independiente de los dos anteriormente mencionados debido a sus ventajas únicas si el caso de estudio y su contexto aplican para este enfoque investigativo.

Las características de este método son prácticamente las mismas mencionadas en los apartados individuales de ambos en enfoques, pero cabe recalcar que algunas de las utilidades y características de este enfoque mixto pueden variar dependiendo del contexto investigativo del estudio, ya que van a ver puntos que solo puedan ser aplicables si dicho estudio tiene un enfoque cuantitativo o cualitativo.

En caso de que se utilice un enfoque mixto y tenga por definición lo mejor de ambos enfoques, puede llegar a mermar en este aspecto en específico, debido a una mala elección, de ahí la importancia de conocer el contexto investigativo perfectamente para la correcta asignación de un enfoque, que cumpla con las necesidades del estudio y no dejarse llevar por un enfoque mixto que aunque sea muy sólido y descriptivo con los datos que su ejecución determina, puede llegar a no ser suficiente para algunos estudios que ameritan un enfoque específico de los ya mencionados.

Enfoque de Investigación Seleccionado

El enfoque que se ha seleccionado para esta investigación es el enfoque mixto, como anteriormente se mencionó, este combina las cualidades de un enfoque cualitativo y uno

cuantitativo a la vez, que busca maximizar aspectos del estudio que ameriten un trato diferente, pero igual de necesarios para responder a las incógnitas que la problemática principal plantea.

Un enfoque de este tipo para el presente estudio permitirá una compresión más amplia y precisa del problema por resolver, como lo es la gestión de la seguridad de la información en el entorno empresarial de Electric Cars of Costa Rica, ya que permitirá integrar datos técnicos medibles con percepciones, experiencias o comportamientos del personal involucrado en estos apartados dentro de la empresa.

Este enfoque es seleccionado en este estudio ya que la naturaleza de la problemática identificada abarca apartados técnicos, administrativos y humanos, pues por un lado existen deficiencias tecnológicas evidentes, como la falta de controles de acceso a salas de importancia crítica para la empresa, pero también carece de políticas por las cuales regirse en estos casos. Partiendo de no tener estos factores nacen unos nuevos, como la carencia de procedimientos adecuados para la seguridad de la información, ya que estos parten de las políticas que debería tener dicha empresa para operar de manera correcta, sumándole el desconocimiento propio del personal sobre prácticas óptimas de la seguridad de la información y su importancia.

Esto crea varios apartados que dependen unos de otros para poder ser ejecutados de manera correcta y con base en los estándares internacionales seleccionados para este estudio, siendo este mismo punto, el porqué se elige un enfoque mixto para el mismo, son apartados que se complementan entre sí, como se había mencionado en la explicación de un enfoque mixto se puede aprovechar este tipo de casos para sacar resultados más acertados y de gran utilidad para el planteamiento de un propuesta que sea beneficiosa para la empresa.

El componente cuantitativo de esta investigación permitirá la realización de un diagnóstico para medir el nivel de la seguridad de la información actual de la empresa, mediante herramientas como el análisis de riesgos y lo que dictan los marcos internacionales.

Esta información permitirá establecer una base de prioridades dentro del estudio, así como la clasificación de riesgos, incidentes registrados y el nivel de cumplimiento de los colaboradores, con las prácticas de la seguridad de la información en la actualidad.

Por otra parte, el componente cualitativo del estudio sería comprender el apartado humano, que incide en la seguridad de la información de la empresa. Por medio de observaciones y estudio

del entorno interno se buscará determinar el nivel de conocimiento del personal en la temática, así como debilidades en la comunicación interna, comportamientos o prácticas que puedan representar un riesgo para la protección de los activos, lo cual ayudará a la formulación de políticas realistas y sostenibles para el caso específico de Electric Cars of Costa Rica y sus colaboradores.

Tipos de Investigación

Los tipos de investigación son aquellos en los que toda investigación científica debe sustentarse, a fin de que oriente el proceso de recolección, análisis e interpretación de los datos obtenidos, su selección dependerá del planteamiento tanto de la problemática como de los objetivos del estudio en sí. Una definición más formal la proporciona Hernández Sampieri (2017):

> El alcance es una especie de pivote entre lo que encontraste en la revisión de literatura y formulación de la hipótesis. Del alcance dependerá tu estrategia de investigación, incluido el diseño, los procedimientos y otros elementos. Los alcances son cuatro: exploratorio, descriptivo, correlacional y explicativo, pero en la práctica, cualquier investigación puede incluir elementos de uno o varios (p.74).

Siendo cuatro los principales alcances como se les define en la anterior cita, dependerá del investigador la selección del tipo de investigación más apto para el estudio en cuestión, o al menos un enfoque principal, debido a que, dependiendo del estudio, puede requerir factores presentes en otros tipos de investigación para su ejecución. Esto no es un punto negativo, sino todo lo contrario, ya que permite darle versatilidad y de esta manera responder a las incógnitas planteadas en el estudio con mayor precisión y facilidad.

Investigación Exploratoria

La investigación exploratoria es aquella que entra en juego cuando la temática propia de la investigación puede llegar a ser muy innovadora o se adentra en un territorio en el cual no hay muchos estudios a disposición del investigador. Hernández Sampieri (2017) lo define de la siguiente manera:

> Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o que no se ha abordado antes. Es decir, cuando la revisión de la literatura se revelo, tan solo hay guías no

> investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si queremos indagar sobre temas y áreas desde nuevas perspectivas. (p.75).

Este estudio se enfoca principalmente en el apartado de lo desconocido por la ciencia, en donde depende del ingenio humano crear un estudio que permita establecer las bases de un nuevo campo, o indagar de manera completamente pionera en temas que para la ciencia de hoy en día es desconocido, este tipo de investigaciones ha sido un pilar fundamental para el desarrollo de la humanidad y su conocimiento, aplicando la manera más efectiva y poderosa de adquirir y aprender nuevo conocimiento: la prueba y el error.

Investigación Descriptiva

Las investigaciones descriptivas, a diferencia de las exploratorias, atacan otro enfoque completamente diferente, ya que parten de una base de propiedades y características del objeto de estudio, para generar un análisis de los datos recopilados de estas cualidades y proporcionar resultados de estos. Este estudio amerita de métodos ya estudiados para poder usar los datos proporcionados por las cualidades del objeto de estudio, para poder operar de manera correcta. Según Hernández Sampieri (2017), una definición para este tipo es la siguiente:

> Con los estudios descriptivos se busca especificar las propiedades, características, perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, mide o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno que se investiga. En un estudio descriptivo el investigador selecciona una serie de cuestiones (que denominamos variables) y después recaba información sobre cada una para representar lo que si investiga. (p.76).

Este tipo de investigación tiene una base fuerte en la recolección de datos y sus métodos para recabarlos, es un tipo de investigación mucho más flexible y adaptable con todo el material académico a disposición de los investigadores hoy en día, siendo un método más común en varios estudios académicos y científicos por su versatilidad y facilidad para asimilar datos, proporcionando resultados óptimos a los investigadores, que los apliquen de manera correcta en sus estudios.

Investigación Explicativa

Este tipo de investigación va un paso más allá de la anterior, ya que rebusca principalmente en las raíces de la problemática planteada e intenta eliminarla desde ese punto, asimilando más que todo el porqué de la causa de las problemáticas y los fenómenos que se relacionan con ella, una definición más formal para este tipo de investigación la comenta Hernández Sampieri (2017):

> Con los estudios explicativos son más que la descripción de conceptos o fenómenos o el establecimiento de relaciones entre variables, más bien, están diseñados para determinar las causas de los eventos y fenómenos físicos y sociales. Como su nombre lo indica, su interés se centra en explicar porque ocurre un fenómeno y en qué condiciones se manifiesta, o porque se relacionan dos o más variables. (p.78).

Este tipo de investigación también permite un enfoque más profundo de la problemática planteada una vez puesta en acción, ya que puede evidenciar carencias y explicar el cómo se llegó a ellas en un primer lugar, proporcionando no solo una base sólida, sino también una puesta en evidencia de los factores que llevaron a la existencia de dicha deficiencia dentro del objeto de estudio.

Tipo de Investigación Seleccionado

El tipo de investigación seleccionado para el presente estudio es el descriptivo ya que el propósito principal es la elaboración de políticas y procedimientos con el fin de proteger activos críticos para la empresa; para ello se deberá pasar por un proceso de análisis y detalle de la seguridad de la información presente en Electric Cars of Costa Rica, características propias de este tipo de investigación.

Además, este enfoque permitirá a la investigación determinar por qué se manifiestan las deficiencias presentes en la gestión de dichos activos dentro de la empresa, identificando gracias a su estudio, condicionales que influyen en el nivel de seguridad de la empresa, apartado crítico para la elaboración de políticas y procedimientos efectivos con el fin de enmendar dicha brecha de seguridad.

Esta selección además se alinea con otro punto importante que invalidaría el uso de otro tipo de investigación para el estudio, no se busca la experimentación ni el establecimiento de

relaciones que tengan una causa y un efecto en específico, características de una investigación explicativa. Tampoco se busca explorar en una temática desconocida o un tema poco abordado y estudiado como lo sería en el caso de una investigación exploratoria.

Mediante el enfoque electo, se podrá realizar un diagnóstico adaptado a la problemática, que sirva de base para la formulación de la propuesta como tal de políticas y procedimientos para el fortalecimiento de la seguridad de la información, además de que varios puntos en la problemática ya expuesta, como lo son la falta de controles de acceso, respaldos, cifrados, aspectos humanos, entre otros, podrán ser abordados de manera más completa con este tipo de investigación.

Otro aspecto importante es que el propio estudio se apoya y basa principalmente en los marcos internacionales electos -NIST SP 800-53 e ISO/IEC 27001-, marcos ya estudiados y probados en la sociedad internacional, siendo estos los principales referentes para la investigación y su problema por resolver, invalidando los usos de un tipo investigación exploratorio totalmente y no cumpliendo con muchas de las características clave de un tipo de investigación explicativo, aunque no limitándose a incluir alguna de sus cualidades para reforzar su causa, dejando la opción descriptiva como la más apta para llevar a cabo la tarea.

En conclusión, basado en lo anteriormente mencionado, un tipo de investigación descriptiva es la que más se adapta a las necesidades de este estudio, gracias a cómo este tipo de investigación puede presentar una visión completa de la problemática existente, de tal manera que permita una linealidad y conexión entre los objetivos del estudio, el problema y las propuestas que se plantea para darle solución. A través de este tipo de investigación, se busca que el presente estudio no solo documente la realidad actual de la seguridad de la información de Electric Cars of Costa Rica, sino que también sirva como base sólida y escalable para la mejora continua, en los apartados de seguridad de la información de los activos críticos de la empresa, tanto actualmente como en el futuro.

Fuentes de Información

Las fuentes de información son todos aquellos recursos que son utilizados con el fin de proporcionar datos confiables sobre algún tema en específico. Cada investigación debe disponer no solo de una sola fuente, sino de varias que justifiquen y complementen todos los aspectos del estudio en sí, dándole una credibilidad y validación académica al estudio en el que se trabaja. Estas

fuentes además deben poder ser consultables por el lector para garantizar la existencia y veracidad de lo que mencionan, por esto mismo es necesario tener más de una sola fuente para un tema o estudio además de la propia visión expuesta en él, funcionando como un pilar de la propia investigación.

El tipo y enfoque de investigación se relacionan directamente con este apartado ya que dependiendo de ellos y de los objetivos de estudio se consultarán diferentes formatos de fuentes que sean relevantes para el estudio, como pueden libros, encuestas, documentos de instituciones reconocidas, entrevistas, periódicos y videos, entre otros.

Cada fuente de información debe ser considerada confiable y esto será medido en el sentido de qué tan comprobable es la información presentada en dicha fuente, siendo esto otra de las razones de por qué se deben consultar varias y conocer el origen y reconocimiento de dichas fuentes, para que sean útiles para la investigación.

Fuentes de Información Primaria

Las fuentes de información primaria son todas aquellas que se consideren el origen de la información o que sean de primera mano, son como su nombre lo indica, son los principales referentes para el estudio por realizar debido; la definición de esta la presenta Maranto (2015):

> Este tipo de fuentes contienen información original es decir son de primera mano, son el resultado de ideas, conceptos, teorías y resultados de investigaciones. Contienen información directa antes de ser interpretada, o evaluado por otra persona. Las principales fuentes de información primaria son los libros, monografías, publicaciones periódicas, documentos oficiales o informes técnicos de instituciones públicas o privadas, tesis, trabajos presentados en conferencias o seminarios, testimonios de expertos, artículos periodísticos, videos documentales, foros. (p.3).

Estas fuentes son las que más deben ser estudiadas previo a su selección para el estudio, ya que son un pilar fundamental. Son las que proporcionarán una base sólida a los demás tipos de fuente para su correcto desarrollo y aporte dentro de la investigación.

Fuentes de Información Secundarias

Las fuentes secundarias son todas aquellas que son existentes y que se apoyan en fuentes primarias. Son las encargadas principalmente de sustentar conceptos puntuales, aclarar dudas de poca complejidad en cuanto a la temática de estudio y sobre todo sustentar y apoyar las fuentes primarias; proporcionan una interpretación diferente partiendo de los mismos principios expuestos en el primer grupo. Al respecto, Maranto (2015) comenta:

> Este tipo de fuentes son las que ya han procesado información de una fuente primaria. El proceso de esta información se pudo dar por una interpretación, un análisis, así como la extracción y reorganización de la información de la fuente primaria. (p.3).

Cabe destacar que estas también pueden ser principalmente interpretaciones o menciones a fuentes primarias vistas en el contexto de estudio de la fuente secundaria consultada, esto no lo hace inservible para el estudio dentro de la propia investigación, sino todo lo contrario ya que proporciona una diferente perspectiva aplicable, basado en los términos expuestos de una fuente primaria.

Fuentes de Información Terciaria

Las fuentes terciarias son principalmente compilaciones, catálogos o bases de datos que resumen información alojada principalmente en una fuente secundaria, sin contar con un referente específico, siendo su objetivo principal la ampliación de materiales disponibles dentro de la fuente secundaria consultada, para fortalecer la veracidad del estudio. Una definición más formal la brinda Maranto (2015):

> Este tipo de fuentes son las que recopilan fuentes de información primarias o secundarias. Estas fuentes son utilizadas para buscar datos o para obtener una idea general sobre algún tema, algunas son; bibliografías, almacenes, directorios, donde se encuentran la referencia de otros documentos, que contienen nombres, títulos de revistas y otras publicaciones. (p.3)

La anterior cita presenta de mejor manera dónde se puede encontrar una fuente terciaria, cabe destacar que estas variables tienen un objetivo principal similar a las secundarias, pero antes de su uso se debe tener una base sólida de fuentes, tanto primarias como secundarias, para que

puedan aportar algo significativo y complementario a los otros dos tipos de fuentes ya presentes dentro de la investigación.

Variables

Las fuentes terciarias son principalmente compilaciones, catálogos o bases de datos que resumen información alojada principalmente en una fuente secundaria, sin contar con un referente específico, siendo su objetivo principal la ampliación de materiales disponibles dentro de la fuente secundaria consultada, para fortalecer la veracidad del estudio. Una definición más formal la brinda Maranto (2015):

> Este tipo de fuentes son las que recopilan fuentes de información primarias o secundarias. Estas fuentes son utilizadas para buscar datos o para obtener una idea general sobre algún tema, algunas son; bibliografías, almacenes, directorios, donde se encuentran la referencia de otros documentos, que contienen nombres, títulos de revistas y otras publicaciones. (p.3).

La anterior cita presenta de mejor manera dónde se puede encontrar una fuente terciaria, cabe destacar que estas variables tienen un objetivo principal similar a las secundarias, pero antes de su uso se debe tener una base sólida de fuentes, tanto primarias como secundarias, para que puedan aportar algo significativo y complementario a los otros dos tipos de fuentes ya presentes dentro de la investigación.

Variables Conceptuales

Las variables conceptuales son todas aquellas que tiene un concepto específico definido. Se especializan en describir la esencia propia de la variable y sus respectivas características, que las adecuan a los requerimientos de la investigación presente. Algunos ejemplos pueden ser conceptos científicos, definiciones académicas, entre otros.

Variables Operacionales

Las variables operacionales, a diferencia de las conceptuales, definen cómo se llevará cabo una variable conceptual, en pocas palabras, es llevar a la práctica lo expuesto en una variable conceptual con el objetivo de medirla o evaluarla de acuerdo con el contexto de la investigación.

Esta se enfoca en determinar el comportamiento o cumplimiento del fenómeno de estudio, gracias a esto se podrá obtener un resultado que sea de aporte a la investigación.

La practicidad de estas variables además le al propio investigador da una guía del proceder, para probar lo expuesto dentro del estudio y resolver la problemática presente, por medio de lo planteado en los objetivos, dando linealidad a la investigación.

Variables Instrumentales

Las variables instrumentales, hacen referencia a las herramientas o instrumentos que se utilizan para obtener y analizar los datos relacionados a variables conceptuales y operacionales. Éstas son como tal, el puente entre el apartado conceptual y operacional de este apartado, ya que define los medios en como los conceptos expuestos en los objetivos serán sometidos a prueba por medio de las herramientas e instrumentos que estas variables facilitan al investigador.

Las variables instrumentales hacen referencia a las herramientas o instrumentos que se utilizan para obtener y analizar los datos relacionados con variables conceptuales y operacionales. Son el puente entre el apartado conceptual y el operacional, ya que define los medios como los conceptos expuestos en los objetivos serán sometidos a prueba por medio de las herramientas e instrumentos que estas variables facilitan al investigador.

Para tener unas variables instrumentales definidas de manera clara, se debe tomar en cuenta las dos anteriores, ya que si no se realiza la linealidad de este procedimiento, no determinará resultados de utilidad para la investigación. Su diseño debe ser enfocado en evitar errores graves en la recolección de la información, para mantener una integridad y calidad de los resultados.

Tabla 2

Unidades de Análisis.

