Análisis de las Vulnerabilidades Tecnológicas, a Nivel de Personal e Infraestructura, en la Empresa Sonda Costa Rica, a partir del Segundo Cuatrimestre del Año 2023

Marianela Isabel Marín Masís

Facultad de Ingeniería, Universidad Latina de Costa Rica

Trabajo Final de Graduación para Optar por el Grado de Licenciatura en Sistemas de la Información con Énfasis en Tecnologías para la Gestión de los Negocios

Profesor: Omar Alejandro Palma Sagot

San Pedro, agosto, 2023

UNIVERSIDAD LATINA DE COSTA RICA
POWERED BY Arizona State University

TRIBUNAL EXAMINADOR

Este proyecto titulado: Análisis de las Vulnerabilidades Tecnológicas, a Nivel de Personal e Infraestructura, en la Empresa Sonda Costa Rica, a partir del Segundo Cuatrimestre del Año 2023, por el (la) estudiante: Marianela Isabel Marín Masís, fue aprobado por el Tribunal Examinador de la carrera de Ingeniería de la Universidad Latina, Sede San Pedro, como requisito para optar por el grado de Licenciatura en Sistemas de la Información con Énfasis en Tecnologías para la Gestión de los Negocios:

OMAR ALEJANDRO PALMA SAGOT (FIRMA)
Digitally signed by OMAR ALEJANDRO PALMA SAGOT (FIRMA)
Date: 2023.10.03 07:30:54 -06'00'

Ph.D.Omar Alejandro Palma Sagot
Tutor


Firmado digitalmente por RAUL JAVIER CHANG TAM (FIRMA)
Fecha: 2023.10.08 14:56:57 -06'00'

Mba. Ing Raúl J. Chang T.
Lector

Fabiola Chavarría Arredondo
Firmado digitalmente por Fabiola Chavarría Arredondo
Fecha: 2023.10.10 10:40:33 -06'00'

Lic. Fabiola Chavarría Arredondo
Lector

RONALD DAVID CAMACHO PEREZ (FIRMA)
Firmado digitalmente por RONALD DAVID CAMACHO PEREZ (FIRMA)
Fecha: 2023.10.16 11:51:43 -06'00'

Ronald David Camacho Pérez
Representante

DECLARACIÓN JURADA

Yo, Marianela Isabel Marín Masís estudiante de la Universidad Latina de Costa Rica, declaro bajo la fe de juramento y consciente de las responsabilidades penales de este acto, que soy Autor Intelectual del Trabajo Final de Graduación titulado:

Análisis de las Vulnerabilidades Tecnológicas, a nivel de Personal e Infraestructura, en la Empresa Sonda Costa Rica, a partir del segundo cuatrimestre del año 2023.

Por lo que librero a la Universidad de cualquier responsabilidad en caso de que mi declaración sea falsa.

Firmo en San José, 18 de octubre de 2023

Marianela Isabel Marín Masís

Licencia De Distribución No Exclusiva (carta de la persona autora para uso didáctico)

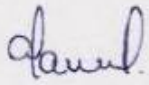
Universidad Latina de Costa Rica

Yo (Nosotros):	Marianela Isabel Marín Masís
De la Carrera / Programa:	Licenciatura en Sistemas de la Información con énfasis en Tecnologías para la Gestión de los Negocios
Modalidad de TFG:	Tesis
Titulado:	Análisis de las vulnerabilidades tecnológicas, a nivel de personal e infraestructura, en la empresa Sonda Costa Rica, a partir del segundo cuatrimestre del año 2023.

Al firmar y enviar esta licencia, usted, el autor (es) y/o propietario (en adelante el "**AUTOR**"), declara lo siguiente: **PRIMERO:** Ser titular de todos los derechos patrimoniales de autor, o contar con todas las autorizaciones pertinentes de los titulares de los derechos patrimoniales de autor, en su caso, necesarias para la cesión del trabajo original del presente TFG (en adelante la "**OBRA**"). **SEGUNDO:** El **AUTOR** autoriza y cede a favor de la **UNIVERSIDAD U LATINA S.R.L.** con cédula jurídica número 3-102-177510 (en adelante la "**UNIVERSIDAD**"), quien adquiere la totalidad de los derechos patrimoniales de la **OBRA** necesarios para usar y reusar, publicar y republicar y modificar o alterar la **OBRA** con el propósito de divulgar de manera digital, de forma perpetua en la comunidad universitaria. **TERCERO**: El **AUTOR** acepta que la cesión se realiza a título gratuito, por lo que la **UNIVERSIDAD** no deberá abonar al autor retribución económica y/o patrimonial de ninguna especie. **CUARTO**: El **AUTOR** garantiza la originalidad de la **OBRA,** así como el hecho de que goza de la libre disponibilidad de los derechos que cede. En caso de impugnación de los derechos autorales o reclamaciones instadas por terceros relacionadas con el contenido o la autoría de la **OBRA**, la responsabilidad que pudiera derivarse será exclusivamente de cargo del **AUTOR** y este garantiza mantener indemne a la **UNIVERSIDAD** ante cualquier reclamo de algún tercero. **QUINTO**: El **AUTOR** se compromete a guardar confidencialidad sobre los alcances de la presente cesión, incluyendo todos aquellos temas que sean de orden meramente institucional o de organización interna de la **UNIVERSIDAD SEXTO**: La presente autorización y cesión se regirá por las leyes de la República de Costa Rica. Todas las controversias, diferencias, disputas o reclamos que pudieran derivarse de la presente cesión y la materia a la que este se refiere, su ejecución, incumplimiento, liquidación, interpretación o validez, se resolverán por medio de los Tribunales de Justicia de la República de Costa Rica, a cuyas normas se someten el **AUTOR** y la **UNIVERSIDAD**, en forma voluntaria e incondicional. **SÉPTIMO**: El **AUTOR** acepta que la **UNIVERSIDAD**, no se hace responsable del uso, reproducciones, venta y distribuciones de todo tipo de fotografías, audios, imágenes, grabaciones, o cualquier otro tipo de

presentación relacionado con la **OBRA**, y el **AUTOR**, está consciente de que no recibirá ningún tipo de compensación económica por parte de la **UNIVERSIDAD**, por lo que el **AUTOR** haya realizado antes de la firma de la presente autorización y cesión. **OCTAVO**: El **AUTOR** concede a **UNIVERSIDAD.**, el derecho no exclusivo de reproducción, traducción y/o distribuir su envío (incluyendo el resumen) en todo el mundo en formato impreso y electrónico y en cualquier medio, incluyendo, pero no limitado a audio o video. El **AUTOR** acepta que **UNIVERSIDAD.** puede, sin cambiar el contenido, traducir la **OBRA** a cualquier lenguaje, medio o formato con fines de conservación. **NOVENO**: El **AUTOR** acepta que **UNIVERSIDAD** puede conservar más de una copia de este envío de la **OBRA** por fines de seguridad, respaldo y preservación. El **AUTOR** declara que el envío de la **OBRA** es su trabajo original y que tiene el derecho a otorgar los derechos contenidos en esta licencia. **DÉCIMO:** El **AUTOR** manifiesta que la **OBRA** y/o trabajo original no infringe derechos de autor de cualquier persona. Si el envío de la **OBRA** contiene material del que no posee los derechos de autor, el **AUTOR** declara que ha obtenido el permiso irrestricto del propietario de los derechos de autor para otorgar a **UNIVERSIDAD** los derechos requeridos por esta licencia, y que dicho material de propiedad de terceros está claramente identificado y reconocido dentro del texto o contenido de la presentación. Asimismo, el **AUTOR** autoriza a que en caso de que no sea posible, en algunos casos la **UNIVERSIDAD** utiliza la **OBRA** sin incluir algunos o todos los derechos morales de autor de esta. **SI AL ENVÍO DE LA OBRA SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA U ORGANIZACIÓN QUE NO SEA UNIVERSIDAD U LATINA, S.R.L., EL AUTOR DECLARA QUE HA CUMPLIDO CUALQUIER DERECHO DE REVISIÓN U OTRAS OBLIGACIONES REQUERIDAS POR DICHO CONTRATO O ACUERDO. La presente autorización se extiende el día** 18 **de** octubre **de** 2023 **a las** 13:30

Firma del estudiante(s):



CARTA DEL FILÓLOGO

San Pedro, 15 de agosto de 2023

Señores
Comité de Trabajos Finales de Graduación
Escuela de Tecnologías de la Información y Comunicación
Universidad Latina de Costa Rica
S. D.

Estimados Señores:

He revisado y corregido el trabajo final de graduación denominado: "**Análisis de las vulnerabilidades tecnológicas a nivel de personal e infraestructura, en la Empresa Sonda Costa Rica, a partir del segundo cuatrimestre del Año 2023**, elaborado por la estudiante Marianela Isabel Marín Masís, cédula de identidad 114860275, para optar por grado académico de Licenciatura en Sistemas de la Información con énfasis en Tecnologías para la Gestión de los Negocios.

Corregí el trabajo en aspectos, tales como: construcción de párrafos, vicios del lenguaje que se trasladan a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico y, desde ese punto de vista, considero que está listo para ser presentado como Trabajo final de graduación, por cuanto cumple con los requisitos establecidos por la Universidad.

Se suscribe de ustedes, cordialmente,

JOSE ANTONIO CABRERA GUADAMUZ (FIRMA)

Firmado digitalmente por JOSE ANTONIO CABRERA GUADAMUZ (FIRMA)
Fecha: 2023.08.15 23:59:28 -06'00'

M.Sc. José Antonio Cabrera Guadamuz
Carné N° 5979-82
Colegio de Licenciados y Profesores en Letras, Filosofía, Ciencias y Artes
Teléfono: 88189074
Correo electrónico: apgtecnologias@gmail.com

Agradecimiento

Quiero agradecer en primer lugar a Dios por permitirme finalizar con éxito esta etapa de mi vida, a todas las personas e instituciones que contribuyeron a la realización de este trabajo de investigación. Su apoyo y colaboración fueron fundamentales para alcanzar los objetivos y obtener resultados significativos. En particular, deseo expresar mi gratitud a mis profesores por su orientación experta, valiosos consejos y paciencia a lo largo de este proceso de investigación, a la empresa Sonda que brindó acceso a sus recursos y datos, lo que permitió llevar a cabo este estudio de manera efectiva.

A mis compañeros y colegas, por sus ideas y comentarios constructivos, que enriquecieron el trabajo y estimularon el debate, pero, sobre todo, a mi familia por su apoyo incondicional, comprensión y ánimo en todo momento. Este trabajo de investigación no habría sido posible sin su colaboración y apoyo.

Agradezco sinceramente a cada uno de ustedes por su contribución, ya que su compromiso hizo que este trabajo se convirtiera en una realidad. Su generosidad y disposición para ayudar son invaluables, y espero que este escrito sea útil y beneficioso para la comunidad académica y profesional.

Gracias nuevamente por su apoyo y confianza en esta investigación

Dedicatoria

Este trabajo está dedicado a mi familia, en especial a mi esposo Claudio y mi hijo Antonio, quienes con su constante apoyo y sacrificio han sido la fuerza motivante detrás de cada logro que he alcanzado. Agradezco a mi mamá Rosario y mi hermano José Esteban cuyo amor incondicional y apoyo inquebrantable me han impulsado a alcanzar mis metas y superar obstáculos a lo largo de mi vida.

También quiero dedicar este trabajo a mis profesores y mentores, cuyo conocimiento y guía me han enriquecido académicamente y me han alentado a nunca dejar de aprender y crecer. A todas aquellas personas que han dejado una huella en mi vida, que me han empujado a seguir adelante y me han demostrado que el esfuerzo y la perseverancia dan frutos, les dedico este trabajo con gratitud y admiración.

Gracias a cada una de estas personas especiales por ser mi constante inspiración y mi razón para seguir esforzándome día a día. Sin ustedes, este logro no sería posible.

Resumen

En el presente trabajo de investigación se realizará una evaluación sobre el estado de la ciberseguridad en la empresa SONDA. Con esto, se podrán detectar puntos débiles y áreas de mejora, para los cuales se enumerarán recomendaciones técnicas, con el fin de mejorar la robustez en seguridad digital de la compañía.

En un mundo íntimamente relacionado con el Internet y la tecnología, el resguardo de la presencia en estos medios tecnológicos toma especial relevancia. Las consecuencias de un ataque cibernético pueden ser devastadoras, sin importar el objeto de ataque; personas, empresas y hasta países enteros pueden sufrir daños considerables si descuidan su seguridad digital.