Objetivo específico	Variable	Variable conceptual	Variable Instrumental	Variable Operacional
Crear un protocolo de seguridad física para la sala de equipos críticos, sustentado en un análisis de riesgos y que incluya controles de acceso físico conforme lo que dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.11.1.	Seguridad física	Según International Business Machines Corporation (IBM, 2025a) "La seguridad física consta de: Seguridad del sitio, Redundancia de hardware, Recuperación de negocio y Archivado de datos" (párr.1).	Guía de Observaciones Guía Entrevistas	Observación Entrevista
Elaborar políticas y procedimientos de cifrado de comunicaciones que integren el uso de TLS, claves digitales y buenas prácticas de protección de los datos, conforme lo que dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.10.1.	Cifrado de comunicaciones	Según Matthew Kosinki (2025): El cifrado es el proceso de transformar texto simple legible en texto cifrado ilegible para ocultar información confidencial a usuarios no autorizados. Las organizaciones utilizan habitualmente el cifrado en la seguridad de datos para proteger la información confidencial del acceso no autorizado y las filtraciones de datos. (párr.1)	Guía de Entrevistas Guía de Encuestas	Entrevista Encuestas
Crear un plan de respaldos y recuperación de los datos, que incluya lineamientos de verificación e integridad según las normas NIST SP 800-53 e ISO/IEC 27001 A.12.3.	Respaldos y recuperación de los datos	Según International Business Machines Corporation (IBM, 2025b): "La recuperación de datos empresariales es el proceso de restaurar los datos perdidos, dañados, eliminados accidentalmente o inaccesibles a su servidor, ordenador, dispositivo móvil o dispositivo de almacenamiento (o en un nuevo dispositivo si el dispositivo original ya no funciona)" (párr.1). Según International Business Machines Corporation (IBM, 2025a): La copia de seguridad y la restauración se refieren a tecnologías y prácticas para realizar copias periódicas de datos y aplicaciones en un dispositivo secundario separado y luego utilizar esas copias para recuperar los datos y las aplicaciones, y las operaciones comerciales de las que dependen. (párr.1)	Guía de Observaciones Guía de Encuestas	Observación Encuesta
Elaborar documentos de gestión correcta de los activos críticos de la empresa, en los que se describa la segmentación y configuración de *firewall* y la política para el correcto acceso, con base en las normas NIST SP 800-53 e ISO/IEC 27001 A.8.1 y A.12.6.	Activos críticos	Según International Business Machines Corporation (IBM, 2025c): El término "activo" puede referirse tanto a bienes físicos como inmateriales que las empresas poseen y utilizan para generar valor. Ejemplos de activos físicos incluyen maquinaria, fábricas, material de oficina, plantas de producción, líneas de montaje, flotas de vehículos, edificios e infraestructuras civiles. Ejemplos de activos inmateriales incluyen software, propiedad intelectual, marcas registradas y patentes. (párr.1)	Guía de Entrevistas Guía de Observaciones	Entrevista Observación
Crear políticas de seguridad de la información según lo dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.5.1.	Políticas de seguridad de la información	Según International Business Machines Corporation (IBM, 2025c): La política de seguridad define qué es lo que desea proteger y qué espera de los usuarios del sistema. Proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual. Describe responsabilidades del usuario como las de proteger información confidencial y crear contraseñas no triviales. (párr.3)	Guía de Entrevistas Guía de Observaciones Guía de Encuestas	Observación Entrevista Encuestas

Fuente: Elaboración propia.

Población

La población es el universo completo relevante a la investigación, siendo como tal la totalidad que le concierne al mismo estadísticamente hablando. Esta población se base en un grupo de personas y objetos de cualquier tipo de naturaleza ya que, a vista de un estudio probabilístico, la población puede ser referida a cualquiera de estos dos grupos, la delimitación de esta es un factor importante para sacar una muestra efectiva para el estudio, este apartado lo amplía Hernández Sampieri (2017) de la siguiente manera: "La deficiencia que se presenta en algunos trabajos de investigación es que no describen lo suficiente las características de la población o consideran que la muestra la representa de manera automática. La población debe delimitarse de manera muy concreta" (p.130).

Una vez definida de manera correcta la población, se puede pasar al cálculo de la muestra, la cual será la encargada de ayudar al investigador en la resolución, por medio del uso de los instrumentos propuestos para resolver la problemática de la investigación. En el caso de Electric Cars of Costa Rica, su población sería de 21 en total, que será con la que se va a trabajar en este estudio.

Muestra

La muestra es básicamente una pequeña parte de la población relevante al estudio por realizar, será la que se someta a los instrumentos que darán veracidad a la investigación en una ambiente controlado y completamente aleatorio, para que los datos recogidos sean de utilidad para generar un veredicto a la investigación. Una definición más formal la brinda Hernández Sampieri (2017):

> Una muestra es un subgrupo de la población o universo que nos interesan sobre el cual se recolectará los datos pertinentes y deberá ser presentativa de dicha población (de manera probabilística), para que podamos generalizar los resultados encontrados en la muestra a la población. (p.126).

Para efectos de esta investigación no se calculará la muestra debido a que se va a utilizar toda la población, siendo un apartado necesario de mención, pero para efectos de este estudio no se estará trabajando con una parte de la población, sino con la totalidad.

Instrumentos de Recolección de Datos

En una investigación es de vital importancia el proceso de recolección de los datos, ya que por medio de estos instrumentos se podrá obtener la información necesaria para responder a preguntas de investigación y los objetivos propuestos. Este procedimiento busca que las herramientas propuestas para la recolección de los datos lo hagan de tal manera que permita que se recaben de manera estructurada y sistemática.

Además de ser un pilar en sí de la investigación, el enfoque que puede adoptar puede variar dependiendo del tipo de investigación seleccionado, dando a entender que no todos los métodos de recolección de datos serán efectivos, sino que corresponde al tipo correcto de investigación seleccionado por el investigador.

Entrevista

La entrevista es un instrumento de recolección de datos en su mayoría de tipo cualitativo, donde se permite un diálogo para que los individuos puedan explicarse con sus propias palabras y así se puedan asimilar los factores que se desean recabar para la investigación; una definición más formal la presenta Hernández Sampieri (2017):

> Las entrevistas se basan en una guía de asuntos o preguntas sobre las variables de interés del planteamiento del problema de la investigación. En ocasiones el entrevistador realiza su tarea siguiendo una guía de preguntas específicas, a la que se sujeta rigurosamente. (p.166).

Dichas entrevistas pueden dividirse en tres tipos: entrevistas estructuradas, las cuales siguen de manera estricta un guion, las preguntas se realizan exactamente de la misma manera a todos los participantes; la semiestructurada, la cual permite más libertad de seguimiento al entrevistador sobre una temática o respuesta a una pregunta anteriormente predefinida y, por último, las no estructuradas, que carecen de linealidad y que son más que todo libres entre el entrevistador y el entrevistado, siendo su enfoque algo más libre y dispuesto al cambio durante su práctica.

Observación

La observación como método de recolección de datos es un instrumento práctico, ya que permitirá evaluar y recolectar información relevante con el estudio por medio de una percepción directa de procedimientos, conductas y el entorno del objeto de estudio por el investigador, la definición la presenta Hernández Sampieri (2017): "Registro sistemático, válido, confiable de fenómenos, procesos, comportamientos, seres vivos o hechos, de acuerdo con un conjunto de normas y procedimientos predeterminados y derivados del planteamiento del problema de investigación" (p.165).

Se cuenta con tres tipos: la participante, donde el investigador involucra al grupo o fenómeno que se está estudiando, la no participante, que sería el contrario al anterior, donde el investigador se limita a observar el grupo o fenómeno y la estructurada, donde el investigador busca específicamente comportamientos o situaciones de su interés para fundamentar su estudio.

Encuesta

La encuesta o cuestionario como método de recolección de datos es un instrumento del ámbito cuantitativo, que sirve principalmente para recolectar datos que se puedan medir por medio de preguntas a los colaboradores de la empresa con el fin de responder a las incógnitas planteadas en el estudio, la definición la brinda Hernández Sampieri (2017):

> Un cuestionario es un conjunto de preguntas respecto a una o más variables que se van a medir. El contenido de las preguntas de un cuestionario es tan diverso como los aspectos que evalúa. Fundamentalmente, se consideran dos tipos de preguntas: cerradas y abiertas. Las preguntas cerradas presentan a los participantes o sujetos o categorías u opciones de respuesta que han sido delimitados previamente para que escojan una o varias dependiendo de la clase de pregunta. En cambio, las preguntas abiertas no delimitan de antemano las opciones de respuesta, por lo cual el numera de categorías es muy elevado y puede variar. (p.155).

Este método es muy sólido a la hora de recolectar datos puntuales, servirá para dar un primer paso en la investigación, pero las preguntas deber tener una claridad y precisión sobresaliente, para que puedan ser comprensibles para quienes las responden, por ende, se debe evitar utilizar

terminología ambigua, amplia o de doble sentido. Con estos detalles este instrumento puede aportar datos de gran precisión y efectivos para el estudio.

Proceso para la Recolección y Análisis de Datos

Este apartado detallar el proceso de recolección de datos del estudio, una de las etapas más relevantes para la investigación, ya que gracias a él se recabarán datos importantes para que el estudio se lleve a cabo y responda a las incógnitas planteadas. El presente estudio se enfoca principalmente en el fortalecimiento de la seguridad de la información en la empresa Electric Cars of Costa Rica.

Esta recopilación con un enfoque mixto permitirá la combinación de técnicas del ámbito cuantitativo y cualitativo para obtener una visión más detallada de la situación actual de la empresa y de esta manera elaborar políticas y procedimientos aplicables a la empresa y fundamentados en los marcos internacionales seleccionados NIST SP 800-53 e ISO/IEC 27001.

Por medio de las herramientas de observación propuestas se estará evaluando principalmente la infraestructura de la empresa en general y el uso diario que se les da a los equipos de la empresa. Esto con el objetivo de identificar las condiciones actuales de seguridad de la información de la empresa en apartados como sus servidores, redes y configuración de controles de seguridad, entre otros.

De igual manera los instrumentos de encuestas y entrevistas estarán enfocados en sacar datos de importancia, cada uno enfocado en un diferente apartado, cuantitativo y cualitativo, siendo las encuestas al personal las que se encargarán del primer aspecto, mientras las entrevistas, del segundo.

De esta manera se logrará tener una perspectiva completa de procedimientos actuales ejecutados por los colaboradores, cultura propia de la empresa respecto a términos como la seguridad de la información y familiarización con los marcos internacionales y las prácticas cotidianas que pueden resultar riesgos cibernéticos, entre otros aspectos.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Encuesta

En este apartado se va a indagar cómo la encuesta puede aportar de manera eficaz datos para la investigación, para determinar qué tanto es el conocimiento sobre políticas y procedimientos de la seguridad de la información dentro de la empresa en general, con el objetivo de conseguir respuestas que aporten de manera positiva a la investigación y al desarrollo de la propuesta.

En la encuesta se indagará en apartados como respaldos de los datos, políticas de seguridad de la información, cultura empresarial, cifrado y comunicaciones. Estas temáticas están enfocadas, como se mencionó anteriormente, en destacar el nivel de entendimiento de los colaboradores de la empresa actualmente frente a estas temáticas, su dominio, percepción o experiencia brindada de manera puntual y precisa para ser recabada para un mejor entendimiento sobre la situación actual de la empresa y sus políticas y procedimientos actuales.

Resultados

En las encuesta realizada los resultados evidencian que la empresa cuenta con bases funcionales en materia de la seguridad de la información, pero no hay ningún aspecto formalizado en la realización de dichos procesos que se podría considerar prácticos, exponiéndolos a riesgos informáticos importantes, los colaboradores exponen un conocimiento moderado sobre aspectos importantes en seguridad de la información no se puede percibir como un pilar solido para la empresa.

Observación

La observación en este apartado proporcionará una perspectiva más presencial de cómo se tratan apartados en los que la empresa opera, esto con el objetivo de tener un segundo punto de vista, más realista, de lo que ocurre en los aspectos de seguridad de la información de la empresa.

En dichas observaciones se buscan objetivos como la detección de activos físicos de la empresa, la presencia de políticas y regulaciones actuales con los apartados de seguridad de la información, una evaluación general de la seguridad de los dispositivos de los colaboradores, procedimientos de respaldos de los datos y su metodología actual y accesos a áreas que se

consideren en la actualidad críticas para la empresa y que se tengan procedimientos o regulaciones efectivas.

Resultados

En las observaciones realizadas se evidencia la presencia de varios métodos no oficiales o fieles a ningún referente internacional en específico, realizando tareas como los respaldos de manera preferente sin seguir un régimen, política o procedimiento que formalice este aspecto; la designación del personal para entrar en áreas que se consideren confidenciales o portadora de información comprometedora no cumple con procesos de selección adecuados, lo cual puede llevar a filtraciones de la información; manipulación indebida de los datos y error humano en general, siendo un brecha de seguridad grande y que justifica las soluciones propuestas de este estudio.

Entrevista

La entrevista va a proporcionar una perspectiva más directa por parte de los colaboradores involucrados en los apartados digitales de la empresa, esto ayudará a compactar los dos enfoques anteriores, por medio de este instrumento se logrará ver el porqué de los comportamientos y procedimientos contemplados en las observaciones y opiniones positivas o negativas reveladas por la encuesta realizada.

Este apartado abarcará tópicos como el cifrado de comunicaciones, las políticas de seguridad de la información y los activos tecnológicos, de esta manera el colaborador de la empresa al que se realice la entrevista proporcionará una perspectiva central de cómo y por qué se realizan los procedimientos actualmente en la empresa.

Resultados

En las entrevistas realizadas se puede evidenciar la falta de una estructura general para la protección de activos físicos y digitales dentro de la empresa, la falta de capacitaciones, conocimiento y sobre carga de responsabilidades en TI debido al poco entendimiento de los otros colaboradores o terceros que participen en las operaciones de la empresa. Esto evidencia la necesidad en la empresa de una propuesta que ayude a organizar todo este apartado, con establecimiento de políticas y procedimientos basados en referentes internacionales que sirvan como base escalable para la protección de sus activos físicos y digitales, así como un personal de otras áreas de la empresa más preparado frente a incidentes informáticos.

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

FACULTAD DE INGENIERÍA INFORMÁTICA

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENIERIA DEL SOFTWARE

Título de la investigación:
Propuesta para la protección de activos físicos y digitales, basándose en las normas ISO/IEC 27001 y NIST SP 800-53 para la empresa Electric Cars of Costa Rica, ubicada en Heredia.

Nombre del estudiante:
Fernando José Artavia García

Sede San José

Septiembre, 2025

CONTENIDO

CAPÍTULO V: PROPUESTA

Electric Cars of Costa Rica es una empresa de origen costarricense que se encarga de la venta, reparación y mantenimiento de automóviles de origen ecológico en nuestro país, dicha empresa está ubicada en San José y cuenta con más de veinte años de experiencia y existencia en el mercado nacional con marcas reconocidas como EZGO y Cushman, pertenecientes al conglomerado industrial de los Estados Unidos Textron.

Su visión como empresa es brindar a los costarricense soluciones de desplazamiento limpias y respetuosas con el medio ambiente, reduciendo las emisiones de CO_2 en la atmósfera, optando por estas soluciones innovadoras y sostenibles en el largo plazo tanto para las personas como para el medio ambiente, sin dejar de lado una atención al cliente admirable y comprometida para cualquier caso que se presente de sus productos ya sean por fines de mantenimientos, venta de partes y venta general de algún vehículo eléctrico.

La seguridad de la información hoy en día se ha vuelto un apartado complemente crítico en la estructura digital de toda empresa que implemente servicios cibernéticos en todos los ámbitos, no basta con tener una funcionalidad básica que permita la operación general de la empresa, se ocupa una inversión general a nivel de seguridad de la información para que tanto datos de la empresa como activos físicos y digitales e información de los clientes no se vean comprometidos en ningún tipo de situación.

La empresa de estudio se enfrenta a grandes desafíos de seguridad de la información y su implementación, la cual se alinee a normativas internacionales seleccionadas como ISO/IEC 27001 y NIST SP-853.

En la siguiente sección se indagará sobre las problemáticas principales y sus deficiencias, adicionalmente se procederá a desarrollar y explicar cada problemática basándose en los datos recolectados de instrumentos como encuestas, entrevistas y observaciones de los procedimientos, políticas, cultura y opiniones de colaboradores sobre las deficiencias detectadas y cómo estas pueden llegar a comprometer la operabilidad de la empresa en caso de no ser corregidas y adaptadas en un contexto de seguridad de la información válido y confiable tanto en el corto como en el largo plazo.

Objetivo General:

Elaborar una propuesta de políticas y procedimientos de seguridad de la información para Electric Cars of Costa Rica, basada en las normas NIST SP 800-53 e ISO/IEC 27001, que permita la mitigación de vulnerabilidades, la protección de activos físicos y digitales y el establecimiento de controles de acceso y respuesta ante incidentes.

Objetivos Específicos

Crear un protocolo de seguridad física para la sala de equipos críticos, sustentado en un análisis de riesgos y que incluya controles de acceso físico conforme lo que dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.11.1.

Elaborar políticas y procedimientos de cifrado de comunicaciones que integren el uso de TLS, claves digitales y buenas prácticas de protección de los datos, conforme a lo que dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.10.1.

Crear un plan de respaldos y recuperación de los datos que incluya lineamientos de verificación e integridad según las normas NIST SP 800-53 e ISO/IEC 27001 A.12.3.

Elaborar documentos de gestión correcta de los activos críticos de la empresa, en los que se describa la segmentación y configuración de *firewall* y la política para el correcto acceso, con base en las normas NIST SP 800-53 e ISO/IEC 27001 A.8.1 y A.12.6.

Crear políticas de seguridad de la información según lo dictan las normas NIST SP 800-53 e ISO/IEC 27001 A.5.1.

Acceso no Controlado a Sala de Equipos Críticos

Una de las brechas de seguridad detectadas es el acceso no controlado a las salas donde se alojan equipos críticos de la empresa, esto puede llegar a comprometer la infraestructura principal de la empresa, donde puede ocurrir filtraciones de la información, identificación de debilidades físicas y difusión de información delicada de la empresa, entre otros. Debido a esto, el primer paso para poder proponer una solución a esta problemática es la realización de un análisis de riesgos.

El presente análisis de riegos se enfocará en la seguridad física de la sala de equipos críticos de la empresa, tomando como referencia las buenas prácticas y aportes que las normas ISO/IEC 27001 y NIST SP-853 pueden proponer para el caso de Electric Cars of Costa Rica, con el objetivo de identificar amenazas, vulnerabilidades y riesgos que se asocien a la mala gestión del acceso del personal a la sala de equipos críticos presente en la empresa.

Este análisis se hace uso de instrumentos como la entrevista, las observaciones estructuradas y entrevistas, para mayor coherencia y entendimiento de este punto específico del caso de la empresa.

Identificación de Activo Crítico

El activo principal de este análisis de riegos corresponde a la sala de equipos críticos, donde se alojan dispositivos esenciales para la operación general de la empresa, entre ellos servidores, equipos de telecomunicaciones y unidades de alimentación. Este activo se considera crítico a nivel empresarial por las siguientes razones:

- Mantiene la operación a nivel digital de la empresa
- Permite la continuidad operativa
- Aloja información sensible y confidencial a nivel empresarial
- Su comprometimiento impacta la operación de la empresa en un ámbito general

Revelación de Amenazas

Partiendo como base de la importancia del activo en cuestión, las amenazas más comunes asociadas a la seguridad física de este activo son más de carácter humano, donde puede verse involucrado el propio error humano, la mala gestión, el sabotaje o la ingeniería social. Siendo el

error humano el principal factor contra la seguridad de la información, se pueden enumerar las siguientes amenazas contra el activo:

- Acceso de personal no autorizado
- Daños a equipo por motivaciones malignas o de sabotaje
- Robo de equipo
- Manipulación indebida y no autorizada de equipo, ya sean servidores o dispositivos de telecomunicaciones
- Acceso de terceros debido a falta de control de la entrada

Estas amenazas representan posibles escenarios fatales que puede tomar forma real por la falta de controles físicos adecuados de este activo dentro de la empresa, exponiendo un grupo de vulnerabilidades internas de la empresa que representa un peligro para la seguridad de la información debido a la ausencia de una autoridad sobre el activo en cuestión.

Identificación de las Vulnerabilidades

La información proporcionada anteriormente ayuda a identificar las vulnerabilidades propias de este activo que se asocian con la seguridad de la información, con base en la información presente se pueden enumerar las siguientes:

- Inexistencia de controles formales
- Falta de autenticación para ingreso
- Bitácora de acceso
- Señalización inadecuada
- Falta de políticas basadas en un método confiable de la industria sobre la gestión de acceso al área
- Ineficiencia en monitoreo de la sala

Siendo en este caso un número considerable de vulnerabilidades, todas parten de la inexistencia de la presencia de un lineamiento internacional o autoridad sobre el activo, donde el control de este es prácticamente informal y poco efectivo para la magnitud del problema que podría provocar en caso de que una de las amenazas anteriormente expuesta se convierta en una realidad.

El impacto que se reflejaría sería de tipo físico y se podría clasificar como de alto nivel, debido a que se interrumpe prácticamente del todo las operaciones de la empresa, se puede corromper la información, adicional a las pérdidas económicas que conllevaría el incidente, tales como costos de reparación, reestructuración de la infraestructura tecnológica general de la empresa, con su correspondiente inversión.

Debido a la inexistencia de controles físicos robustos y a la falta de políticas apoyadas por referentes internacionales como las normas ISO/IEC 27001 y NIST SP-853 entre otros que pueden resultar favorables, la ocurrencia de este tipo de incidentes es de carácter alto, principalmente si se considera el factor de que varios colaboradores o terceros pueden permanecer libremente en dichas instalaciones críticas. Esto expone a la empresa a estar completamente a vulnerable y poco preparada si se da un ataque de este tipo.

Conclusión de Análisis de Riesgo

El análisis expuesto demuestra la clara necesidad de una solución eficiente para la protección de este activo de la empresa, siendo crítico para su operación a nivel general y la reputación y confianza de sus clientes actuales y potenciales. Al tratarse de un riesgo de carácter alto hay necesidad de crear una solución basada en referentes internacionales flexibles y adaptables como las normas ISO/IEC 27001 y NIST SP-853, siendo esto no solo su principal factor a favor, sino que también resultará escalable en el largo plazo, posiblemente resolviendo el problema de seguridad de la información y estructurando una base sólida para el futuro de la empresa en ese aspecto.

Documento de Controles de Acceso Físico para la Sala de Equipos Críticos

La seguridad de la información no solo depende de un controlo logístico contundente, sino también de la correcta protección física en el sentido literal de los activos físicos que la soportan. La sala donde se alojan los equipos críticos representa un punto débil de bastante importancia, ya que sin el debido control de acceso a ella se pueden derivar accidentes de seguridad e interrupciones en los servicios esenciales para la empresa.

En el contexto actual de la empresa Electric Cars of Costa Rica, este documento busca ayudar al establecimiento de controles formales que regulen el acceso físico a la sala donde se

encuentran los equipos críticos de la empresa con el objetivo de reducir riesgos de seguridad potenciales asociados a este caso por una mala gestión de este aspecto. El documento servirá como una guía de utilidad para dicha sala a fin de que su protección esté alineada con buenas prácticas reconocidas por entidades internacionales como lo son las normas ISO/IEC 27001 y NIST SP-853.

Objetivo y Alcance del Documento

El objetivo principal de este documento es el establecimiento de controles de acceso físico a la sala donde se alojan estos equipos críticos para la empresa, reduciendo el acceso únicamente al personal autorizado, para que de esta manera se contribuya a una estructura de seguridad de la información más robusta de sus activos físicos.

El documento y sus controles aplica únicamente para la sala física donde se alojan los equipos críticos de la empresa Electric Cars of Costa Rica, incluyendo todos los dispositivos que abarca dicha sala, ya sean servidores, equipos de telecomunicaciones u otros esenciales para la operación. Los controles están enfocados en el acceso físico a dicha sala y no contempla aspectos relacionados con logística, configuraciones específicas o implementaciones futuras no relacionadas con los marcos implementados en este estudio. Asimismo, este documento se centra en el control de nivel general escalable, y podrá ser ajustado de acuerdo con las necesidades de la empresa en un futuro.

Roles y Responsabilidades

Para la correcta aplicación de roles y sus responsabilidades se definen los siguientes conceptos con el fin de facilitar la compresión de los procedimientos de los controles establecidos al personal de la empresa:

- Controles de acceso: Medida administrativa y técnica destinada para restringir, registrar y supervisar el acceso a un área específica.
- Personal autorizado: Colaboradores y terceros con la capacidad de acceder a la sala de equipos críticos.
- Acceso físico: Capacidad de acceso ya sea autorizado o no de manera presencial a cierta área determinada.

Para la correcta aplicación de estos controles el documento presente clasifica y define los siguientes roles y responsabilidades para así aportar a la seguridad de la información de este activo físico:

- Gerencia: Pone a regir el presente documento mediante su aprobación y proporciona los recursos necesarios para la implementación y mantenimiento de los controles propuestos.
- TI o infraestructura: Encargado de supervisar el cumplimiento de los controles de acceso al personal técnico y velar por la protección del activo de la empresa.
- Terceros: Acceden únicamente bajo una autorización de TI y supervisión del personal técnico responsable, respetando los controles definidos que tengan relación con su presencia en el área.

Marco Normativo de Referencia

Los controles de acceso fisco del presente documento se fundamentan en buenas prácticas funcionales y lineamientos definidos y probados por estándares internacionales reconocidos en la materia de la seguridad de la información, los cuales se encargarán de brindar su referencia y línea de aprendizaje para poder fundamentar la propuesta bajo la sombra de entidades reconocidas en el sector y escalables a largo plazo dependiendo de las necesidades de la empresa. Los aspectos que destacan son los siguientes:

- ISO/IEC 27001: La ISO se centrará en los controles relacionados con la seguridad física del entorno, orientados a prevenir accesos no autorizados, daños a equipo o interferencia de los activos de la información.
- NIST SP-853: Con los controles que establece específicamente esta publicación, se fundamentarán las directrices para limitar el acceso físico a equipos que albergan información que se considere sensible o crítica para la empresa, además de complementar los propuestos por la ISO.

Es de gran importancia la lectura de los controles y la indagación de estas publicaciones en los respectivos puntos mencionados en caso de querer adaptar, mejorar o implementar alguna mejora a este documento de manera satisfactoria y escalable a futuro.

Controles de acceso físico

Control 1: Autorización de acceso

El acceso a la sala donde se alojan los equipos críticos pertenecientes a la empresa estará estrictamente limitado al personal que tenga una autorización de Gerencia o TI, estas autorizaciones deberán documentarse, actualizarse y estar sujetas a revisiones para garantizar el ingreso y control del personal que opera dentro del área.

ISO/IEC 27001 Working in secure areas 7.6: *Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.*

NIST SP-853 Physical and Environmental Protection PE-2: *Desarrollar, aprobar y mantener una lista de individuos con autorización de acceso a donde reside el sistema. Emitir credenciales de autorización para el acceso a las instalaciones. Revisar la lista de acceso que detalla el acceso autorizado a las instalaciones por parte de las personas. Eliminar a las personas de la lista de acceso a las instalaciones cuando el acceso ya no sea necesario.*

Justificación de la metodología: La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.11.1, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente serían todos los anexos pertenecientes a la familia de *Physical controls*, abarcando desde el 7.1 hasta la 7.14 del documento. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Control 2: Ingreso a la sala

Este control responde a la necesidad de crear barreras físicas de acceso a la sala de equipos críticos de la empresa, con el fin de restringir el acceso a personal no autorizado, tales como puertas con un control de acceso, cerraduras físicas y una señalización adecuada. Estos mecanismos deberán estar operativos siempre y recibir un mantenimiento periódico para asegurar su efectividad.

ISO/IEC 27001 Physical entry 7.2: *Las áreas seguras deberán estar protegidas por controles de entrada y puntos de acceso adecuados.*

NIST SP-853 Physical and Environmental Protection PE-3: *El control de acceso físico se aplica a empleados y visitantes. Las personas con autorizaciones permanentes de acceso físico no se consideran visitantes. Los controles de acceso físico para áreas de acceso público pueden incluir registros de acceso físico, guardias o dispositivos y barreras de acceso físico para evitar el movimiento de áreas de acceso público a áreas no públicas.*

- Mantener registros de auditoría de acceso físico.
- Controlar el acceso a las áreas dentro de las instalaciones designadas como de acceso público mediante la implementación de los siguientes controles: [Asignación: controles de acceso físico definidos por la organización].
- Acompañar a los visitantes y controlar su actividad [Asignación: circunstancias definidas por la organización que requieran acompañamiento y control de la actividad de los visitantes].
- Proteger las llaves, combinaciones y otros dispositivos de acceso físico. Asignación de dispositivos de acceso físico definidos por la organización.
- Cambiar las combinaciones y las llaves (Asignación: frecuencia definida por la organización) o cuando se pierdan las llaves, se vulneren las combinaciones o se transfieran o despidan a las personas que poseen las llaves o combinaciones.

Justificación de la metodología: La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.11.1, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente serían todos los anexos pertenecientes a la familia de *Physical controls*, abarcando desde el 7.1 hasta la 7.14 del documento. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Control 3: Monitoreo

Se deberá contar con un mecanismo de supervisión que permita registrar los accesos realizados a la sala de equipos críticos, por medio de bitácoras (físicas o digitales). Dichos registros deberán contar con una revisión periódica por el personal responsable con el fin de detectar accesos inusuales o no autorizados.

ISO/IEC 27001 Physical security monitoring 7.4: *Las instalaciones deberán ser monitoreadas continuamente para detectar accesos físicos no autorizados.*

NIST SP-853 Physical and Environmental Protection PE-6: *La monitorización del acceso físico incluye áreas de acceso público dentro de las instalaciones de la organización. Ejemplos de monitorización del acceso físico incluyen el uso de guardias, equipos de videovigilancia (es decir, cámaras) y sensores. Revisar los registros de acceso físico puede ayudar a identificar actividades sospechosas, eventos anómalos o posibles amenazas.*

- Supervisar el acceso físico a las instalaciones donde se encuentra el sistema para detectar y responder a incidentes de seguridad física.
- Revisar los registros de acceso físico [Asignación: frecuencia definida por la organización] y ante las ocurrencias [Asignación: eventos definidos por la organización o posibles indicios de eventos].
- Coordinar los resultados de las revisiones e investigaciones con el equipo de respuesta a incidentes de la organización.

Justificación de la metodología: La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.11.1, debido a la actualización del documento al formato aprobado dicho documento fue reorganizado y ahora su equivalente serían todos los anexos pertenecientes a la familia de *Physical controls*, abarcando desde el 7.1 hasta la 7.14 del documento. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Control 4: Control de acceso a terceros

El acceso de visitantes o terceros a la sala de equipos críticos debe ser autorizado previamente por el área de TI y además debe estar bajo supervisión incondicional mientras se realiza la labor que requiera la presencia de este tipo de personal dentro de la sala, todo acceso deberá ser registrado, monitoreado e indicar el responsable de dicha autorización.

ISO/IEC 27001 Working in secure areas 7.6: *Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.*

NIST SP-853 Physical and Environmental Protection PE-8: *Los registros de acceso de visitantes incluyen los nombres y organizaciones de las personas que los visitan, sus firmas, formas de identificación, fechas de acceso, horarios de entrada y salida, propósito de las visitas y los nombres y organizaciones de las personas visitadas. La revisión de los registros de acceso determina si las autorizaciones de acceso están vigentes y siguen siendo necesarias para apoyar la misión de la organización y las funciones comerciales. Los registros de acceso no son necesarios para las áreas de acceso público.*

- Mantener los registros de acceso de visitantes a las instalaciones donde se encuentra el sistema durante [Asignación: periodo definido por la organización].
- Revisar los registros de acceso de visitantes [Asignación: frecuencia definida por la organización].
- Informar de cualquier anomalía en los registros de acceso de visitantes a [Asignación: personal definido por la organización].

Justificación de la metodología: La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.11.1, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente serían todos los anexos pertenecientes a la familia de *Physical controls*, abarcando desde el 7.1 hasta la 7.14 del documento. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Control 5: Ubicación del equipo crítico

La sala deberá ubicarse en un área designada, protegida contra accesos, monitoreada y con la señalización correcta, además de que la disposición de su equipamiento deberá minimizar riesgos de operación y facilitar su supervisión por parte del personal.

ISO/IEC 27001 Equipment siting and protection 7.8: *El equipo deberá ubicarse de forma segura y protegida.*

NIST SP-853 Physical and Environmental Protection PE-18: *Los riesgos físicos y ambientales incluyen inundaciones, incendios, tornados, terremotos, huracanes, terrorismo, vandalismo, pulsos electromagnéticos, interferencias eléctricas y otras formas de radiación electromagnética entrante. Las organizaciones consideran la ubicación de los puntos de entrada*

donde personas no autorizadas, aunque no tengan acceso, podrían estar cerca de los sistemas. Esta proximidad puede aumentar el riesgo de acceso no autorizado a las comunicaciones de la organización mediante detectores de paquetes inalámbricos o micrófonos, o de divulgación no autorizada de información.

Justificación de la metodología: La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.11.1, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente serían todos los anexos pertenecientes a la familia de *Physical controls*, abarcando desde el 7.1 hasta la 7.14 del documento. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Control 6: Mantenimiento

El mantenimiento requerido para la sala de equipos críticos deberá realizarse por personal autorizado por gerencia, supervisado por TI y en horarios previamente discutidos y definidos. El acceso preferente de manera temporal deberá ser registrado y monitoreado hasta que las actividades de mantenimiento sean concluidas.

ISO/IEC 27001 Equipment maintenance 7.13: *El equipo deberá mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.*

Justificación de la metodología: La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.11.1, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente serían todos los anexos pertenecientes a la familia de *Physical controls*, abarcando desde el 7.1 hasta la 7.14 del documento. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Elaboración de Políticas y Procedimientos para el Cifrado Correcto de las Comunicaciones.

En la actualidad los sitios web representa uno de los principales métodos de exposición de información confidencial, ya sea de clientes o de la propia organización. Una correcta configuración de los protocolos de comunicación, certificados digitales o controles de seguridad correctamente implementados pueden prevenir las filtraciones de este tipo de información a

atacantes con fines maliciosos, daño a la reputación de la empresa y comprometimiento de activos digitales, como es en este caso específico del sitio web de la empresa.

Para verificar la postura de seguridad del sitio web oficial de la empresa se procede a realizar un análisis de seguridad con el objetivo de identificar posibles brechas de seguridad que puedan exponer datos confidenciales de clientes e información confidencial de la empresa, entre otros aspectos.

Objetivo del Análisis

Evaluación general de seguridad del sitio web oficial de la empresa mediante herramientas especializadas en apartados como la reputación, detección de *malware*, protocolos criptográficos, con el fin de identificar posibles debilidades de seguridad con la finalidad de justificar las medidas propuestas, como lo son procedimientos y guías para este apartado del proyecto orientados a ISO/IEC 27001 y NIST SP 800-53.

Alcance

El análisis se realizó con el dominio oficial de la empresa, la URL: https://electriccarscr.com/, limitándose solo al apartado externo del sitio web y viendo rubros como:

- Reputación
- Indicadores sobre algún *malware* o *phishing*
- Protocolos seguros de comunicación (TLS/SSL)
- Certificaciones digitales

Esto no incluye apartados como las evaluaciones internas de servidores, redes privadas de la empresa ni otros programas que la empresa posea.

Herramientas para la Ejecución de Análisis

Para la realización de una evaluación adecuada de la postura de seguridad se utilizaron las herramientas *open source* en la URL https://electriccarscr.com/:

- VirusTotal
- IBM X-force

- Cisco Talos
- Qualys SSL Labs

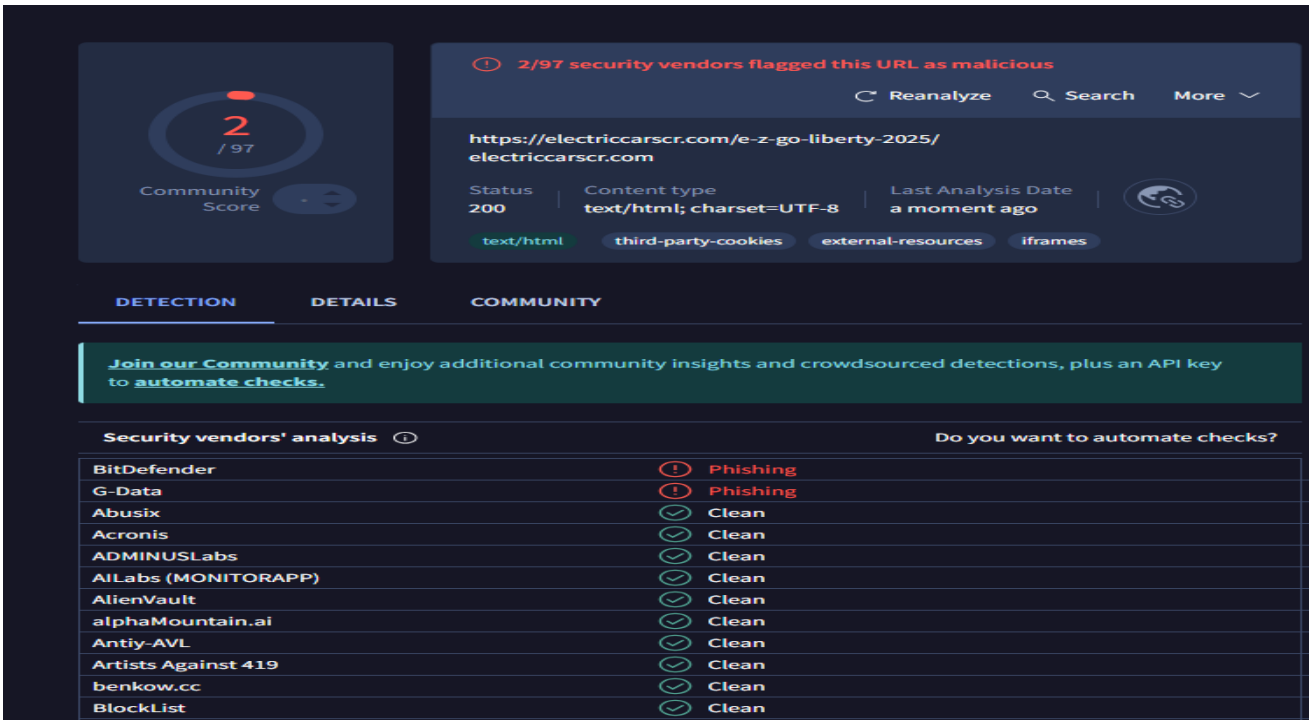
Estas herramientas permiten un enfoque no intrusivo, brindando información como reputación, amenazas cibernéticas y configuraciones criptográficas que puedan servir para detectar fundamentos ausentes en la actualidad del sitio web de la empresa.