Se eligió la empresa SONDA debido a la facilidad con la que se pueden adquirir los datos necesarios para la investigación. La confidencialidad juega un papel importante en esta obra, pues la información sensible no será violentada durante el desarrollo del trabajo.

Para llevar a cabo la investigación, se evaluará la empresa en dos dimensiones: infraestructura tecnológica y colaboradores. Con la primera dimensión, se revisará la edificación digital que posee SONDA y se determinarán cuáles prácticas recomendadas siguen, tanto en ciberseguridad como seguridad física de sus centros de datos.

Con respecto al personal, se realizarán encuestas que permitan conocer el grado de conocimiento en la materia. Tomando estos resultados como insumo, se conocerán áreas débiles que podrían comprometer tanto la seguridad digital de SONDA como la de sus

colaboradores. Para subsanar esta problemática, se realizarán recomendaciones a seguir que minimicen el riesgo del personal de sufrir un ataque cibernético.

Abstract

The following text will make an evaluation about the state of cybersecurity in the company Sonda. With this, weak points and improvement areas will be detected, for which technical recommendations will be enlisted, towards an improvement in the company's digital security robustness.

In a world closely related to the Internet and technology, protection of the presence in these technological means takes special relevance. The consequences of suffering a cyber-attack can be devastating, regardless of the type of attack; people, companies and even whole countries can suffer considerable damages if they disregard their digital security.

The company SONDA was chosen due to the ease with which the data necessary for the investigation can be acquired. Confidentiality plays an important role in this text, since sensible information won't be violated during the development of it.

To carry out the research, the company will be evaluated in two dimensions: technological infrastructure and collaborators. With the first dimension, the digital infrastructure that Sonda owns will be reviewed and the recommended practices will be determined, both in cybersecurity and physical security of their data centers.

With respect to personnel, surveys will be carried out to determine the degree of knowledge in the matter. By taking these results as an input, weak areas will be known that could compromise both the digital security of Sonda and that of its collaborators. To correct this

problem, recommendations will be made to minimize the risk of personnel suffering a cyber attack.

Tabla de contenido

Índice de Figuras

Índice de Tablas

Capítulo 1: Generalidades del Proyecto

1.1 Introducción

En el presente trabajo se realizará una evaluación sobre el estado de la ciberseguridad en la empresa SONDA. Con esto, se podrán detectar puntos débiles y áreas de mejora, para los cuales se enumeran recomendaciones técnicas, con el fin de mejorar la robustez en seguridad digital de la compañía. “Cada día más empresas y Corporativos, se adaptan a los nuevos cambios y necesidades de la sociedad, por tal motivo se encuentran sistematizando la información mediante uso de tecnologías de computación y muy especialmente la implementación de redes informáticas” (Martínez, Ocampo, & Bermúdez, 2017, pág. 22).

En un mundo íntimamente relacionado con el Internet y la tecnología, el resguardo de la presencia en estos medios tecnológicos toma especial relevancia. Las consecuencias de un ataque cibernético pueden ser devastadoras, sin importar el objeto de ataque; personas, empresas y hasta países enteros pueden sufrir daños considerables si descuidan su seguridad digital. A pesar de que los medios de comunicación bombardean con sus noticias sobre ataques cibernéticos a empresas de renombre mundial, lo cierto es que, cualquier compañía está propensa a recibir un ataque, basta con tener una computadora con acceso a Internet para sufrir desde un robo o alteración de información por parte de los hackers hasta una suplantación de identidad inclusive, realizando ataques a terceras personas.

Se eligió la empresa SONDA debido a la importancia en el mercado costarricense en el ámbito de las tecnologías de la información y las comunicaciones, además la facilidad de adquisición de los datos necesarios para la investigación y la anuencia de sus personeros en contribuir con esta investigación. La confidencialidad juega un papel importante en esta investigación, pues la información sensible no será violentada durante el desarrollo del trabajo.

Para llevar a cabo la investigación, se evaluará la empresa en dos dimensiones: infraestructura tecnológica y colaboradores. Con la primera dimensión, se revisará la edificación digital que posee SONDA y se determinarán cuáles prácticas recomendadas siguen, tanto en ciberseguridad como seguridad física de sus centros de datos: El término ciberseguridad es definido por la Unión Internacional de Telecomunicaciones (UIT) como:

> La colección de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, pautas, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, garantías y tecnologías que pueden usarse para proteger la entorno cibernético y organización y activos del usuario. (Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S, 2022)

Con respecto a la segunda dimensión correspondiente al personal, se realizarán encuestas que permitan conocer el grado de conocimiento en temas de ciberseguridad. Tomando estos resultados como insumo, se conocerán áreas débiles que podrían comprometer tanto la seguridad digital de SONDA como la de sus colaboradores. Para subsanar esta problemática, se realizarán recomendaciones a seguir que minimicen el riesgo del personal de sufrir un ataque cibernético.

1.2. Antecedentes del Problema

En los últimos años, el mundo ha sido testigo de un aumento significativo en la dependencia de la tecnología digital y la conectividad en todos los aspectos de la vida. Las organizaciones han migrado hacia entornos digitales para operar y almacenar datos, lo que ha generado una cantidad creciente de información valiosa y sensible en línea. Sin embargo, esta creciente dependencia también ha llevado a un aumento en los ciberataques y las amenazas cibernéticas.

En una investigación realizada por la Promotora del Comercio Exterior de Costa Rica, se refleja la necesidad de las empresas por invertir en ciberseguridad, en este estudio, el 89% de los encuestados se ha visto afectado por la ciberdelincuencia y se observa una necesidad de las empresas costarricenses en incluir dentro de sus costos anuales con el fin de minimizar amenazas y evitar la exposición de una manera significativa. De acuerdo con este estudio,

Entre las empresas que invierten, la protección mediante la aplicación de controles para mitigar riesgos y proteger activos es su principal prioridad; seguido de otros intereses como la detección de amenazas (para el 85% de las empresas); y la identificación de las probabilidades de los riesgos (81%). Este perfil de prioridades refleja que el abordaje de ciberseguridad en las empresas es mayormente preventivo, pero con poco enfoque en acciones centradas en respuesta (38%) y recuperación ante ataques (66%). (Apuy, 2022)

En este contexto, las empresas a nivel mundial se encuentran ante el desafío de proteger los sistemas, datos y activos internos y de sus clientes contra una variedad de riesgos, incluyendo ataques de hackers, malware, phishing, ransomware y vulnerabilidades de software. La evolución constante de las tácticas de ataque y la aparición de nuevas amenazas hacen que la ciberseguridad sea una tarea continua y en constante evolución.