Resultados del Análisis

En este apartado se presentan los análisis de cada herramienta más una descripción detallada de la información recopilada.

Figura 1

Análisis de Virtus Total.



Fuente: Virtus Total

Descripción del Análisis Virus Total

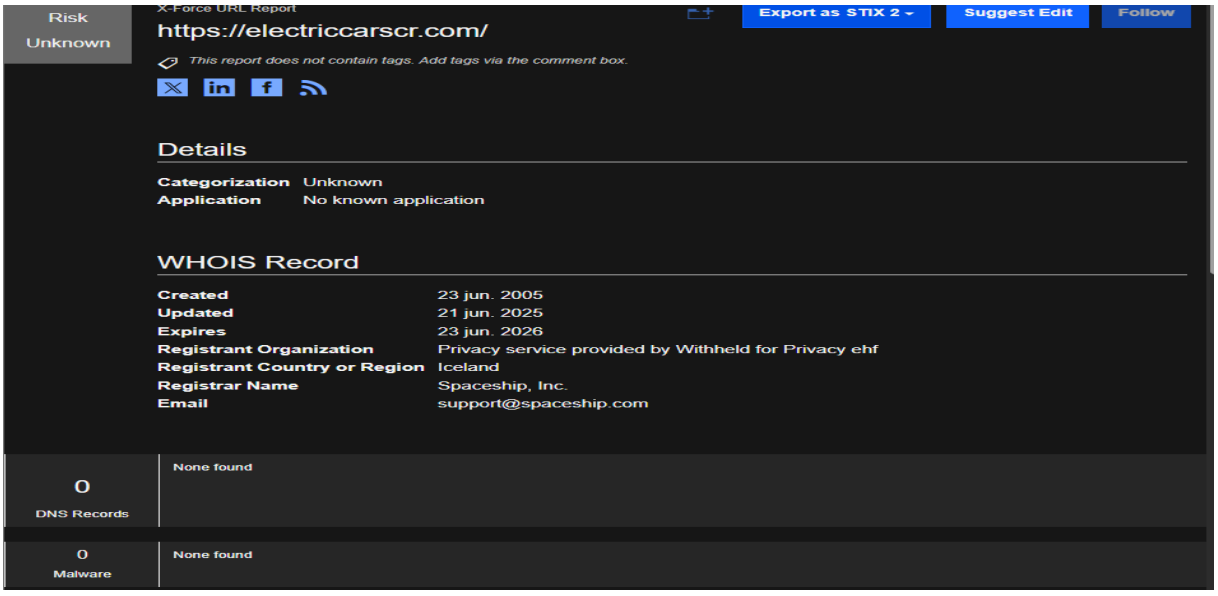
El análisis del dominio que arrojó VirusTotal indica que 2 de 97 motores de seguridad clasifican a la URL como *Phishing*, mientras que la otra gran parte de los proveedores la marcan como segura. Este resultado evidencia que no hay amenazas comprometedoras, señala un riesgo reputacional de bajo nivel, el cual puede deberse a:

- Estructura del contenido web
- Uso de *cookies* de algún tercero
- Promociones web específicas

En conclusión, no se detectan amenazas activas, pero sí una señal de alerta convenientemente temprana para la implementación de procedimientos formales relacionados con este apartado.

Figura 2

Análisis de IBM X-force.



Fuente: IBM X-force

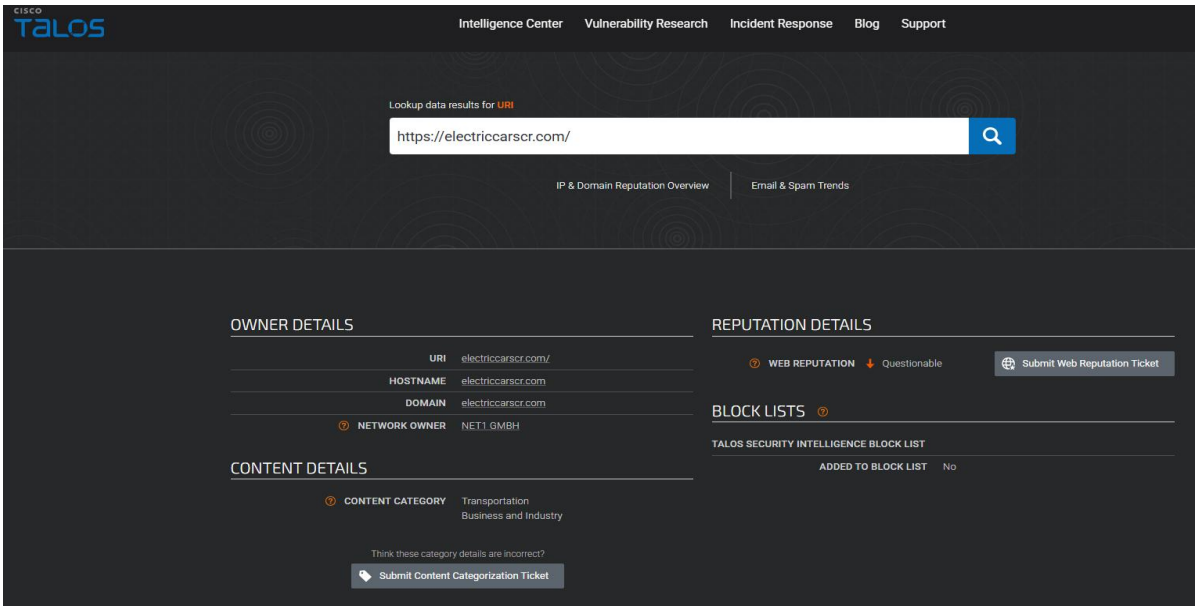
Descripción del análisis de IBM X-force

Según IBM X-force, el dominio no presenta indicadores evidentes de *malware*, además de no presentar reportes de usuarios de un historial malicioso de *malware* en el pasado, pero lo deja clasificado como *Unknown*, lo cual significa que el dominio no es malicioso, pero no cuenta con una clasificación de confianza sólida según esta fuente.

En conclusión, esta fuente refleja que no hay actividad comprometedora en el sitio, pero también revela que no cuenta con una categorización consolidada, evidenciando la necesidad en el refuerzo de la seguridad de la información para una mejor protección de las comunicaciones.

Figura 3

Análisis de Cisco Talos.



Fuente: Cisco Talos

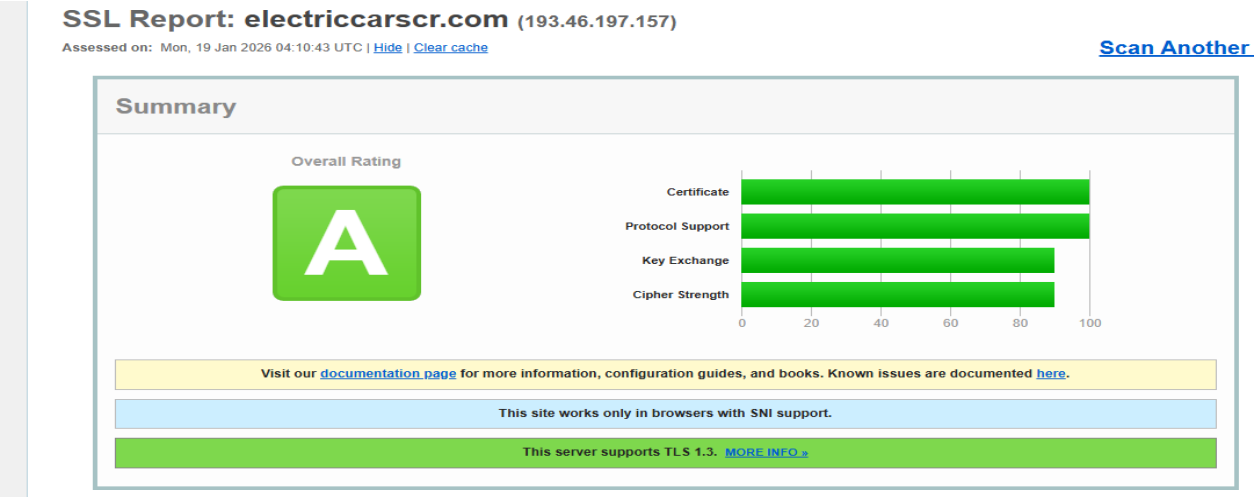
Descripción del Análisis Cisco Talos

Cisco Talos presenta una perspectiva más empresarial, clasificándolo como un servicio de este tipo, pero refleja algo similar a X-force, ya que también lo clasifica como *Questionable*, lo cual significa que el sitio web no presenta actividad maliciosa, pero deja la puerta abierta un nivel de riesgo por la falta de evidencia de seguridad con respecto a la reputación del sitio.

En conclusión, el sitio es representado como cuestionable, no como seguro, que sería lo ideal, esto puede afectar a la reputación propia de la empresa a nivel técnico y generar desconfianza de los clientes hacia la empresa, reforzando la idea de la implementación de los procedimientos propuestos.

Figura 4

Análisis de Qualys SSL Labs.



Fuente: *Qualys SSL Labs*

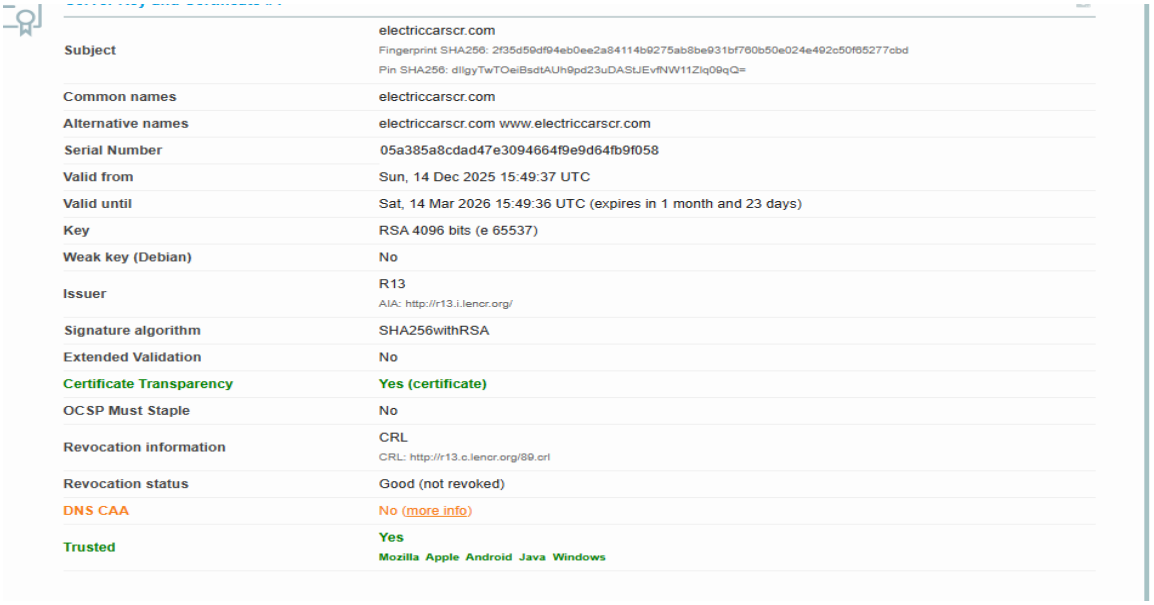
Descripción del Análisis de Qualys SSL Labs

Este análisis refleja varios puntos por tomar en cuenta del aspecto criptográfico del sitio web de empresa:

- Uso de protocolo HTTPS
- Certificados digitales válidos
- Emisión de certificaciones por una entidad confiable
- No hay detección de problemas de revocación

Figura 5

Análisis de Qualys SSL Labs dos.



Subject	electriccarscr.com Fingerprint SHA256: 2f35d59df94eb0ee2a84114b9275ab8be931bf760b50e024e492c50f65277cbd Pin SHA256: dIlgyTwTOeiBsdtAUh9pd23uDAStJEvfNW11Zlq09qQ=
Common names	electriccarscr.com
Alternative names	electriccarscr.com www.electriccarscr.com
Serial Number	05a385a8cdad47e3094664f9e9d64fb9f058
Valid from	Sun, 14 Dec 2025 15:49:37 UTC
Valid until	Sat, 14 Mar 2026 15:49:36 UTC (expires in 1 month and 23 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R13 AIA: http://r13.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL CRL: http://r13.c.lencr.org/89.crl
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Fuente: *Qualys SSL Labs*

Pero también hay aspectos preocupantes que pueden servir como alerta en el futuro, entre los más relevantes se encuentra:

- Ausencia de registros DNS CAA
- Falta de OCSP
- Certificado sin validación extendida
- Fecha de expiración de certificación próxima

En conclusión, el cifrado TLS parece correctamente implementado, pero no existe evidencia de un procedimiento formal para la gestión de certificados digitales, lo que puede llevar a un riesgo operativo dentro de la empresa, así como en la continuidad del servicio.

Conclusión del análisis de postura de seguridad

El análisis de postura de seguridad de la empresa evidencia que no existen alertas de compromiso del sitio, *malware* o ataques en curso o historial de ellos. El principal riesgo evidenciado sería la reputación, configuraciones criptográficas funcionales, pero cuestionables, siendo un punto de mejora evidente, además de una gestión mejorable de los protocolos de cifrado y certificaciones.

Estas condiciones son relativamente positivas, pero también justifican la necesidad de procedimientos y guía formales que regulen este tipo de protocolos de comunicación de la empresa que estén alineados con las normas ISO/IEC 27001 y NIST SP 800-53, con el fin de fortalecer por completo la seguridad de la información del sitio, así como la postura de seguridad de la empresa.

Procedimiento para la adopción de estándares como TLS y AES-256

El uso de protocolos de comunicación inseguros o configuraciones criptográficas inadecuadas incrementan exponencialmente los riesgos cibernéticos. La protección del tránsito de la información es fundamental para una organización que vele por su seguridad de la información, principalmente cuando hay datos sensibles, ya sean de clientes o de la propia empresa.

En respuesta a los resultados obtenidos en el análisis de postura de seguridad del sitio web oficial de la empresa, se establece el presente procedimiento para formalizar la adopción de estándares criptográficos reconocidos internacionalmente como los son *Transport Layer Security* (TLS) y *Advanced Encryption Standard* de 256 bits"(AES-256) para asegurar y reforzar la fuerza informática presente dentro de la empresa de las transferencias de datos ya sea entre usuarios o el sistema de la empresa propiamente.

NIST SP-853 Cryptographic Protection SC-13*: La criptografía puede emplearse para respaldar diversas soluciones de seguridad, incluyendo la protección de información clasificada e información no clasificada controlada, la provisión e implementación de firmas digitales, y la aplicación de la separación de información cuando las personas autorizadas cuentan con las autorizaciones necesarias, pero carecen de las aprobaciones formales de acceso necesarias.*

Dicha adopción formal de estos estándares de cifrado según lo propuesto permitirá la reducción de riesgos de la seguridad de la información posibles durante transferencias de datos. Aunque el sitio de la empresa ya implementa HTTPS, la ausencia de un procedimiento documentado representa una carencia en aspectos como lo son el control y la gobernanza. Este procedimiento ayudará a que el cifrado no dependa de configuraciones informales, sino que responda a marcos normativos alineados con los estándares de ISO/IEC 27001 y NIST SP 800-53, fortaleciendo de esta manera la postura de seguridad de la empresa.

La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.10.1, debido a la actualización del documento al formato

aprobado, dicho documento fue reorganizado y ahora su equivalente sería *Use of Criptography* o A.8.24. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Objetivo del procedimiento

Establecer un procedimiento formal que defina los lineamientos, parámetros y responsabilidades necesarias para a la adopción de los estándares TLS y AES-256, para reforzar la confidencialidad, integridad y seguridad de la información que se transmite hacia y desde los sistemas de la empresa Electric Cars of Costa Rica.

Alcance

Este procedimiento se limita únicamente al sistema de la empresa Electric Cars of Costa Rica y su sitio web oficial. Esto basado en el análisis de postura de seguridad ejecutado durante este estudio, siendo este procedimiento la respuesta a los datos recopilados en dicho análisis.

Además, el procedimiento se enfocará exclusivamente en la adopción de estándares criptográficos ya mencionados y no contemplará configuraciones internas específicas u otros *softwares*.

Procedimiento

1. **Identificación de servicios que requieren cifrado**

   ISO/IEC 27001 Use of cryptography 8.24: *Se definirán e implementarán reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.*

   - El área de TI deberá identificar todos los servicios que realicen transferencias de datos con clientes o terceros que de acuerdo con lo expuesto en este procedimiento se considere necesario cifrar.
   - Se priorizará los servicios que manejen información que se considere delicada en todo su umbral.

2. **Selección de los estándares criptográficos**

   NIST SP-853 Cryptographic key Establishment and Management SC-12*: Las organizaciones definen los requisitos de gestión de claves de acuerdo con las leyes,*

decretos, directivas, reglamentos, políticas, estándares y directrices aplicables, y especifican las opciones, parámetros y niveles adecuados. Las organizaciones gestionan los almacenes de confianza para garantizar que solo los anclajes de confianza aprobados formen parte de dichos almacenes.

- TLS será el protocolo obligatorio por defecto para la protección de comunicaciones de red.
- AES-256 como cifrado simétrico para la protección de dichos datos transmitidos.
- Se evitará el uso de protocolos que se consideren obsoletos, inseguros o no alineados con marcos internacionales.

3. **Configuración de protocolo de comunicación**

NIST SP-853 Cryptographic Module Authentication IA-7: *Es posible que se requieran mecanismos de autenticación dentro de un módulo criptográfico para autenticar a un operador que accede al módulo y verificar que esté autorizado a asumir el rol solicitado y realizar los servicios dentro de ese rol.*

- Asegurarse de que los servicios web operen exclusivamente con conexiones HTTPS.
- Asegurarse de que los certificados digitales sean válidos y que las negociaciones criptográficas utilicen algoritmos fuertes.
- TI deberá verificar periódicamente que estas configuraciones cumplan con los estándares ya definidos, dicha configuración solo podrá ser realizada por personal de TI.

4. **Certificados Digitales**
    - Los certificados deberán emitirse por autoridades confiables.
    - Establecimiento de un control para la vigencia y renovación de dichos certificados.
    - El uso de certificaos vencidos está prohibido debido a los riesgos que amerita.
5. **Pruebas y monitoreo**
    - Realización de pruebas en herramientas como Qualys SSL Labs para realizar evaluaciones periódicas.
    - Verificaciones de que los protocolos TLS y algoritmos criptográficos estén siempre alineados con los marcos internacionales.