Además, la implementación de regulaciones y estándares de cumplimiento, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos, ha llevado a las organizaciones a tomar medidas más sólidas para garantizar la privacidad y protección de los datos de sus clientes.

Existen estudios internacionales donde se mide el nivel se cultura en materia de ciberseguridad de las empresas, tal es el caso del informe presentado por PWR realizado en España en el año 2020, entre sus manifestaciones se encuentran, “El 86% de las compañías considera que no existe una cultura de ciberseguridad en la organización o bien esta debería de mejorarse. El resultado del estudio muestra poca madurez en la cultura de ciberseguridad de las compañías actuales en España.” (PWR, 2020)

SONDA es una empresa latinoamericana, líder en tecnología, que posee varias sedes en la región, una de ellas en Costa Rica, en este país cuenta con más de 50 empleados y ofrece a sus clientes servicios basados en dos grandes divisiones, Digital Business y Digital Services. Dentro de la división de servicios, se encuentran subdivisiones como ciberseguridad, workplace services, cloud & datacenter y servicios de plataforma, de esta manera le permite extender soluciones como gestión de plataformas de ciberseguridad, detección de amenazas y vulnerabilidades, seguridad ofensiva, consultoría, entre otros.

Con respecto a la seguridad de datos a nivel interno en la regional de Costa Rica, hace unos años se realizó una implementación de mejoras en seguridad por parte del departamento de informática interna. Sin embargo, debido al ingreso de nuevo personal en los últimos años, no se ha tenido claridad en los procesos de aseguramiento de la información interna.

En definitiva, no todos los ataques cibernéticos vienen en forma de virus o malware, existen otras formas de infectar a las empresas.

> En la actualidad la potencia de las herramientas informáticas y su fácil acceso nos enfrenta a todo tipo de ataques, desde los más sofisticados que acabamos de presentar, hasta un niño que descarga y explota de Internet y sin tener mayor conocimiento de lo que hace, lo ejecuta contra nuestra empresa. (Corletti Estrada, 2017, pág. 43).

De esta manera se tiene claro que, sin importar el tamaño de la empresa, todas están expuestas a cualquier tipo de ataque. Por esto, es importante que los colaboradores tengan claras las mejores prácticas de ciberseguridad que permitan a la organización consolidar una sólida defensa contra ataques y vulnerabilidades informáticas.

Aunado a lo anterior, tras la pandemia por la COVID-19 iniciada en el año 2019, la modalidad de teletrabajo ha sido implementada en la mayoría de las empresas, incluyendo SONDA Costa Rica. Esto provocó que los colaboradores utilicen herramientas de acceso remoto a los sistemas, en una época donde los ciberataques se han enfocado en comprometer los sistemas e infectar toda una red, o robar información importante y comprometedora de una organización.

Por estas razones, la revisión y el análisis de las posibles amenazas internas es esencial para las empresas que trabajan con datos confidenciales e incluye desarrollar políticas y obtener el compromiso de cada colaborador en el proceso del aseguramiento de la información.

1.3 Justificación

En un mundo en constante cambio y evolución, es crucial tomar decisiones informadas y estratégicas en todos los ámbitos de la vida, ya sea en los negocios, en la educación, la salud u otros campos. De esta forma, las empresas cada vez se ven en la necesidad de proteger sus datos de posibles ataques en la red.

En los últimos años, la cantidad de usuarios en Internet ha aumentado exponencialmente.

> En enero del 2023, el número de usuarios de internet en el mundo alcanzó los 5.160 millones de personas, lo que representa al 64,4% de la población mundial. El número de internautas se incrementó un 1,9% respecto de 2022, en 98 millones de personas, un ritmo algo inferior al de los años anteriores. (Galeano, 2023).

Puesto que se tiene una presencia cada vez mayor en Internet y, de manera similar, una adopción continua de la tecnología, se incrementan también los riesgos de sufrir ataques cibernéticos y esto se ha ido incrementando desde hace varios años. “En los inicios de la pandemia por la Covid-19 se registró un aumento de 300% en los crímenes cibernéticos” (Clavellina Miller & Domínguez Rivas, 2020).

Es alarmante la cantidad de intentos de robo de identidad, “Durante agosto del 2020, Google detectó 18 millones de correos phishing relacionados a la pandemia cada día” (Hernández Armenta, 2020). De esta forma, en la actualidad, cada vez se nota más la importancia de la seguridad de la información en las organizaciones. Costa Rica no es la excepción.

De acuerdo con el informe del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), el ciberataque al Gobierno de Costa Rica es un ataque informático de índole extorsivo que se habría iniciado el domingo 17 de abril del 2022 en perjuicio de distintas

> instituciones públicas de la República de Costa Rica, incluido el Ministerio de Hacienda, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el Instituto Meteorológico Nacional (IMN), la Radiográfica Costarricense Sociedad Anónima (RACSA), el Ministerio de Trabajo y Seguridad Social (MTSS), el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y la Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC), la Caja Costarricense del Seguro Social (CCSS).
>
> El grupo de origen ruso Conti (también conocido como Wizard Spider, TrickBot, Ryuk, UNC1878 y Karakurt) se atribuyó el ciberataque (a excepción del caso de la CCSS que fue un incidente en sus redes sociales y en sus bases de datos que CONTI no se atribuyó) y solicitó un rescate de 10 millones de dólares estadounidenses a cambio de no liberar la información sustraída del Ministerio de Hacienda, la cual podría incluir información sensible como las declaraciones de impuestos de los ciudadanos y empresas que operan en Costa Rica. (Comisión Nacional de Emergencias, 2022)

Los datos anteriores reflejan una necesidad imperiosa de resguardar la presencia en Internet y el uso de dispositivos digitales. Como se puede apreciar, los delitos cibernéticos ocurren indistintamente del contexto o del autor que ejecute la interacción con los medios tecnológicos: personas, empresas y países son afectados por igual cuando de cibercriminales se trata. Aún más, con el continuo crecimiento en Internet y el advenimiento de tecnologías más modernas, como el Internet de las Cosas (IoT, por sus siglas en inglés), es de esperar que el interés por los delitos cibernéticos y la ciberseguridad incrementen en los años siguientes.

El presente trabajo pretende proveer una introducción a la ciberseguridad y los beneficios que reporta su adopción, tanto para individuos como empresas. Además, busca analizar el estado

de la seguridad cibernética actual de la compañía SONDA, estudiando tanto su infraestructura tecnológica como el conocimiento de sus colaboradores en temas de ciberseguridad. Con esto, se generará conciencia sobre los riesgos presentes en la constitución actual de la empresa.

Se enumerarán y presentarán las recomendaciones a seguir para optimizar los procesos y aspectos de ciberseguridad relacionados a la empresa. De esta forma, la compañía tendrá un beneficio directo, al recibir sugerencias de mejora sobre sus procesos digitales. Por su parte, los colaboradores serán beneficiados indirectos, al adquirir conocimiento relacionado a la materia.

1.4 Planteamiento del Problema

En la era digital actual, las organizaciones enfrentan constantemente amenazas cibernéticas que buscan comprometer la seguridad de sus redes y sistemas. A medida que evolucionan las técnicas y herramientas utilizadas por los atacantes, resulta crucial que las empresas implementen medidas de seguridad efectivas para proteger su información confidencial y mantener la continuidad de sus operaciones.

> En definitiva, la tecnología progresa a la par que avanza la sociedad, razón por la cual, resulta imprescindible la creación de programas y métodos capaces de contrarrestar la creciente oleada de delincuencia que opera a través de la red. Esto lo conseguiremos, como comentábamos anteriormente, a través de programas capaces de penetrar en los sistemas de seguridad del ordenador, como son el malware, spyware, adware, entre otros. (Sánchez, J. F. E, 2019).

Uno de los elementos clave en la estrategia de seguridad de una organización es el sistema de detección de intrusiones en red, el cual tiene como objetivo detectar y prevenir actividades maliciosas dentro de la red corporativa.

> En muchas ocasiones hasta los sistemas más seguros pueden ser infligidos por los mismos usuarios autorizados, por lo tanto, mantener un sistema de seguridad no es nada fácil y peor aún diseñar estos tipos de programas a prueba de todo tipo de error es un proceso difícil de llevar a cabo, se debe tener en cuenta otros tipos de controles adicionales y externos de la máquina. (Martínez, Ocampo, & Bermúdez, 2017).

Sin embargo, la eficacia de estos sistemas puede variar según diversos factores, como la configuración, las reglas de detecciones utilizadas, la capacidad de adaptación a nuevas amenazas y la colaboración con otros componentes de seguridad. Por lo tanto, surge la necesidad

de llevar a cabo una investigación que evalúe de manera integral la eficacia de los sistemas de detección de intrusiones en redes corporativas.

1.5 Problema general

De acuerdo con lo anterior es que se define la siguiente pregunta como problema general.

¿Cómo minimizar el impacto de un posible ataque cibernético, a nivel del personal e infraestructura tecnológica, en la empresa Sonda Costa Rica a partir del segundo cuatrimestre del año 2023?

1.6 Problemas Específicos

A continuación, se detallan los problemas específicos identificados como parte de la investigación:

¿Cómo conocer las vulnerabilidades tecnológicas que tiene Sonda Costa Rica respecto al estándar ISO 27001?

¿Cómo diagnosticar vulnerabilidades tecnológicas y categorizar su riesgo, dentro de Sonda Costa Rica?

¿Cómo identificar el nivel de conocimiento del personal de Sonda Costa Rica en aspectos de ciberseguridad?

¿Qué herramienta debe utilizar el personal de Sonda para minimizar el impacto de un ataque cibernético?

1.7 Objetivos

El objetivo principal de esta investigación es analizar y comparar de acuerdo con los estándares de ciberseguridad, las prácticas que se realizan en la empresa SONDA con el fin de identificar fortalezas, debilidades y áreas de mejora en su desempeño. Además, se pretende investigar las mejores prácticas para la configuración y gestión de la seguridad de la red, buscando proporcionar a la organización recomendaciones sólidas y basadas en evidencia para mejorar su postura de seguridad cibernética y protegerse de manera efectiva contra las amenazas actuales y futuras.

Luego, se graficarán los resultados obtenidos y se realizará una guía con recomendaciones a seguir a partir de ellos. Con esto, se mejorará la seguridad digital de SONDA y se proveerá de conocimiento más especializado a sus colaboradores. En el siguiente apartado se definen los objetivos de la investigación, de acuerdo con lo presentado anteriormente.

1.7.1 Objetivo general

A continuación, se presenta el objetivo general de la investigación:

Recomendar un plan de acción que debe ser ejecutado por el personal de Sonda Costa Rica, respecto a las mejores prácticas en temas de seguridad para su infraestructura tecnológica, a partir del segundo cuatrimestre del año 2023.

1.7.2 Objetivos específicos

En el siguiente apartado se presentan los objetivos específicos del trabajo de investigación:

1. Identificar el nivel de cumplimiento de la empresa Sonda con respecto a la norma ISO 27001, mediante una evaluación informática que considere las prácticas de seguridad aplicadas en la actualidad.

2. Analizar los riesgos informáticos, de infraestructura y personal, identificando la severidad de cada vulnerabilidad encontrada.

3. Realizar una encuesta para conocer los hábitos de seguridad de la información en el personal, para determinar su nivel de experticia.

4. Elaborar un plan de acción que considere los lineamientos establecidos en el documento ISO 27001 y los hallazgos de la encuesta.

1.8 Delimitación del Tema

La delimitación del tema en un trabajo de investigación es un proceso crucial que permite establecer los límites y alcance de la investigación, definiendo claramente qué aspectos serán abordados y cuáles serán excluidos. En el campo de la ciberseguridad, donde las amenazas y desafíos son abundantes y en constante evolución, la delimitación del tema se vuelve aún más relevante para garantizar la viabilidad y el enfoque adecuado de la investigación.

Para lograr facilitar la realización de este trabajo se van a definir los alcances investigativos proporcionando información necesaria como descripción, límites, objetivos, personas involucradas, entre otros factores importantes con el fin de delimitar, aclarar y detallar lo más posible la importancia del proyecto. Sin embargo, es esencial establecer una delimitación precisa para evitar la dispersión y asegurar un enfoque más profundo y significativo.