- Los resultados deberán ser documentados como evidencia de cumplimiento.
- TI dará seguimiento a posibles nuevas vulnerabilidades relacionadas con protocolos con el fin de adaptarse.
- El procedimiento será revisado a nivel de general de manera periódica para adaptarse a cambios necesarios de acuerdo con las necesidades de este ámbito.
- Todo cambio o ajuste debe ser documentado y justificado.

Guía sobre buenas prácticas para el manejo de certificados digitales, gestión de claves y correcta rotación de estas

La protección de la información mientras está en tránsito depende bastante del correcto uso de certificados digitales y sus claves criptográficas. Aunque tengan protocolos integrados como lo son TLS, el no tener una base práctica formal buena puede llevar a vulnerabilidades que comprometan la seguridad de la información a causa de errores humanos.

La presente guía establece un conjunto de buenas prácticas resumidas orientadas a reforzar ese apartado en el personal de la empresa, lo que ayudar a un mejor manejo, gestión y rotación de las claves y que estén alineados con lo mencionado en los marcos internacionales ISO/IEC 27001 y NIST SP 800-53.

Objetivo de la Guia

Proporcionar información que sea considerara útil y estructurada para orientar al personal de Electric Cars of Costa Rica en el manejo seguro de certificados digitales y la correcta gestión de claves y sus rotaciones.

Alcance

Esta guía aplica a todos los servicios, sistemas y plataformas en los cuales la empresa aplique mecanismos criptográficos, incluyendo su sitio web oficial. Esta guía busca orientar y podrá ser ajustada conforme a la evolución tecnológica de la empresa o las necesidades de esta que lo ameriten a futuro.

Buenas prácticas para el manejo de certificados digitales

ISO/IEC 27001 Use of cryptography 8.24: *Se definirán e implementarán reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas*

NIST SP-853 Cryptographic key establishment and management SC-12*: Las organizaciones gestionan almacenes de confianza para garantizar que solo los anclajes de confianza aprobados formen parte de dichos almacenes. Esto incluye certificados con visibilidad externa a los sistemas de la organización y certificados relacionados con las operaciones internas de los sistemas.*

- Usar certificados digitales emitidos por autoridades conocidas y confiables.
- Verificación periódica de la vigencia de los certificados.
- Proteger las claves asociadas a dichos certificados, evitando exposición de estas, así como asegurarse de su correcto almacenamiento dentro de las instalaciones de la empresa.
- Documentación sobre la ubicación, responsables a cargo de cada certificado, así como un control de uso de estos.
- Revocar cualquier certificado que se considere obsoleto, descontinuado o si se diera el caso comprometido, para no arriesgar la seguridad de la información.

Buenas prácticas para gestión de claves

- La generación de las claves debe ser por medio de mecanismos seguros y conocidos por el sector.
- El acceso a dichas claves debe ser exclusivo para el personal autorizado.
- No compartir las claves sin tener un método ni control sobre su trazabilidad.
- Almacenamiento seguro, evitando cualquier tipo de exposición que pueda comprometer su confidencialidad.
- Los roles y responsabilidades del personal a cargo deben ser definidos para dichas claves.
- Documentación de todo el ciclo de vida de las claves, uso, almacenamiento, personal a cargo, actualización, renovación, entre otros.

Buenas prácticas para una correcta rotación

- Se deben establecer periodos estrictamente definidos de vigencia de las claves.
- Realizar rotación ante sospecha mínima de filtración o uso indebido para evitar comprometimiento de los sistemas asociados.
- Registro actualizado y documentado de cada rotación como evidencia de cumplimiento con nota del personal a cargo de dicha clave y su gestión.
- Dicha rotación debe no interrumpir la operabilidad digital de la empresa.

Creación de protocolo de respaldo de datos

Este apartado corresponde a la creación de un protocolo de respaldo de los datos de la empresa, debido a la inexistencia de un protocolo formal y definido dentro de la empresa, este contemplara la generación de respaldos, la verificación periódica de la integridad de los datos, así como su restauración en caso de algún incidente que amerite dicha acción, conforme a los establecido por las normas ISO/IEC 27001 y NIST SP 800-53.

Esta brecha de seguridad puede comprometer a la empresa en caso de sufrir ataques informáticos relacionados con la integridad y consistencia de los datos, además de la inexistencia de un método de restauración de los datos. Los respaldos en la actualidad se realizan por lapsos semanales no definidos, dependiendo de la necesidad inmediata de realizar uno o de la ocasión que amerite un cambio en el momento. Esta inconsistencia es una brecha que no se puede ignorar según las normas y puede costarle a la empresa este apartado de su seguridad de la información.

La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.12.3, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente sería *Information backup* o A.8.13. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

ISO/IEC 27001 Information backup 8.13: *Se mantendrán copias de seguridad de la información, el software y los sistemas y se probarán periódicamente de acuerdo con la política acordada sobre copias de seguridad específicas para cada tema.*

NIST SP-853 System Backup CP-9: *La información a nivel de sistema incluye información sobre el estado del sistema, el software del sistema operativo, el middleware, el software de aplicación y las licencias. La información a nivel de usuario incluye información que no pertenece al sistema. Los mecanismos empleados para proteger la integridad de las copias de seguridad del sistema incluyen firmas digitales y hashes criptográficos.*

Procedimiento para la generación de respaldos

Este procedimiento tiene como objetivo definir la generación de respaldos de datos de la información, para que esté a disponibilidad de los colaboradores ante incidentes u otras situaciones que lo ameriten. Se trata del establecimiento de copias de seguridad de los datos que se consideren críticos para el correcto operar la de empresa.

Alcance

Este procedimiento solo aplica para el contexto de operación de la empresa, sus colaboradores y equipo con el cual se realizará este procedimiento específico.

Procedimiento

- Identificación de la información que deberá ser respalda, considerando el impacto de estos datos para la organización en sí.
- Definir el medio por el cual será respaldada para su posterior almacenamiento.
- Generación del respaldo una copia de seguridad.
- Almacenamiento del respaldo por el medio definido, asegurándose de su resguardo de manera adecuada.
- Registro de la realización del respaldo, incluyendo información tal como fecha, colaborador, motivo del respaldo, descripción del respaldo entre otra.

Procedimiento de verificación periódica de la integridad de copias de seguridad

El objetivo de este procedimiento es la definición de lapsos coherentes y agendados para la revisión periódica de las copias de seguridad previamente generadas, esto le brindará a la empresa un mayor control sobre la información e historial, con el fin de detectar cambios, intrusiones y

poseer a mano copias actualizadas listas en caso de incidente, según las normas ISO/IEC 27001 y NIST SP 800-53.

NIST SP-853 Software, firmware and Information Integrity SI-7: *Los mecanismos de verificación de integridad, incluidas las comprobaciones de paridad, las comprobaciones de redundancia cíclica, los hashes criptográficos y las herramientas asociadas, pueden supervisar automáticamente la integridad de los sistemas y las aplicaciones alojadas.*

Alcance

Este procedimiento solo aplica para el contexto de operación de la empresa, sus colaboradores y equipo con el cual se realizará este procedimiento específico.

Procedimiento

- Establecimiento de una periodicidad para la verificación de la integridad de las copias de seguridad, dicha fecha debe ser inamovible y siempre cumplida por el personal a cargo.
- Selección de las copias de seguridad según la periodicidad previamente definida.
- Comprobación de los respaldos en su totalidad, accesibilidad, pertinencia de la información almacenada y comprobación de errores evidentes o de otra índole.
- Registrar la consulta de la verificación, incluyendo el periodo definido y el colaborador que realizo la verificación.
- En caso de inconsistencias o modificaciones no autorizadas, notificar al responsable correspondiente y proceder con la generación de un nuevo respaldo y documentar el porqué de este.

Plan de restauración de datos en caso de incidentes

El objetivo de este plan es la correcta restauración de los datos en caso de que la empresa sufra un incidente del ámbito informático que vulnere la seguridad de la información de la empresa según las normas ISO/IEC 27001 y NIST SP 800-53.

NIST SP-853 System Recovery and Reconstitution CP-10*: La recuperación consiste en ejecutar las actividades del plan de contingencia para restablecer la misión de la organización y las funciones del negocio. La reconstitución se lleva a cabo tras la recuperación e incluye*

actividades para que los sistemas vuelvan a su estado plenamente operativo. Las operaciones de recuperación y reconstitución reflejan la misión y las prioridades del negocio; el punto de recuperación, el tiempo de recuperación y los objetivos de reconstitución; y las métricas de la organización, coherentes con los requisitos del plan de contingencia. La reconstitución incluye la desactivación de las capacidades provisionales del sistema que pudieran haberse necesitado durante las operaciones de recuperación.

Alcance

Este procedimiento solo aplica para el contexto de operación de la empresa, sus colaboradores y equipo con el cual se realizará este procedimiento específico.

Procedimiento

- Identificación del incidente que afectó la operación de disponibilidad de la información a la empresa.
- Evaluación del alcance de información perdida o corrupción de los datos.
- Determinar cuál de las copias de seguridad es la más apta para realizar la restauración.
- Autorización del proceso de restauración de los datos por medio del colaborador autorizado.
- Restauración de los datos a partir de la copia de seguridad seleccionada.
- Verificación de que los datos restaurados estén operativos y a disponibilidad de los colaboradores.
- Registro del incidente, las acciones que se realizaron durante el proceso de restauración de datos y los responsables incluidos en él.

Elaboración de documentos de gestión correcta de los activos críticos de la empresa

Este apartado corresponde a la elaboración de documentos de gestión propiamente de activos de la empresa, los cuales son fundamentales para sus operaciones y la seguridad de la información, en el caso de Electric Cars of Costa Rica los activos tanto físicos como digitales soportan procesos esenciales como la comunicación entre sus colaboradores, dentro de la red interna de la empresa; al no contar con ningún tipo de control formal se pueden dar accesos no autorizados a dicha red y provocar exposición, ataques o interrupciones.

La ausencia de una documentación formal para la gestión de este acceso representa una gran brecha de seguridad para la empresa, por esa razón el presente documento propondrá políticas y procedimientos para el correcto acceso a la infraestructura y una configuración de *firewall* óptima, alineándose con referentes internacionales como ISO/IEC 27001 y NIST SP 800-53.

La referenciación original de este documento correspondiente a la ISO fue bajo la numeración correspondiente de A.12.6 y A.8.1, debido a la actualización del documento al formato aprobado, dicho documento fue reorganizado y ahora su equivalente sería A.5.15, A.8.21 y A.8.21. El contenido y propósito se mantienen consistentes, por lo cual su aplicación resulta alineada con el instrumento original.

Objetivo

Establecer políticas y procedimientos formales para que regulen el acceso a la red interna e infraestructura de Electric Cars of Costa Rica con una configuración de *firewall* óptima y segura para la empresa con el objetivo de fortalecer la seguridad de la información y reducir los riesgos mencionados.

Alcance

El presente documento aplica específicamente a la infraestructura de Electric Cars of Costa Rica, incluyendo sus servidores, red interna y externa, además de dispositivos que regulen el tráfico de ambos medios. Este documento contemplará nada más la actualidad de la empresa, no las configuraciones específicas de *software* o desarrollos futuros, aunque está estructurado para ser escalable y servir como base para futuro en la empresa.

Política para Solicitar Acceso a la Red Interna y su Infraestructura

Los accesos no autorizados a la red interna y su respectiva infraestructura representan una amenaza potencial para la empresa, aunque dicho problema es común, también es uno de los que poseen más consecuencias a nivel de seguridad de la información. Entre algunas amenazas específicas a este caso se encuentran: abuso de privilegios, exposición de la información, accesos innecesarios sin registro ni motivo para una correcta supervisión. Esta política establecerá los lineamientos necesarios para regular de manera correcta este procedimiento.

Objetivo

Definir el procedimiento formal para la gestión de acceso a la red interna y su infraestructura, asegurándose que solo el personal autorizado cuente con los debidos privilegios para realizar sus funciones dentro de las operaciones de la empresa.

Política

El acceso a la red interna deberá ser solicitado formalmente y se otorgará conforme la jerarquía de la empresa y las funcionalidades del colaborador, cada acceso a dicha red es personal y exclusivo de dicho colaborador. Se deberá contar con un registro actualizado de los colaboradores u otro personal con acceso autorizado y además el acceso remoto será controlado y justificado en caso de darse.

ISO/IEC 27001 Access Control 5.15: *Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros activos asociados, en función de los requisitos de seguridad de la información y del negocio.*

NIST SP-853 Account Management AC-2: *Los usuarios que requieren privilegios administrativos en las cuentas del sistema están sujetos a un escrutinio adicional por parte del personal de la organización responsable de aprobar dichas cuentas y el acceso privilegiado, incluyendo al propietario del sistema, al propietario de la misión o del negocio, al responsable superior de seguridad de la información de la agencia o a un funcionario superior de la agencia en materia de privacidad. Entre los tipos de cuentas que las organizaciones podrían prohibir debido al mayor riesgo se incluyen las compartidas, las de grupo, las de emergencia, las anónimas, las temporales y las de invitado.*

NIST SP-853 Access Enforcement AC-3: *Las políticas de control de acceso controlan el acceso entre entidades o sujetos activos (es decir, usuarios o procesos que actúan en nombre de los usuarios) y entidades u objetos pasivos (es decir, dispositivos, archivos, registros, dominios) en los sistemas organizacionales.*

Proceder de la Solicitud

- Colaborador o tercero deberá presentar una solicitud formal a la debida autoridad para el acceso.
- La solicitud deberá especificar y justificar el motivo de la solicitud de acceso.
- El tipo de acceso que se requiere para la realización de la tarea por completar.
- La autoridad presente será la responsable de aprobar o rechazar la solicitud.
- En caso de ser aprobado, TI pasará a la configuración de dicho acceso para el colaborador o tercero.

Revisión y Revocación de Accesos

- Todo acceso será revocado una vez que deje de ser necesario y se dejará registro de dicha acción.
- En caso de finalización laboral de algún colaborador con acceso a la red, este deberá ser inmediatamente eliminado.
- Se procederá con revisiones periódicas para verificar los accesos activos y los privilegios respectivos de cada uno con el fin de tener un control y registro en caso de que estos se requieran a futuro.

Procedimiento para la Correcta Configuración del *Firewall*

El *firewall* actuará como línea defensiva para la red interna y el entorno externo, con el fin de evitar alguna infiltración o ataque cibernético. Una configuración adecuada podrá prevenir estos accesos no deseados y monitorear el tráfico de la red y reducir los ataques propiamente a la infraestructura que se considere crítica.

Objetivo

Elaboración de un procedimiento que permita configurar, filtrar y monitorear por medio del *firewall* de la empresa y que a su vez se alinee con los referentes internacionales ISO/IEC 27001 y NIST SP 800-53.

Alcance

Este procedimiento solo aplica para el *firewall* actual de la empresa que protege tanto servidores como el tráfico externo e interno, cualquier modificación a futuro no fue contemplada en este procedimiento y deberá actualizarse en caso de ser el caso.

Configuración

ISO/IEC 27001 Network Security 8.20: *Las redes y los dispositivos de red deberán estar protegidos, gestionados y controlados para proteger la información en los sistemas y las aplicaciones.*

ISO/IEC 27001 Security of Network Services 8.21: *Se identificarán, implementarán y supervisarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.*

NIST SP-853 Boundary Protection SC-7: *Las interfaces administradas incluyen puertas de enlace, enrutadores, cortafuegos, guardias, análisis de código malicioso basado en red, sistemas de virtualización o túneles cifrados implementados dentro de una arquitectura de seguridad. Las subredes separadas física o lógicamente de las redes internas se denominan zonas desmilitarizadas o DMZ. Restringir o prohibir interfaces dentro de los sistemas organizacionales incluye restringir el tráfico web externo a servidores web designados dentro de las interfaces administradas, prohibir el tráfico externo que parezca estar falsificando direcciones internas y prohibir el tráfico interno que parezca estar falsificando direcciones externas.*

Reglas del Cifrado

- El tráfico se limitará únicamente lo necesario para la operación.
- Todo tráfico sospecho o directamente no autorizado será bloqueado.
- Las reglas deberán ser expuestas y justificarse a profundidad.

Segmentación

- La red interna deberá segmentarse para separar servicios que se consideren críticos o confidenciales.

- El acceso entre segmentos debe ser limitado, justificado y controlado para maximizar la seguridad de la información y la efectivada del *firewall*.

Monitoreo del Tráfico

- Se deberán registrar eventos relevantes dentro de la red.
- Monitorear patrones a la primera sospecha de ser maliciosos o anormales a la normalidad de la operación.
- En caso de algún incidente, este deberá ser documentado.

Cambios dentro del *firewall*

- Todo cambio en la configuración del *firewall* deberá ser justificado y aprobado por la autoridad.
- En caso de ser aprobado, el cambio deberá ser documentado.
- No se permiten configuraciones informales de ningún tipo y bajo ninguna justificación.

Mantenimiento y Revisión

- Se deberán realizar revisiones periódicas sobre las reglas y verificar si ocupan cambios o actualizaciones para mayor efectividad.
- En caso de ser necesarios cambios, las reglas obsoletas deberán ser eliminadas y documentar la justificación de su eliminación.
- En caso de la creación de nuevas amenazas, actualizar la configuración para que esté operativa y efectiva frente a las nuevas amenazas inidentificadas.

Este documento está ideado para una mejora continua por medio de actualizaciones periódicas de su procedimiento y asegurar que la empresa tenga una base en la cual apoyarse en este aspecto. Cualquier actualización deberá alinearse con los referentes internacionales y apartados expuestos y la infraestructura propia de la empresa para mantener su efectividad frente a nuevas amenazas a futuro.

Políticas para la Seguridad de la Información

La seguridad de la información de los activos críticos no tiene políticas claras donde estas regulen cómo debe manejarse la información de los clientes, esto genera principalmente un mal manejo de la información ya sea en caso de un incidente o de delegar responsables claros a la hora de manipular información que se considere confidencial. La ausencia formal de dichas políticas y procedimientos incrementa el riesgo de uso indebido de dichas informaciones, exponiéndose a filtraciones o respuestas ineficientes frente a incidentes.

En el caso de Electric Cars of Costa Rica, se ha identificado una falta específica en el cómo se debe manejar la información de los clientes y sus activos correspondientes, debido a esta situación el presente apartado propondrá las políticas necesarias para que la empresa pueda manejar estos apartados de manera correcta y alineada a referentes internacionales como las normativas ISO/IEC 27001 y NIST SP 800-53.

Objetivo

Establecer políticas formales de seguridad de la información que permitan proteger la información de los clientes y los activos de la empresa que participen, manteniendo confidencialidad, integridad y disponibilidad propia de la información y alineándose con las normas NIST e ISO.

Alcance

El presente apartado se rige bajo el contexto de la empresa Electric Cars of Costa Rica y los activos, ya sean físicos o digitales, que participan en la manipulación, protección y tráfico de la información de sus clientes, donde las políticas propuestas sirvan como un marco general escalable que pueda ser complementado y actualizado según las necesidades de la empresa.

Políticas y Procedimientos para la Seguridad de la Información de los Activos Críticos

Se presentará las políticas y procedimientos para la protección de la información de los clientes y los activos correspondientes, en los cuales se detallará cómo debe ser gestionado de manera correcta, sirviendo como una base general para su protección.

ISO/IEC 27001 Policies for information security 5.1: *La política de seguridad de la información y las políticas específicas de cada tema deberán ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas pertinentes, y revisadas a intervalos planificados y si se producen cambios significativos.*

NIST SP-853 Boundary Protection PL-1: *Las políticas y los procedimientos contribuyen a garantizar la seguridad y la privacidad. Por lo tanto, es importante que los programas de seguridad y privacidad colaboren en su desarrollo. La política puede incluirse como parte de la política general de seguridad y privacidad o estar representada por múltiples políticas que reflejen la naturaleza compleja de las organizaciones.*

Objetivo

Crear las políticas necesarias para la correcta gestión de la información de los clientes y los activos participantes de Electric Cars of Costa Rica.

Alcance

Estas políticas aplicarán a toda la información relacionada con los colaboradores, terceros y sistemas que participen en la manipulación de la información que la empresa posea sobre los clientes y los activos, ya sean físicos o digitales, que sirvan como herramienta para su correcta gestión.

Política para la Protección de la Información según su Clasificación

La información debe ser protegida dependiendo del nivel de su clasificación y su acceso se concede bajo el privilegio asignado y correspondiente, donde cualquier actividad deberá poder ser documentada y tener un responsable de cada acción. TI deberá encargarse del cumplimiento de dicha política una vez que Gerencia la haya aprobado y los colaboradores la hayan estudiado para su correcta aplicación.

Responsabilidades para la correcta aplicación

- Aprobación por parte de Gerencia.

- Supervisión completa de TI sobre el cumplimiento y aplicación correcta de la política.
- Asesorar al colaborador de la empresa y asegurarse la buena práctica de la política en el ambiente empresarial.

Incumplimiento

El incumplimiento o irrespeto a esta política deberá derivar medidas de carácter administrativo conforme a lo que dicta la normativa interna de la empresa relacionada con los casos de incumplimientos.

Política para el Control de Acceso de Información

Esta política establece los lineamientos para que la información de los clientes y sus activos críticos sean solo otorgados al personal correspondiente, dependiendo de su rol dentro de la estructura empresarial, responsabilidades y funciones. El acceso a dicha información será bajo el principio del privilegio mínimo, para que cada usuario tenga únicamente los requisitos necesarios para realizar su labor de manera correcta. Todo acceso debe ser autorizado, documentado y sometido a revisión.

Objetivo

Mantener un control de acceso óptimo y justificado para una correcta operabilidad dentro del entorno empresarial, reforzando la seguridad de la información por medio del control de la información de la empresa.

Alcance

El alcance de este procedimiento se limitará exclusivamente a lo expuesto en la política de este apartado, los apartados de los referentes expuestos y los roles que participan en esta.

Responsabilidades para la Aplicación Correcta

- Gerencia: Aprobación del funcionamiento de la política.
- TI: Administración y revisión del funcionamiento general de la política.
- Colaborador: Usar los accesos concedidos de acuerdo con su rol de manera responsable y únicamente con fines empresariales.

Incumplimiento

El incumplimiento o irrespeto a esta política deberá derivar medidas de carácter administrativo conforme a lo que dicta la normativa interna de la empresa relacionada con los casos de incumplimientos.

Política de Manejo de la Información y su Clasificación

Esta política busca la definición concreta para la clasificación y manejo de la información según el nivel de confidencialidad que posea, esto con el objetivo de proteger mejor los datos de los clientes y activos de la empresa. Toda la información deberá poseer una clasificación según el nivel de sensibilidad que se detecte y manejarse de acuerdo con ese aspecto. La información de carácter confidencial ameritará un trato diferente a la demás clasificación debido a lo crítico de esta para la operabilidad de la empresa.

Objetivo

Tener una clasificación eficiente y efectiva para evitar filtraciones de la información, además de manejar de manera correcta y distinta los diferentes tipos de información según su clasificación.

Alcance

El alcance de este procedimiento se limitará exclusivamente a lo expuesto en la política de este apartado, los apartados de los referentes expuestos y los roles que participan en esta.

Responsabilidades

- Toda información deberá ser asignada a una categoría.
- TI deberá encargarse de su correcta administración.
- Los colaboradores deben ser notificados y tener conciencia de la clasificación de la información que manejan para evitar filtraciones por error humano.

Incumplimiento

El incumplimiento o irrespeto a esta política deberá derivar medidas de carácter administrativo conforme a lo que dicta la normativa interna de la empresa relacionada con los casos de incumplimientos.

Procedimiento para la Aplicación de la Política de Seguridad

Este procedimiento precede a la política de seguridad anteriormente expuesta y su correcta asignación para los colaboradores de la empresa, en donde se verá el flujo y comportamiento esperado sobre el accionar y puesta en acción de esta.

Objetivo

La correcta práctica de la política para la protección de los activos relacionados con la información de los clientes de la empresa.

Alcance

El alcance de este procedimiento se limitará exclusivamente a lo expuesto en la política de este apartado, los apartados de los referentes expuestos y los roles que participan en esta.

Procedimiento

- Comunicado oficial de la política a todo el personal de interés y participación en este apartado de la operabilidad de la empresa.
- Aplicación de los controles y apartados expuestos de los referentes.
- Puesta en práctica de la política, más una capacitación de los colaboradores.
- Supervisión del cumplimiento del procedimiento tal como se dicta.
- Reportes y revisión sobre la efectividad y práctica de la política y su misión.
- En caso de necesitarse, solicitar una actualización y documentar el motivo de esta para adaptarse a nuevas amenazas que pueda comprometer la seguridad de la información de los activos participantes.

Procedimiento para la Gestión de Acceso a la Información

Este procedimiento precede a la política de control de acceso a la información y el cómo debe ser puesta en práctica mediante este procedimiento, el cual dictará el proceder de dicha política puesta en acción.

Objetivo

Definición del procedimiento de solicitud, aprobación o modificación a la información dentro de los activos físicos o digitales de la empresa.

Alcance

Este procedimiento aplica a todos los accesos otorgados a colaboradores de la empresa o terceros que hayan sido autorizados, deberán alinearse con lo dictado a la clasificación de la información, rol y tarea que se disponga en Electric Cars of Costa Rica.

Procedimiento

- Solicitud formal para el acceso a la información por parte del colaborador.
- Evaluación de TI y decisión final.
- Asignación de accesos según la tarea por realizar.
- Registro y documentación del acceso otorgado al colaborador.
- En caso de desvinculación con el colaborador o un cambio de rol de este se deberá aplicar una revocación inmediata del acceso a dicha información.

Procedimiento para la Clasificación y Manejo de la Información

Este procedimiento precede a la política de clasificación y manejo de la información, y el cómo debe ser puesta en práctica mediante este procedimiento, el cual dictará el proceder de dicha política puesta en acción.

Objetivo

El objetivo de este procedimiento es la clasificación correcta de la información de la empresa y su manejo adecuado en todo su ciclo de vida útil.

Alcance

Aplica para la información de carácter físico o digital de la empresa que tenga relación con los clientes y operaciones de esta que se consideren dentro del espectro que maneja la clasificación de la información de la entidad.

Procedimiento

- Identificación del tipo de información.
- Asignación a una clasificación según lo discutido en la fase de identificación.
- Aplicar los controles necesarios según lo que demanda la clasificación de dicha información.
- Notificar al personal sobre la actualización y manejo que se le debe dar a la información.
- Revisiones periódicas por parte de TI a la clasificación de la información.

Manual de Clasificación de Datos

Este manual estará enfocado en la clasificación de la información y asignación de un riesgo potencial, con esto se delimitará y mantendrá un orden de prioridad sobre dicha información y el nivel de seguridad asignado y el porqué de cada uno. La ausencia de un manual de esta índole puede provocar el mal manejo de información sensible e incrementar el riesgo de exposición ya sea por un error humano o puramente cibernético.

Objetivo

Definir una clasificación que permita identificar el nivel de confidencialidad necesaria para los datos que maneja la empresa y poder reaccionar de manera adecuada, ya sea en protección de estos o frente a un incidente que aporte a su protección.

Alcance

El alcance de este manual solo se limita a la información manejada por Electric cars of Costa Rica y los colaboradores que participen en la manipulación de los datos correspondientes bajo la guía de este manual.

Clasificación de la Información

- Información de carácter Público: Información destinada al público y cuya propagación no represente un riesgo operativo de ningún tipo para la seguridad de la información.
- Información de carácter Interno: Información que se considere de uso exclusivo a menos que reciba autorización previa de su divulgación y motivo del porqué entre los colaboradores de la empresa.
- Información de carácter Confidencial: Información sensible de colaboradores, clientes o procesos internos cuya divulgación esté sujeta a apartados de carácter legal o financiero, entre otros.
- Información de carácter Crítico: Información que se considere incondicional para la correcta operación de la empresa, que pueda significar la alteración, el estancamiento o la continuidad del negocio en su totalidad en caso de ser comprometida.

Manejo y Uso Correcto de la Clasificación

Cada tipo de información deberá tener un control respectivo acorde a su jerarquía, el acceso propio a esta clasificación se limitará únicamente a colaboradores de la empresa o personal tercero autorizado para evitar filtraciones.

- La información de carácter confidencial deberá ser cifrada y protegida siguiendo los más altos estándares.
- El almacenamiento de la información declarada en la clasificación deberá cumplir con los estándares expuestos en los referentes y políticas relacionadas al correcto almacenamiento de la información.

Protocolo de Respuesta a Incidentes y Directrices para el Uso de Dispositivos Personales

La capacidad para poder responder de manera efectiva ante un incidente informático es indispensable ya sea para minimizar impactos o directamente prevenir un ataque cibernético. Asimismo, el uso de dispositivos de carácter personal puede representar un riesgo de la seguridad de la información si no se aplican directrices acordes a estos.

Objetivo

Definir un protocolo de respuesta a incidentes de la seguridad de la información y a su vez proponer directrices frente al uso de dispositivos personales dentro de las instalaciones de la empresa.

Alcance

Este apartado está limitado a la capacidad de responder ante incidentes de la empresa Electric Cars of Costa Rica y sus colaboradores, así como las directrices de los dispositivos personales tanto de los propios colaboradores como de terceros dentro de las instalaciones de la empresa.

Protocolo

ISO/IEC 27001 Information Security Incident Management Planning and Preparation 5.24: *La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.*

NIST SP-853 Policy and Procedures IR-1: *Las políticas y procedimientos de respuesta a incidentes abordan los controles de la familia IR que se implementan en los sistemas y las organizaciones. La estrategia de gestión de riesgos es un factor importante para establecer dichas políticas y procedimientos. Estas políticas y procedimientos contribuyen a garantizar la seguridad y la privacidad.*

- Identificación del incidente y su naturaleza.
- Comunicarse inmediatamente con TI.
- Medidas de contención del incidente para evitar escalado de privilegios o comprometer la información.
- Análisis del impacto y la causa raíz del ataque.
- Recuperación y reportes de sistemas afectados por el incidente.
- Documentación del proceder y accionar del equipo durante y después del incidente.

Directrices de Uso de Dispositivos Personales

- El uso de cualquier dispositivo personal deberá ser notificado y autorizado por la autoridad presente dentro de la instalación empresarial.
- Los dispositivos deberán cumplir con los controles mínimos de seguridad de empresa para ser utilizados dentro de las instalaciones.
- Está prohibido la grabación, almacenamiento o distribución de información ya sea de carácter sensible o confidencial en dispositivos personales no autorizados por la autoridad presente en la instalación.
- TI podrá tomar medidas de seguridad en caso de incumplimiento, incluyendo el revocamiento del acceso a dicha instalación en caso de que se considere necesario por temas de seguridad de la información.

Lo expuesto en este documento deberá revisarse de manera periódica para que se pueda asegurar de su vigencia y efectividad, en caso de ser actualizado deberá alinearse a los referentes internacionales elegidos y justificar y documentar los cambios.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Lo expuesto en esta investigación sobre la empresa Electric Cars of Costa Rica evidencia las carencias en los apartados de seguridad de la información, principalmente por la ausencia de controles formales dentro de la empresa, procedimientos con su correcta documentación y políticas eficientes que estén alineadas con marcos internaciones de seguridad de la información como lo son ISO y NIST, siendo estas sus principales debilidades frente a riesgos de exposición de la información sensible de clientes y de activos críticos de la organización de carácter digital y físico.

Tras la realización de un análisis de riesgos para verificar la vulnerabilidad física se evidenciaron carencias en la sala de equipos críticos que exponen la seguridad física de estos activos, además de no poseer controles que se alineen con ningún referente internacional confiable, siendo esto un problema a nivel de acceso a dicha sala, control y seguridad física general de la empresa.

Uno de los aspectos importantes dentro de la estructura empresarial fue la ausencia de procedimientos y políticas para el acceso a la infraestructura de la empresa. Esta falta de lineamientos formales para el proceso de solicitud, autorización y control propio del acceso, tanto a colaboradores como a terceros, expone a la organización a brechas de seguridad por accesos no autorizados, falta de documentación de acciones sobre los activos e información y posible afectación a la continuidad operativa de la empresa.

Los mecanismos de cifrado usados por la empresa a nivel práctico resultaron ser más contundentes de lo esperado, pero carecen de un respaldo documentado que formalice estos métodos de manera total en un esquema empresarial. Si bien el sitio web de la empresa utiliza protocolos que se consideran seguros, como TLS y HTTPS, la inexistencia de un apartado documentado que defina estos procedimientos representa una debilidad de carácter normativo y de control dentro de la empresa, según los referentes seleccionados ISO/IEC 27001 y NIST SP 800-53.

Se realizan respaldos de manera aleatoria y sin una fecha que defina de manera correcta este proceder, lo cual expone a la empresa a debilidades de pérdida de información y control sobre ello, como poseer copias de seguridad actualizadas y libres de cualquier método de corrupción ocasionado por un ataque cibernético. La realización de respaldos ocasionales no resulta suficiente

y expone a la empresa a estos problemas, lo cual demanda un protocolo formal de respaldo de la información para que de esta manera la disponibilidad, integridad y continuidad de la información está protegida ante incidentes de seguridad o fallos de equipo.

Las políticas integrales de seguridad de la información dentro de la empresa no regulan áreas como el manejo, clasificación y protección específica de activos físicos y digitales, además de la información de los clientes, crucial para la imagen y confianza de la empresa a nivel operativo. Esta problemática evidencia que, al no haber políticas y procedimientos que regulen esto, puede desembocar en uso indebido de la información, dificultad en la asignación de las responsabilidades debido a la inexistencia de una clasificación de los datos y de quiénes acceden y manipulan dicha información, limitando la capacidad de respuesta ante incidentes y alejando a la organización de las buenas prácticas que establecen los estándares internacionales.

Todo esto en conjunto evidencia la necesidad de fortalecer la postura de seguridad de la información de la Empresa Electric Cars of Costa Rica mediante controles documentados, políticas y procedimientos alineados con ISO/IEC 27001 y NIST SP 800-53, para que sirva de base para la gestión estructurada y formal de la seguridad de la información dentro de la empresa.

Recomendaciones

Implementación formal de los controles propuestos para el uso de estándares criptográficos como TLS y AES, asegurándose de esta manera su incorporación y aplicación en la rutina empresarial, pasando a un estándar formal y obligatorio y no requerido por alguna disconformidad técnica o solución de último momento. Además, que la gerencia pueda aprobar dichos lineamientos y supervisión exclusiva por TI, facilitando así la gobernanza del cifrado, las auditorías y las evaluaciones a futuro.

Capacitación al personal sobre las políticas propuestas en esta investigación para agilizar su ejecución, tener un personal capacitado en el ámbito de la ciberseguridad y sus conceptos es de vital importancia a la hora de aplicar todo lo expuesto en esta investigación. Un personal preparado y organizado con estas nuevas tendencias tecnológicas será la mejor defensa ante un incidente cibernético y su posterior resolución.

Revisiones periódicas de carácter obligatorio de estas políticas, procedimientos y controles para mantenerse actualizado y defendido ante posibles innovaciones en ataques u otros métodos

para la pérdida, control y manipulación indebida de activos físicos, digitales e información sensible de clientes. Esto ayudará a estar al día con requerimientos normativos dentro de la empresa y sus referentes seleccionados y a mantener su postura de seguridad orientada a la mejora continua de sus operaciones.

Escalabilidad de las políticas, procedimientos y controles propuestos con el fin de mantenerse protegidos ante nuevas amenazas que afecten a las operaciones de Electric Cars of Costa Rica, estas servirán como base para una mejor operación o incluso definición en algunos apartados propuestos en esta investigación; además, están diseñados de tal manera que puedan ser modificados y mejorados para una mejor operación, dependiendo de las nuevas amenazas cibernéticas que surjan con el tiempo.

La implementación del protocolo de respaldos de los datos, dado que esta fue una de las mayores brechas de seguridad. Esta información frente a un incidente es vital para lograr la operabilidad de la empresa, tener esta información actualizada y cubierta es de vital importancia, además de una documentación adecuada para que llevar un control total de este apartado.

REFERENCIAS

Electric Cars of Costa Rica. (2025). *Sobre nosotros*. Electric Cars Costa Rica. https://electriccarscr.com/sobre-nosotros/

Flinders, M. (2023). *What is asset reliability?* IBM. https://www.ibm.com/think/topics/asset-reliability

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E54), 87-100.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2014). *Metodología de la Investigación* (M. H. España, Ed.). https://dialnet.unirioja.es/servlet/libro?codigo=775008

Hernández Sampieri, R., Méndez Valencia, S. y Cuevas Romo, A. (2017). *Fundamentos de la investigación.* McGraw Hill.

IBM. (2025a). *¿Qué es la copia de seguridad y restauración?* IBM Think. http://ibm.com/mx-es/think/topics/backup-and-restore

IBM. (2025b). *¿Qué es la recuperación de datos?* IBM Think. https://www.ibm.com/es-es/think/topics/data-recovery

IBM. (2025c). *Política y objetivos de seguridad*. IBM Documentation. https://www.ibm.com/docs/es/i/7.6.0?topic=strategy-security-policy-objectives

IBM. (2025d). *Seguridad*. IBM Sterling B2B Integration SaaS. https://www.ibm.com/docs/es/b2bis?topic=security-physical

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC27001:2022)*. https://www.iso.org/standard/82875.html

Maranto Rivera, M. y González Fernández, M. (2015). *Fuentes de Información*. https://dspace.uaeh.edu.mx/server/api/core/bitstreams/624c644f-fe81-42be-9a5d-2ccde73a78e6/content

Matthew Kosinki, B. C. (2025). *¿Qué es el cifrado?* IBM Think. https://www-ibm-com.translate.goog/think/topics/encryption?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wa

National Institute for Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations.* U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Sepúlveda, S., & Cravero, A. (2021). Diseño de una política de seguridad de la información: una propuesta. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E46).