"La delimitación de las características de la población no solo depende de los objetivos de la investigación, sino de otras razones prácticas". (Hernández Sampieri, Fernández, & Baptista Lucio, 2018, pág. 199). Para esta investigación uno de los alcances serán las personas que participarán del estudio, en total son 27 personas que serán encuestadas, por medio de correo electrónico institucional, en un máximo de un mes y se finalizará cuando el 100% de las personas respondan la encuesta.

Este trabajo será una investigación de tipo descriptiva, pues interesa analizar la situación empresarial y su relación con el fenómeno de los ataques informáticos. Para ello, es necesario describir el contexto que engloba a la compañía en materia de ciberseguridad, así como también enlistar los conocimientos técnicos requeridos para llevar a cabo la investigación.

En el alcance descriptivo ya se conocen las características del fenómeno y lo que se busca, es exponer su presencia en un determinado grupo humano. En el proceso

> cuantitativo se aplican análisis de datos de tendencia central y dispersión. En este alcance es posible, pero no obligatorio, plantear una hipótesis que busque caracterizar el fenómeno del estudio. (Ramos Galarza, 2020).

También se realizará una entrevista a la persona encargada del área de redes y comunicaciones de la empresa SONDA con el objetivo de tener un panorama amplio sobre las prácticas que se mantienen en la compañía en temas de ciberseguridad a nivel de infraestructura realizando una comparación con las mejores prácticas recomendadas por el estándar ISO 27001 para equipos de comunicaciones. De acuerdo con el sitio web de IBM,

> La seguridad de datos es la práctica que consiste en proteger la información digital contra el acceso no autorizado, la corrupción o el robo durante todo su ciclo de vida. Es un concepto que comprende todos los aspectos de la seguridad de la información, desde la seguridad física del hardware y los dispositivos de almacenamiento hasta los controles administrativos y de acceso, así como la seguridad lógica de las aplicaciones de software. También incluye las políticas y los procedimientos de la organización. (IBM, 2021).

De esta forma, se esperan obtener los datos necesarios para continuar con el análisis de estos y obtener las conclusiones respectivas con el fin de brindar las recomendaciones más precisas, también permite enfocar los esfuerzos en áreas específicas de interés, garantizando la viabilidad y relevancia de los resultados obtenidos.

1.9 Restricciones y/o Limitaciones

Este trabajo brinda una introducción a la ciberseguridad, los principales riesgos a los que se exponen quienes la descuidan y su relevancia en la sociedad humana actual. Una vez se ha esclarecido el trasfondo técnico subyacente y reconocido la importancia de la seguridad digital, se tomará como caso de estudio la empresa SONDA, específicamente, para analizar su preparación y conocimiento en la materia.

Para evaluar la seguridad digital en SONDA, se estudiará su cumplimiento de las mejores prácticas de ciberseguridad en dos dimensiones: el personal humano y la infraestructura tecnológica. Con la primera dimensión, se llevarán a cabo encuestas que permitan determinar el nivel de conocimiento y preparación en materia de ciberseguridad, basado en el estándar ISO 27002, así como los riesgos más comunes a los que están expuestos actores individuales dentro de una compañía o en su vida personal.

Con respecto a la infraestructura tecnológica, el presente trabajo se apoyará en información brindada por el personal técnico encargado de la administración de las redes y comunicaciones de la empresa SONDA y su comparación con la normativa ISO 27001. De esta forma, se podrá conocer el grado de robustez adoptado por la compañía, así como puntos débiles que podrán ser blindados antes de sufrir un ciberataque.

Con los datos recolectados en ambas dimensiones, se realizará un análisis estadístico descriptivo que permita visualizar clara y comprensiblemente los resultados obtenidos. Con ellos, se detectarán áreas de mejora y puntos débiles actualmente presentes en SONDA, en ambas dimensiones de estudio. Con los resultados y el análisis de la compañía como base, se elaborará una guía con recomendaciones a seguir para resguardar los procesos relacionados a la seguridad digital que tienen lugar en SONDA.

Por último, se enumeran a continuación las limitaciones que enmarcan el desarrollo del presente trabajo. Estas restricciones fueron identificadas a partir del tiempo, recurso humano y recurso técnico disponible al momento de efectuar la obra escrita:

1. Los procesos relacionados a desarrollo de software no serán considerados para realizar la evaluación de ciberseguridad en Sonda Costa Rica.
2. No se considerarán vulnerabilidades fuera de las halladas durante la evaluación informática.
3. El estudio se realizará solamente a 27 colaboradores de la empresa, encuestadas por medio de correo electrónico institucional, a partir del segundo cuatrimestre del año 2023, para analizar las prácticas en materia de ciberseguridad.
4. No se solicitará información sensible ni confidencial sobre los clientes u otros actores relacionados a Sonda Costa Rica.
5. Se realizarán únicamente recomendaciones a ejecutar por el departamento de Tecnologías de la Información de la empresa Sonda Costa Rica, quien será el encargado de ejecutar y aplicar los cambios que consideren pertinentes.
6. Se seguirán las pautas que establezca el patrocinador por parte de Sonda.
7. Sólo se considerará la empresa Sonda Costa Rica para dicha investigación.
8. La investigación se realizará por un término de un cuatrimestre.

Capítulo 2: Marco Teórico

2.1 Marco Situacional

En el actual entorno empresarial altamente competitivo y en constante cambio, comprender y evaluar el contexto en el que opera una empresa se vuelve esencial para garantizar su éxito y supervivencia a largo plazo. Esta sección proporciona una visión integral de la empresa donde se enfocará la investigación, además de aspectos relevantes que pueden afectar el desempeño y la estrategia de la organización.

SONDA es una empresa de origen chileno, fundada en 1974 por Andrés Navarro Haeussler. Al cabo de la primera década tomaron la decisión de emprender fuera de Chile iniciando un proceso de internacionalización que paulatinamente fue expandiendo sus sedes a través de Latinoamérica, incluyendo Costa Rica en el año 2003. Absorbió una pequeña empresa de tecnología llamada anteriormente Datadec convirtiéndose en un recinto más del líder en transformación digital que es ahora.

Se encuentra ubicada en la provincia de San José, Guadalupe en Ofiplaza del Este. Esta sede cuenta con más de 50 empleados y forma parte del grupo de países CANSAC. Sus 11 sedes se rigen bajo un mismo propósito, que es “contribuir a mejorar la calidad de vida de las personas, innovando y agregando valor por medio de soluciones tecnológicas que desarrollen y transformen el negocio y quehacer de nuestros clientes”. (Sonda.com, 2023).

Sonda corporación cuenta con diferentes clientes de distintas industrias como por ejemplo Smart Cities, Educación, Salud, Minería y recursos naturales, Gobierno, Enterprise Applications, Retail y comercio, siendo su concepto una verticalización por industrias como parte de la estrategia de negocio. También cuentan con soluciones personalizadas que se adaptan a cualquier estilo y preferencia de negocio, siendo esto un valor agregado para la empresa.

2.1.1 Tipo de servicio y mercado meta

SONDA atiende clientes con necesidades en los campos tecnológicos, agregando valor por medio de soluciones que desarrollen y transformen el negocio y el que hacer de los clientes.

"Cuenta con un gran portafolio de servicios y soluciones integradas de TI para dar respuesta a los desafíos de nuestros clientes, responder a sus necesidades del negocio y mejorar la calidad de vida de la sociedad." (Sonda.com, 2023).

Entre sus clientes más importantes en la región se encuentran tanto entidades gubernamentales como organizaciones privadas, de todos los sectores de la industria, por ejemplo acueductos, municipalidad, entidades financieras, entre otros. Esto se debe a la importancia de la transformación tecnológica que han tenido las compañías en esta nueva era.

Dentro de la industria de gobierno, uno de los principales desafíos consiste en el uso eficiente de los recursos públicos, de esta forma, Sonda se manifiesta con un énfasis en la transparencia y visibilidad de los mismos, con el objetivo de aumentar la participación ciudadana y mejorar los mecanismos de fiscalización de la información pública. Por otro lado, en el área de salud, existe un crecimiento y exigencia por parte de los usuarios con respecto a la calidad de los servicios médicos y la atención integral de los pacientes, por lo que Sonda representa un aliado estratégico cuando se trata de implementar nuevas tecnologías para el bienestar de las personas y sus familias.

En cuanto al área de Smart Cities, la demanda por el crecimiento de la población es cada vez mayor, Sonda trata de integrar lo mejor de los servicios tanto públicos como privados, ofreciendo soluciones con servicios públicos y sistemas de transporte mejor diseñadas con el objetivo de aumentar la eficiencia y sostenibilidad del entorno, principalmente en ciudades

donde la preocupación por el medio ambiente y el uso de los recursos naturales sea el eje de la estrategia del negocio.

En esta rama, Sonda cuenta con servicios y soluciones como Smart City Transport, las cuales corresponden a soluciones orientadas a apoyar los sistemas de recaudación y cobro automatizado para la red de transporte público y privado. También está Smart Safety, como soluciones integrales orientadas a la gestión centralizada y eficiente de la red de seguridad y Smart Lighting, enfocados en la administración eficiente del consumo eléctrico de los sistemas de alumbrado público y privado a través de la región.

2.1.2 Misión, visión y valores

Su misión es “contribuir a mejorar la calidad de vida de las personas, innovando y agregando valor por medio de soluciones tecnológicas que desarrollen y transformen el negocio y quehacer de nuestros clientes.” (Sonda.com, 2023).

En cuanto a la visión se encuentran los siguientes apartados:

- ✓ Reconocidos como socio estratégico de nuestros clientes en los procesos de transformación digital.
- ✓ Líder global de la industria TI en soluciones de negocio innovadoras.
- ✓ Compañía ágil, digital y con servicios de excelencia.
- ✓ Un ambiente de trabajo atractivo, que permita atraer y retener talentos tecnológicos con el colaborador al centro.

Los valores de Sonda como corporación son vocación de servicio, empresa de personas, agilidad, actitud positiva y sobriedad. (Sonda.com, 2023)

2.1.3 Políticas institucionales

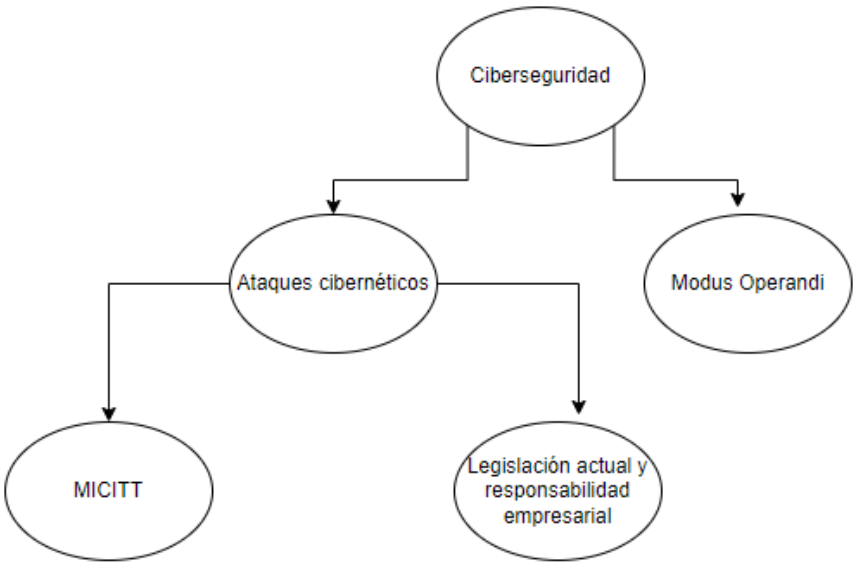
No existe ninguna política institucional que incide directamente en esta investigación, las políticas existentes comprenden códigos de ética, manejo de relaciones con los clientes, manejo de donaciones o aportes sociales, entre otros.

Considerando lo expuesto anteriormente, surge la necesidad de un estudio sobre el manejo de las mejores prácticas en materia de seguridad de la información, así como una validación de la ciberseguridad de la infraestructura física instalada en la empresa, mediante el aprovechamiento de las tecnologías de la información.

2.2 Fundamentación Teórica

En los siguientes apartados se definirán los términos más significativos para la investigación y que son de vital importancia para el entendimiento de la materia que se va a exponer en el trabajo. A continuación, se presenta el árbol genealógico de conceptos para la fundamentación teórica de la investigación:

Figura 1. Árbol genealógico de conceptos.