Villalón Fonseca, R. (2022). *The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity.* (2022). Science Direct. https://www.sciencedirect.com/science/article/pii/S0167404822001997#sec0001

APÉNDICES

APÉNDICE A. GUÍA DE OBSERVACIÓN

Nombre de la Empresa: Electric Cars of Costa Rica

Actividad de la Empresa: Procedimientos y lineamientos actuales de la empresa relacionados con sus activos críticos físicos y digitales.

Objetivo: Observar y evaluar las actividades relacionadas con el proyecto de Propuesta para la Protección de Activos Físicos y Digitales, basándose en las normas ISO/IEC 27001 y NIST SP 800-53 para la empresa Electric Cars of Costa Rica, ubicada en Heredia.

n.º	Aspectos por Observar	Cumple	No Cumple	Oportunidad de Mejora	Detalle de Observación
1	Control de acceso a personal y su procedimiento para la entrada a sala, si existe equipo de vigilancia y registro de ingreso y salida del personal.	X		Formalizar y llevar un control más riguroso en el ingreso y salida.	No hay presencia de ningún modelo para llevar a cabo el acceso. El acceso se da sin aprobación de una autoridad, sino que es más informal y de acuerdo con el contexto de la situación. La vigilancia no es del todo rigurosa para cumplir con lo dicho en los referentes.
2	Metodología actual de respaldo de datos y restauración, tiempo en que se realiza cada respaldo. Con el objetivo de determinar si cumple con estándares competentes.		X	Formalización de los procedimientos para el respaldo de los datos. Adaptación a estándares internacionales	Los respaldos no se realizan en periodos del todo designados y dependen de la necesidad del tiempo. No hay ningún modelo o referente presente en el que se basen para realizar los respaldos. No hay personal formalmente designado para este tipo de tareas.
3	Comparar si existen procedimientos o políticas dentro del entorno laboral y en caso de que existan, si cumplen con los lineamentos ISO/IEC 27001:2022		X	Creación de los procedimientos Cumplimiento con ISO/IEC 27001:2022.	No existen políticas formales a pesar de que el personal tenga una idea sólida sobre ellas. No existe ninguna correlación con la ISO en este apartado, siendo políticas presentes, pero no escalables como el modelo propuesto.

n.º	Aspectos por Observar	Cumple	No Cumple	Oportunidad de Mejora	Detalle de Observación
4	Evaluación de seguridad de los dispositivos utilizados por colaboradores y determinar si siguen directrices alineadas con ISO/IEC 27001:2022 y poseen controles similares de acuerdo con NIST SP 800-53.	X		Alineamiento con ISO/IEC 27001:2022 y NIST SP 800-53. Los dispositivos utilizados exclusivamente para temas de trabajo.	Existen dispositivos para la seguridad utilizados por los colaboradores, pero estos no se alinean con mencionado en la ISO o NIST, siendo poco eficaces en situaciones realistas en caso de incidentes.
5	Detección de activos físicos y digitales que se consideren críticos y sus procesos de seguridad actuales.	X		Mejora en los procesos de seguridad actuales.	Los activos físicos y digitales son reconocibles e identificables por su importancia por el personal, pero los medios y procesos actuales no son escalables ni basados en ningún marco formal para garantizar su efectividad.

Fuente: Elaboración propia.

APÉNDICE B. GUÍA DE ENTREVISTA

Organización: Electric Cars of Costa Rica

Nombre del Entrevistado: Rafael Núñez/ José Delgado

Cargo: Gerente de Operaciones/ Encargado de TI

Preguntas sobre Cifrado de Comunicaciones

Pregunta 1: ¿Qué protocolos de comunicación utiliza actualmente la empresa para transmitir información sensible o que consideran importante?

Esta pregunta busca que el colaborador entrevistado de una explicación extensa de cuáles son los protocolos de información actuales y su ejecución, si ha causado problemas de seguridad de la información y si hay alineaciones con la ISO o el NIST.

Respuesta del gerente Rafael Núñez: Cifrados de extremo a extremo, conexión de red IP privatizada dentro de las instalaciones de la empresa y correos electrónicos propios de esta.

Respuesta de José Delgado, encargado de TI: Cifrado de extremo a extremo con la presencia de una red privada para añadir una capa de seguridad adicional, los demás colaboradores disponen de un correo empresarial por el cual se comunican aspectos puntuales y no factores que puedan comprometer la seguridad de la información.

Interpretación: Los sujetos entrevistados mencionan la presencia de un protocolo base de seguridad de la información, no se mencionan detalles de algún referente o modelo de seguridad específico para llevar esto a cabo.

Pregunta 2: ¿Existen procedimientos internos para cifrar la información que viaja por los sistemas de la empresa o carecen de ellos?

Esta pregunta busca abarcar el total de lo mencionado en el cuestionario y saber por qué se utilizan estos medios de cifrado o siquiera si existen dentro del entorno empresarial, con el objetivo de clasificar este apartado como una gran brecha de seguridad en caso de no contar con ellos.

Respuesta del gerente Rafael Núñez: No, solamente se almacenan en servidor y se respaldan de manera manual en un disco duro.

Respuesta de José Delgado, encargado de TI: No cuentan con procedimientos formales si es a lo que se refiere, se busca más que todo una adaptabilidad puntual, tal como configuraciones de cifrado que cumplan con lo necesario para la ocasión.

Interpretación: Se confirma la ausencia de un apartado dedicado a un protocolo formal, además de no contar con una guía específica, además de depender de sus colaboradores de TI para su corrección o adaptación, dependiendo de lo que se ocupe en el momento, siendo poco escalable y peligroso para la seguridad de la información de la empresa.

Pregunta 3: ¿Tienen algún tipo de monitoreo para las conexiones seguras de la empresa?

Esta pregunta busca comparar los protocolos de monitoreo actuales de la empresa, principalmente en los dispositivos de los colaboradores y si sus conexiones y configuración son seguras para manejar los datos de clientes o información confidencial de la empresa que pueda comprometer sus operaciones.

Respuesta del gerente Rafael Núñez: No, esto no está incluido en ningún aspecto de la red externa de la empresa. Los equipos de los colaboradores y sus movimientos son administrados por TI, siendo una tarea propia de estos.

Respuesta de José Delgado, encargado de TI: No hay un protocolo formal de monitoreo dentro de la red de la empresa, al ser relativamente pequeña casi que cualquier supervisión o manejo de información sensible es algo que se ve de manera presencial en caso de que algún colaborador acuda a nosotros por un imprevisto de este tipo.

Interpretación: No se garantiza que las conexiones sean seguras, ni si están capacitadas para manejar información confidencial de la empresa o clientes, además de no tener un protocolo definido para ello.

Pregunta 4: ¿Cuál es el tipo de personal que tiene acceso a las claves digitales o certificados?

Esta pregunta busca saber el nivel de acceso y a que jerarquía pertenecen los colaboradores que poseen acceso a estas llaves digitales, si son aptos o qué formación y conocimiento tienen y la manera de elegir a dichos colaboradores para que manejen un instrumento que está directamente relacionado con la seguridad de los datos de sus clientes y de la empresa como un todo.

Respuesta del gerente Rafael Núñez: Solo el gerente general y el contador de la empresa.

Respuesta de José Delgado, encargado de TI: Solo el gerente general y el contador de la empresa.

Interpretación: Al ser una respuesta tan directa, se intuye que no hay una jerarquía establecida, sino que dichas claves y certificados están atadas a individuos específicos, lo cual es bueno, pero se pone en duda la efectividad de este método ante una situación de incidente, lo cual es una brecha de seguridad por tomar en cuenta.

Pregunta 5: ¿En el pasado se ha presentado algún altercado relacionado con los métodos de comunicación actuales, nos lo puede detallar?

Esta pregunta busca expandir el historial de la empresa relacionado con accidentes digitales si es que existen, y en caso de que fuera el caso, cómo se realizó la operación, qué pérdidas hubo y el motivo del incidente.

Respuesta del gerente Rafael Núñez: En un pasado hubo un *hackeo* del dominio de la página web, se tuvo que hacer un cambio de proveedor debido a ello.

Respuesta de José Delgado, encargado de TI: Hubo un *hackeo* del dominio de nuestra web, la cual tuvo que cambiar de proveedor, lo que más afectó fue la falta de un plan de acción y la capacidad de respuesta por parte de TI frente a esta situación.

Interpretación: Al haber incidentes digitales de este tipo se confirma que existe poca preparación del personal frente a una situación de este tipo, además de una brecha adicional por la ausencia de un procedimiento y plan de acción en caso de incidentes informáticos.

Preguntas sobre Activos Tecnológicos

Pregunta 1: ¿Cómo se clasifican los activos tecnológicos presentes en la empresa?

Esta pregunta busca saber cuáles son los activos que el colaborador considera críticos para la operación de la empresa, además de su proceso de clasificación o si hay una jerarquía interna entre estos activos y el porqué de su clasificación.

Respuesta del gerente Rafael Núñez: No sabría decirle, realmente en mi caso desconocería con certeza una clasificación específica de los activos en un ámbito informático, podría identificar el área de servidores como un activo físico y la propia información como uno digital.

Respuesta de José Delgado, encargado de TI: En nuestro caso el activo crítico más importante es la información de nuestros clientes, la información de la empresa y los equipos de la empresa en ese orden jerárquicamente hablando, el porqué de esta clasificación se basa en lo que nosotros consideramos nuestra mayor prioridad y tarea en TI.

Interpretación: El área de TI tiene clara la clasificación y una jerarquía funcional de los activos de la empresa, no mencionan un proceso formal de esta jerarquía o política, además de subcategorías dentro de estas que puedan ameritar ser establecidas, lo cual algo funcional, pero no lo preferible.

Pregunta 2: ¿Cuál son los procedimientos actuales para la protección de los activos físicos y digitales?

Esta pregunta toca un punto importante en la investigación ya que se busca saber cuáles son los procesos actuales para la protección de los activos, si siguen alguna norma internacional, en el caso de que sea incorrecto esto sería una brecha de seguridad grave a nivel logístico y digital.

Respuesta del gerente Rafael Núñez: Procedimientos formales no tenemos, este aspecto es puramente de TI y desconocería los detalles técnicos de su operación frente a este tópico.

Respuesta de José Delgado, encargado de TI: A nivel de formalidad no tenemos, los colaboradores del área de TI se limitan a sus tareas de protección digital principalmente debido al problema que tuvimos con el dominio y en el apartado físico sí carecemos bastante de algún procedimiento o norma como las que menciona.

Interpretación: Esto confirma una brecha de seguridad grave dentro de la operabilidad de la empresa, siendo un problema que debe ser corregido para garantizar la seguridad de la información.

Pregunta 3: ¿La arquitectura actual cuenta con un *firewall*? En caso de ser así, ¿qué criterios se utilizan para su configuración y operación?

Esta pregunta busca conocer la presencia de herramientas de ciberseguridad como un *firewall*, cómo funciona, qué configuración utiliza, si se alinea con lineamientos internacionales comprobados y si directamente existe dentro de la estructura empresarial.

Respuesta del gerente Rafael Núñez: Sí, tenemos un *firewall*, los criterios específicos no los tendría claros y tendría que consultar con TI para una explicación más a detalle.

Respuesta de José Delgado, encargado de TI: El *firewall* que tenemos es básico, pero cumple de momento con una protección robusta, siendo el encargado de su operación tres colaboradores de TI, los cuales lo manipulan dependiendo de alguna actividad que lo amerite o notifique y no es basado en ninguna normal internacional.

Interpretación: No se menciona de manera explícita en ambos entrevistados la configuración que utilizan, pero se confirma la presencia de esta herramienta de vanguardia en seguridad de la información de la empresa.

Pregunta 4: ¿Qué medidas se toman en cuenta de cuándo se deben actualizar los parámetros del *firewall* o qué situaciones los ha llevado a realizarlo?

Esta pregunta busca saber en qué situaciones se ha debido usar el *firewall* y sobre todo si ha sido efectivo gracias a su configuración, en caso contrario se debe dar una reorganización de este y poder enriquecerlo con parámetros alienados con lineamientos internacionales comprobados y efectivos.

Respuesta del gerente Rafael Núñez: Los parámetros como tales no los sé, pero sí se tuvo que realizar una modificación grande después de lo ocurrido con el *hackeo* de nuestro dominio en el pasado.

Respuesta de José Delgado, encargado de TI: Generalmente se la hace una revisión periódica, el tiempo en sí no está del todo establecido, pero sí se actualiza de acuerdo con las necesidades que se consideren, no se sigue ningún estudio o guía internacional, se rige únicamente por los colaboradores de TI.

Interpretación: El *firewall* con tal no cumple con los parámetros deseados por las normas, además de no alienarse a ninguna, es una configuración personalizada que se modifica si se amerita, lo cual representa un peligro para la seguridad de la información.

Preguntas sobre Políticas de Seguridad de la Información

Pregunta 1: ¿Tienen conocimiento sobre los marcos internacionales referentes a la seguridad de la información?

Esta pregunta busca saber el conocimiento del entrevistado respecto a referentes internaciones como lo son las normas NIST e ISO, pilares importantes en cada empresa con un entorno de seguridad de la información presente.

Respuesta del gerente Rafael Núñez: Realmente no, dentro de la empresa no conozco estos términos ni su funcionalidad

Respuesta de José Delgado, encargado de TI: Conozco ambas, pero no seguimos ninguna de las dos dentro de la empresa, los criterios de seguridad son más que todo personalizados a nuestras operaciones, pero sería bastante mejor y conveniente un modelo donde podamos implementar dichas normas para una mayor seguridad.

Interpretación: No hay presencialidad de ninguna norma dentro de la empresa, pero sí conocimiento por parte de TI de estas, aunque sin aplicación.

Pregunta 2: ¿Existen políticas de seguridad de la información en la empresa? ¿Se alinean con algún marco internacional?

Se busca saber, en caso de no tener conocimiento sobre la seguridad de la información y sus referentes, cuáles son las políticas internas de la empresa y el porqué de la existencia de estas

en vez de actualizarse con un modelo adaptable y seguro como el que ofrecen las normas NIST e ISO.

Respuesta del gerente Rafael Núñez: No tengo conocimiento sobre estas políticas, pero últimamente hemos buscado una mayor capacitación e inversión en este apartado.

Respuesta de José Delgado, encargado de TI: No existen políticas de seguridad de la información dentro de la empresa de manera formal, lo cual es un punto para mejorar por parte de nosotros ya se depende bastante del conocimiento de TI en este aspecto que se nos delegó.

Interpretación: No existen procedimientos formales ni alineación con marcos internacionales.

Pregunta 3: ¿Qué tanto conocimiento y dominio tiene el personal sobre estas políticas y su importancia?

Esta pregunta busca que el entrevistado, preferiblemente un alto cargo, dé una perspectiva del dominio de sus colaboradores sobre la seguridad de la información en apartados como respuestas a incidentes, dominio del tema y la importancia que tiene para la empresa, tanto para evitar incidentes como para saber responder a ellos en caso de una situación que lo amerite.

Respuesta del gerente Rafael Núñez: Bastante poca, estamos intentando invertir en una cultura empresarial más al tanto de estos temas para una mejor respuesta ante otro incidente como el que ya pasamos.

Respuesta de José Delgado, encargado de TI: Poco por parte del personal aparte del personal de TI, lo cual dificulta ante la respuesta y también una tendencial alta al error de algún colaborador que si querer filtre información sensible.

Interpretación: Esto es una falta grande por parte de la empresa, esta falta de capacitación puede hacer que la curva de aprendizaje para los colaboradores ajenos a TI frente a lo propuesto signifique un reto y una brecha de seguridad evidente.

Pregunta 4: En caso de no tenerlas, ¿qué metodología siguen los colaboradores de la empresa con respecto al trato de la seguridad de la información de la empresa y los activos que este término acoge?

Esta pregunta, en caso de tener una respuesta negativa de la anterior, intenta mapear qué principios siguen los colaboradores relacionados con este tema y cómo enfrentan estos problemas y garantizan la seguridad de los activos dentro de la empresa, buscando saber si son ineficientes o escalables de acuerdo con la propuesta presente.

Respuesta del gerente Rafael Núñez: Hemos hecho varias charlas de ciberseguridad para reforzar este especto dentro de nuestros colaboradores.

Respuesta de José Delgado, encargado de TI: Charlas sobre ciberseguridad principalmente, dentro de TI la metodología que seguimos es impartida por mi persona y las propias habilidades informáticas de mi equipo.

Interpretación: No se puede decir que se garantice la seguridad de activos debido a la gran posibilidad de que colaboradores fuera de TI cometan un error, se evidencia una diferencia grande de conocimiento entre ambas partes de la empresa, ante lo cual la inversión en charlas de ciberseguridad no es suficiente.

Pregunta 5: ¿Considera que el personal conoce el impacto de la seguridad de la información y sus riegos potenciales, con la ausencia de procedimientos y políticas que lo respalden (en caso de concluir que no los tienen) y cómo esto puede afectar al panorama de la empresa en general?

Esta pregunta busca saber si realmente se conocen las consecuencias de la inexistencia de procedimientos y políticas de la empresa y la posición en la cual esto podría dejar a la empresa en caso de no tener el conocimiento, formación, cultura y cuidado respecto a un apartado tan importante como la seguridad de la información en un ambiente empresarial y la correcta protección de sus activos críticos.

Respuesta del gerente Rafael Núñez: Varios colaboradores conocen su impacto, solo que no se considera tan vital desde lo que nos ocurrió en un pasado, ahora lo estamos volviendo una prioridad escalable por medio de charlas y capacitaciones en este tema para una mejor preparación.

Respuesta de José, encargado de TI: Sí, al ver la reciente inversión de la empresa en este tema se ha cambiado la actitud de manera positiva, por medio de charlas y sobre todo capacitaciones, lo cual será beneficioso en el largo plazo.

APÉNDICE C. CUESTIONARIO

En el marco de una investigación sobre de Propuesta para la Protección de Activos Físicos y Digitales, basándose en las normas ISO/IEC 27001 y NIST SP 800-53 para la empresa Electric Cars of Costa Rica, ubicada en Heredia, le invitamos a completar este cuestionario. Su participación es de gran importancia para comprender cómo el tema en estudio influye en la actividad de la organización.

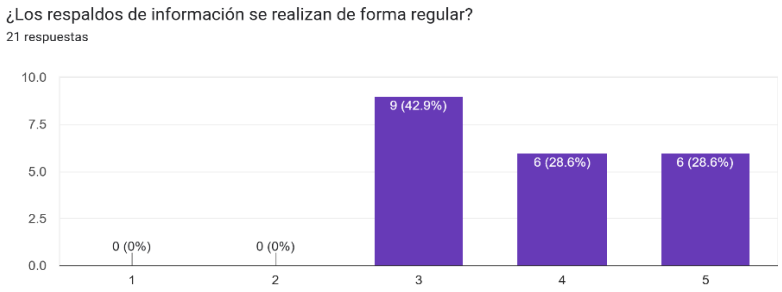
Este cuestionario es confidencial. Sus respuestas solo se utilizarán con fines de investigación y no serán compartidas con ninguna otra persona o institución. Completar el cuestionario tomará aproximadamente 10 minutos.

Las respuestas están ordenadas según el grado de entendimiento de la persona encuestada sobre el tema, problemática u opinión, siendo 1 la opción más baja y 5 la más alta.

Apartado relacionado con el respaldo de los datos

Pregunta 1: ¿Los respaldos de información se realizan de forma regular?

Esta pregunta busca principalmente conocer con qué frecuencia se realizan dentro de la empresa, saber el conocimiento de los colaboradores sobre el tema y si están al tanto de este procedimiento, el cual es importante para la seguridad de los datos no solo de los clientes sino también de la empresa.

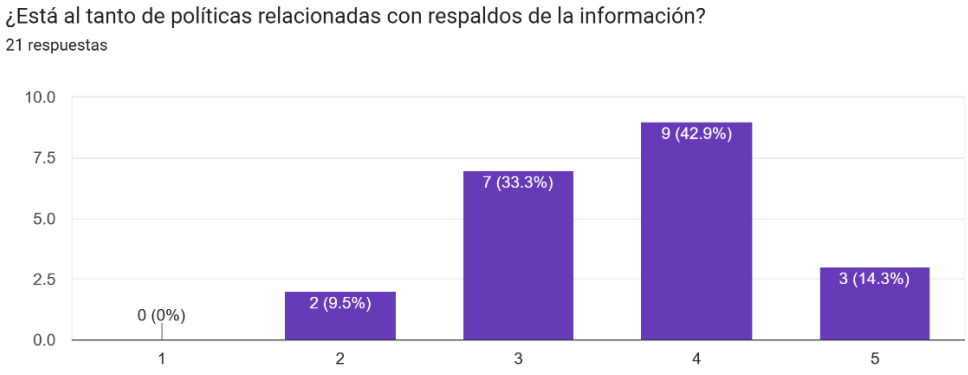


Fuente: Elaboración propia.

Ese resultado remarca una posición neutral, tirando a óptima, con un porcentaje de 42% neutral y un 28% en las posiciones más altas, evidenciando la presencia de este mecanismo de seguridad de la información dentro de la empresa, dejando solo la incógnita de la distribución de la regularidad de estos respaldos y el cada cuanto se realizan o el motivo por el cual se lleven a cabo en la operabilidad general de la empresa.

Pregunta 2: ¿Está al tanto de políticas relacionadas con respaldos de la información?

Siguiendo de la pregunta anterior, esta busca evaluar el conocimiento y teoría sobre los respaldos de la información dentro de la empresa, las políticas que definen este procedimiento y el interés o impacto que podría generar el no tener al menos una percepción básica sobre este concepto.

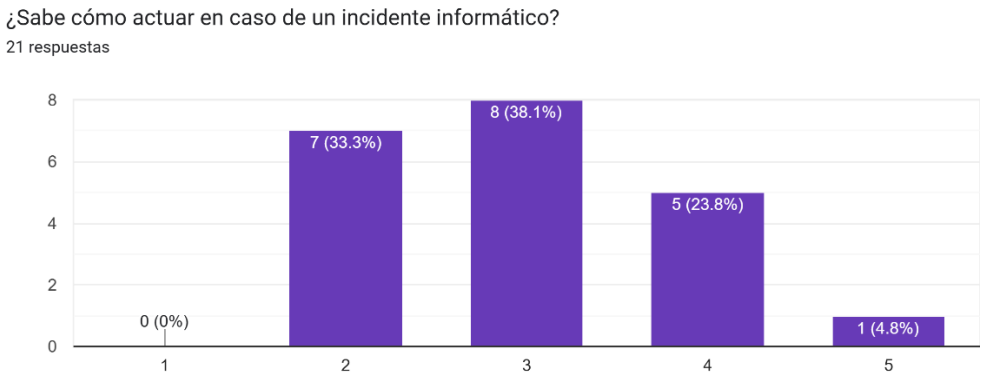


Fuente: Elaboración propia.

La presencia de un conocimiento óptimo dentro del ambiente empresarial es algo bastante positivo, siendo la mayoría de la población conocedora de estos temas en un 42% y un 33% neutral, sentando una buena base de las posibles políticas que la empresa aplica para mantener su seguridad de la información, aunque estas no sean oficiales o posean un referente reconocido. Estos datos confirman el escepticismo y también ciertas causas de los problemas presentes dentro de la empresa respecto a las políticas de seguridad de la información.

Pregunta 3: ¿Sabe cómo actuar en caso de un incidente informático?

Esta pregunta busca evaluar el apartado de acción de los colaboradores en caso de que pase un incidente, de tener una puntuación inferior se entenderá que la empresa no cuenta con un apartado lo suficientemente robusto en caso de incidentes y además que sus colaboradores no están entrenados en las acciones que se deben aplicar en caso de que ocurra.

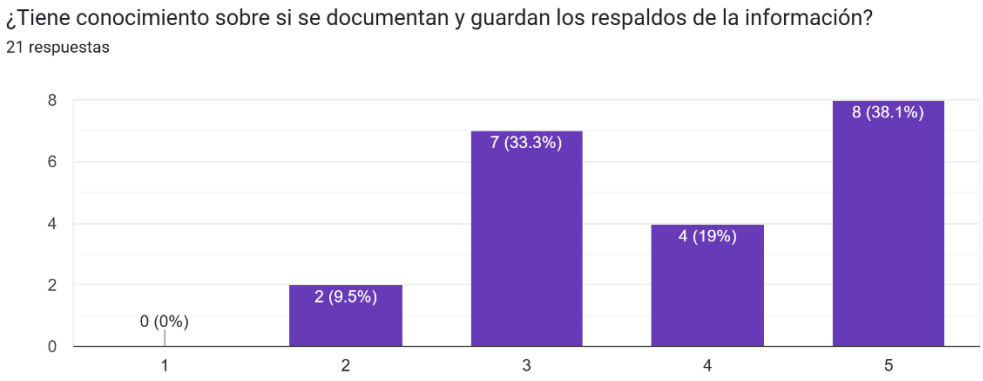


Fuente: Elaboración propia.

Este apartado muestra que a la hora de un incidente informático la mayoría de la población permanece escéptica ante el problema, representado por un 38% con una postura neutral y un 33% como no del todo segura del proceder en el caso de darse un caso y cómo deberán actuar para mitigar los daños a activos físicos y digitales; a pesar de eso, el porcentaje restante refleja que tiene conocimiento y procederes para este tipo de situaciones. Esto confirma la necesidad de un plan de acción frente a incidentes presentes dentro de la operabilidad de la empresa.

Pregunta 4: ¿Tiene conocimiento sobre si se documentan y guardan los respaldos de la información?

Esta pregunta evalúa el conocimiento sobre la existencia de una bitácora, respaldo o copia de seguridad de los datos; si muchos colaboradores tienen el conocimiento del lugar donde se guardan estos respaldos, pues lo contrario podría significar una brecha de seguridad.



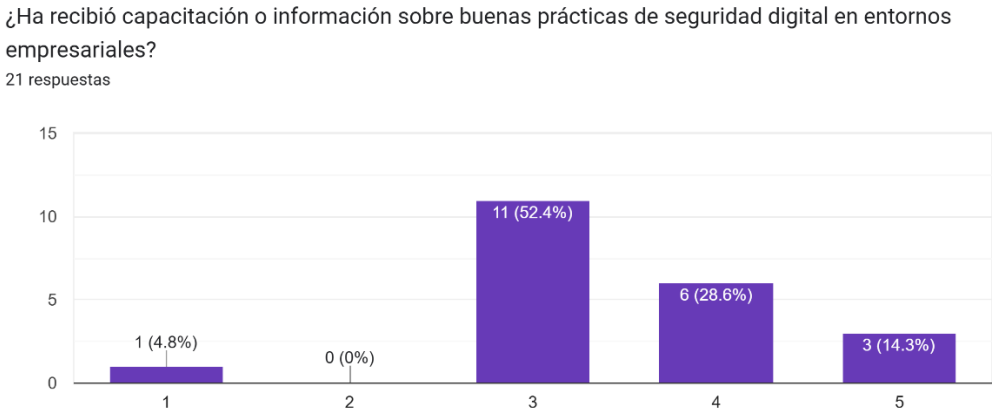
Fuente: Elaboración propia.

Este apartado también brinda un panorama positivo en cuanto a que la mayoría de la población sabe que existe documentación y guardado de datos, representando casi la totalidad dado que solo un 9,5% marcó un desconocimiento -no total- sobre estos procederes dentro de la empresa. Estos resultados serán beneficiosos para la formalización de dichos procedimientos y políticas propuestos.

Apartado relacionado con políticas de seguridad de la información y cultura empresarial

Pregunta 1: ¿Ha recibió capacitación o información sobre buenas prácticas de seguridad digital en entornos empresariales?

Esta pregunta busca ampliar el conocimiento sobre la formación del personal de la empresa sobre los tópicos de seguridad de información y comprobar si la carencia de estos es el motivo de alguna brecha de seguridad de la información y la seguridad digital en entornos empresariales o corporativos.

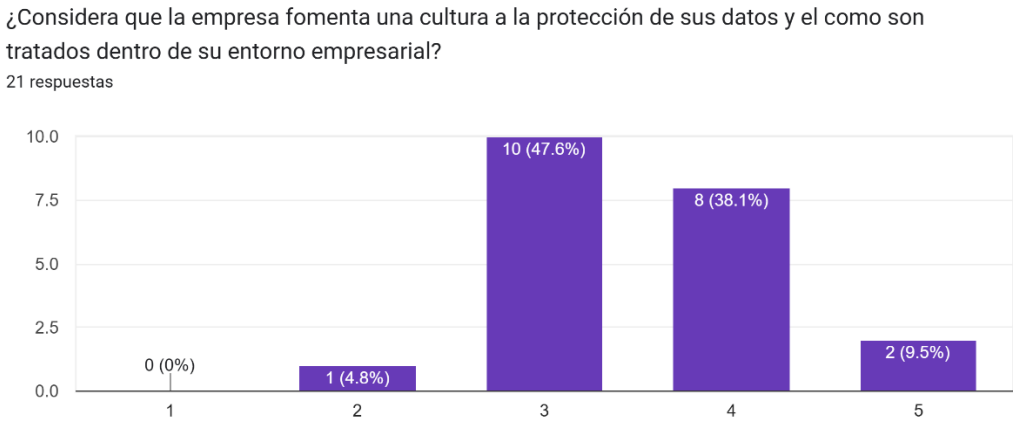


Fuente: Elaboración propia.

Estos resultados reflejan una capacitación principalmente funcional para la mayoría de los participantes, representado casi la totalidad que ha recibió capacitación sobre buenas prácticas de seguridad digital, solo un 4,8% de la población no recibió del todo una capacitación sobre estos temas. Esto facilitará la adaptación del personal a las nuevas políticas y procedimientos propuestos, partiendo de una base funcional para un cambio que beneficiará su operabilidad en este tema.

Pregunta 2: ¿Considera que la empresa fomenta una cultura a la protección de sus datos y el cómo son tratados dentro de su entorno empresarial?

Esta pregunta busca saber si la empresa tiene un interés activo sobre la protección de sus datos y lo fomenta dentro de su ambiente empresarial, para evitar problemas de seguridad de la información, o en el caso contrario, más bien comprometiéndola.

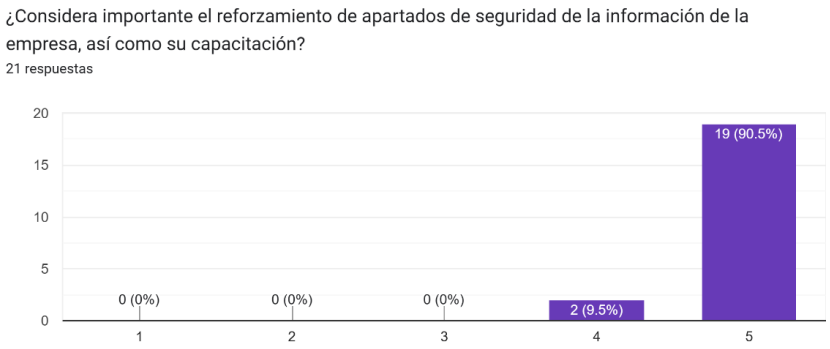


Fuente: Elaboración propia.

Estos resultados demuestran que, aunque existan capacitaciones, la mayoría de los participantes a nivel de cultura empresarial se muestran neutrales, representados por un 47% de la población, un 38% indica que sí se fomenta, evidenciado la existencia de la cultura, pero a su vez no como un pilar dentro de su operabilidad, lo cual puede derivar en un riesgo de seguridad de la información.

Pregunta 3: ¿Considera importante el reforzamiento de apartados de seguridad de la información de la empresa, así como su capacitación?

Esta pregunta busca cerrar esta sección, dándole la posibilidad al colaborador de señalar la carencia de políticas de seguridad de la información si lo considera algo necesario de mejorar, así como su propia formación en estos tópicos, evidenciando la necesidad de una propuesta que ataque esta problemática.



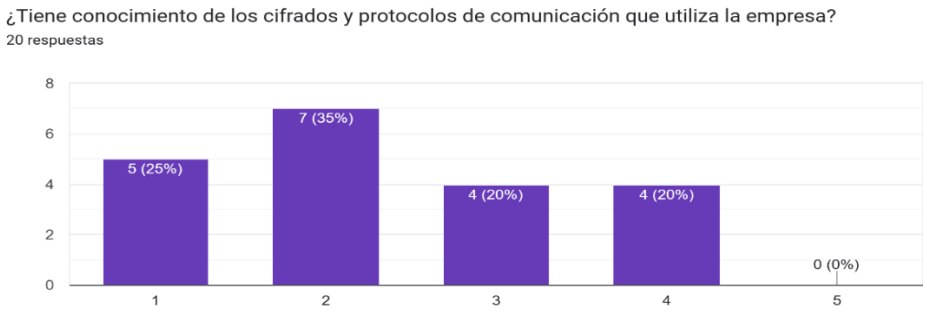
Fuente: Elaboración propia.

Aquí se evidencia que la totalidad de la población confirma la necesidad de la presencia y reforzamiento en los apartados de seguridad de la información, así como su propia capacitación sobre estos temas, confirmando la necesidad propia de la empresa sobre la propuesta de este estudio y lo que puede aportarle para una mejoría escalable y adaptable.

Apartado relacionado con cifrado y comunicaciones

Pregunta 1: ¿Tiene conocimiento de los cifrados y protocolos de comunicación que utiliza la empresa?

Este apartado busca evaluar el conocimiento a nivel técnico sobre temas como el cifrado de datos, tanto en dispositivos utilizados por los colaboradores como los que utiliza la empresa para su operación, al conocer esta posición se podrá evaluar el nivel entendimiento de los colaboradores.

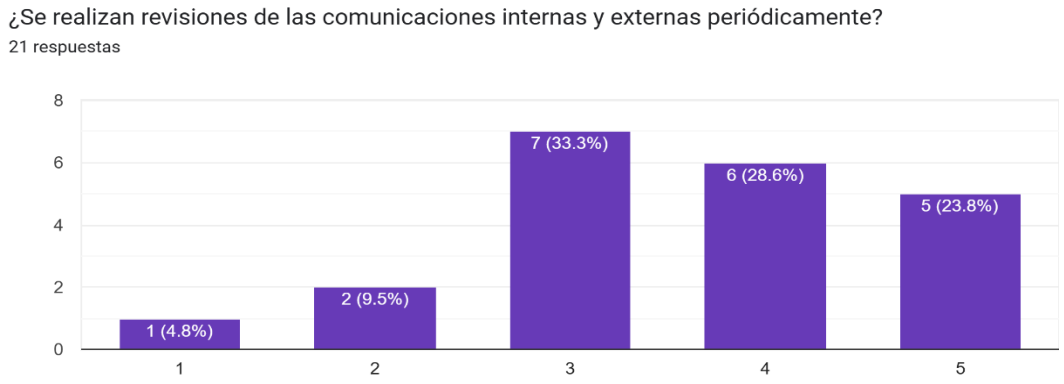


Fuente: Elaboración propia.

Estos resultados, aunque en varias divisiones, indican que la mayoría de la población no tiene conocimientos de ningún tipo sobre estos apartados y aún más preocupante ninguno evidencia domino total sobre ellos, evidenciando que los protocolos pueden ser no seguros u obsoletos, y mostrando un punto débil bastante grande, así como la necesidad de indagación sobre el tema y la operabilidad de este dentro de la empresa.

Pregunta 2: ¿Se realizan revisiones de las comunicaciones internas y externas periódicamente?

Esta pregunta tiene como objetivo saber si hay un control o revisiones sobre las comunicaciones de los dispositivos, esto ayudará a saber si hay brechas de seguridad debido a la falta de revisiones periódicas.



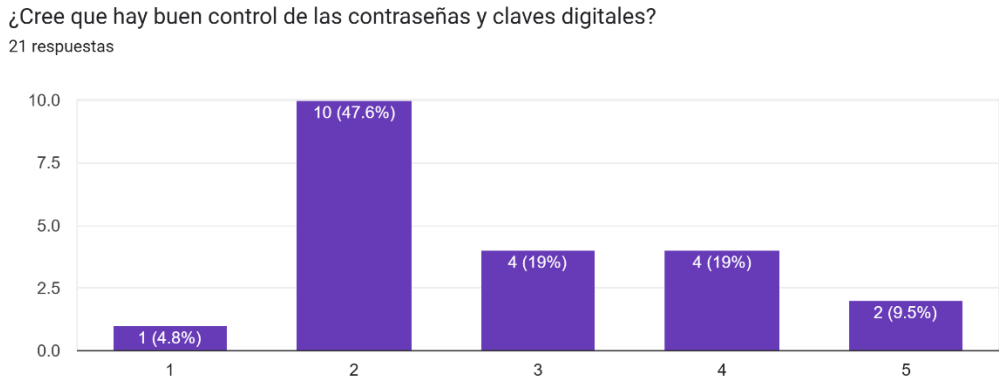
Fuente: Elaboración propia.

Estos resultados evidencian la existencia de dichas revisiones dentro de las comunicaciones de la empresa, estableciendo una periodicidad posiblemente no tan regulada debido a las variantes en las respuestas, pero siendo un punto de partida positivo para la formalización de la periodicidad de dichas previsiones.

Pregunta 3: ¿Cree que hay buen control de las contraseñas y claves digitales?

Esta pregunta busca conocer el nivel control y gestión de contraseñas dentro de la empresa, en caso de que fuera bajo podría significar una brecha de seguridad grave debido al poco

entendimiento sobre la importancia de crear contraseñas por medios seguros, y de las personas que tienen acceso a dichas contraseñas o claves digitales.



Fuente: Elaboración propia.

Estos resultados evidencian una brecha de seguridad grave y justifican la necesidad de políticas y procedimientos formales que puedan controlar estos apartados, siendo que el 47% opina que no hay buen control; este es un porcentaje preocupante debido a la brecha de seguridad que podría significar el mal control de contraseñas y claves digitales.