Fuente: elaboración propia, recuperado de https://app.diagrams.net/

2.2.1 Ciberseguridad

Para entender el concepto de ciberseguridad, primero debe comprenderse el concepto de seguridad que radica en un estado de bienestar, en la ausencia de riesgo por la confianza en alguien o en algo. Existen distintas clases de seguridad como la ambiental, económica, sanitaria, entre otras, sin embargo, generalmente, cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas.

La seguridad puede definirse como:

> La ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son: Prevención del riesgo, Transferir el riesgo, Mitigar el riesgo y Aceptar el riesgo. Cuando se quiere mejorar la seguridad, estas acciones siempre deben ser consideradas sin importar el área. (Romero Castro, y otros, 2018).

Por otro lado, la ciberseguridad "es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica". (Kaspersky.com, 2023).

En la actualidad, es lógico pensar que existen más dispositivos conectados que personas y que los delincuentes son cada vez más creativos.

> Entre los elementos más importantes en la determinación de la calidad de la seguridad informática en una empresa es el respaldo de información y se refiere a este como "uno de los procesos más comunes que realizan las empresas para proteger su información y evitar los problemas con dicha información, los cuales suelen ser muy costosos. (Romero Castro, y otros, 2018).

Adicionalmente, se recomienda tener en cuenta el horario en que se realizan los respaldos, en este caso es mejor programarlos fuera de horario hábil o cuando el tráfico de datos sea menor. También se sugiere un control de medios con el fin de que los respaldos no sean fácilmente accesibles por cualquier persona y mantener una comprensión de la información.

Actualmente, las ciber amenazas son múltiples y heterogéneas y su daño es cada vez mayor debido, principalmente, al crecimiento exponencial de ese espacio cibernético. En el año 2022, 5.000 millones de personas utilizaron Internet y el total global aumentó en casi 200

millones durante el último año. El 63% de la población mundial ahora está en línea y, según el Foro Económico Mundial, los ciberataques están jerarquizados entre los diez riesgos más importantes, tanto en términos de probabilidad de ocurrencia como en generación de daño.

Algunas palabras o términos, desconocidos hace poco tiempo, hoy son fuentes de peligro para la seguridad informática, por ejemplo:

- ✓ El malware consiste en programas que dañan los equipos informáticos sustrayendo datos sin permiso.
- ✓ El spyware son softwares que almacenan y extraen información de computadoras y las traspasan a otras.
- ✓ El ransomware que es una especie de programa que suspende el acceso de las personas a determinadas partes del sistema operativo o a archivos (por ejemplo, encriptándolos), luego el ciberdelincuente solicita un rescate (ransom) económico o de otro tipo para devolver los datos.
- ✓ El ataque distribuido de denegación de servicio (DDoS) que es el bloqueo a un sitio web para impedir la prestación de servicios.
- ✓ El phishing es una operación a través de la cual se solicita información personal que será empleada en beneficio del ciberdelincuente por medio de un sitio web malicioso que se muestra como una entidad legítima y conocida.
- ✓ El hacktivismo, palabra que resulta de la combinación de hacker (o hacking) y “activismo”, para hacer referencia a acciones coordinadas y ejecutadas por miembros de una comunidad online descentralizada para alcanzar un objetivo común. (Romero Castro, y otros, 2018).

Todas estas ciber amenazas poseen características que aumentan su peligrosidad dificultando su control y anulación, de ahí la importancia de la ciberseguridad en el ámbito personal y empresarial.

> En el año 2020 The National Cibersecurity Index (Índice Nacional de Seguridad Cibernética que mide la preparación de los países para prevenir amenazas cibernéticas y gestionar incidentes cibernéticos) ubicaba a Costa Rica en la posición 48 de entre 160 países y en la posición cinco de América, solo superado por Estados Unidos, Paraguay, Chile y Canadá. Para este año 2022, ocupa la posición 65. Esto implica que el país se mantiene en los primeros lugares en cuanto a seguridad informática. (Castro, 2020).

En cuanto a las brechas de ciberseguridad en los últimos años a nivel mundial se pueden mencionar las siguientes:

- ✓ WikiLeaks, noviembre 2010: en el año 2010 se publicaron 251.287 telegramas diplomáticos, intercambiados entre más de 250 embajadas de los Estados Unidos y el Departamento de Estado de los Estados Unidos en Washington.
- ✓ Uber, noviembre 2017: la empresa pagó 100 000 dólares a dos hackers para eliminar los datos robados y ocultar el ciberataque, manteniéndolo en secreto. El ataque incluyó la exposición de nombres, correos electrónicos y números de teléfono de 57 millones de clientes en todo el mundo, así como la información personal de 7 millones de conductores de esa empresa de transporte.
- ✓ Facebook, marzo 2019: cerca de 419 millones de números de teléfono y de identificación de usuario en Facebook fueron almacenados en un servidor online que no estaba protegido por contraseña. Aunque no son tan sensibles como los datos financieros, los números de teléfono pueden ser utilizados por los hackers para spam, phishing o

> fraudes asociados a la tarjeta SIM. Los Estados Unidos, el Reino Unido y Vietnam fueron los países más afectados. (Contreras, 2022).

En Costa Rica, dentro de la Estrategia Nacional de Ciberseguridad de Costa Rica existe un documento llamado “Costa Rica 2030: Objetivos de Desarrollo Nacional”. El escrito plantea los objetivos de desarrollo del país con una visión a largo plazo, a la vez que promueve la colaboración intersectorial y el intercambio de información. En este se establece que el desarrollo de las TIC desempeña un papel de apoyo en diversas dimensiones, incluyendo el crecimiento económico, la inversión social y cultural, y la infraestructura. Según el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), entre los objetivos destaca: “Asegurar telecomunicaciones con diversidad de servicios, cobertura a todos los poblados del país” (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), 2022). Este objetivo busca garantizar el acceso universal a la Internet a través de aumentos incrementales en la conectividad a nivel nacional.

> Desde el mes de abril de 2022, varias entidades gubernamentales costarricenses fueron víctimas de un ataque con ransomware por el grupo Conti, que sustrajo al menos un terabyte de datos del gobierno. Este grupo exigió un rescate de USD 20 millones de dólares y actualmente continúa impactando la capacidad del gobierno para acceder a los sistemas atacados (Álvarez, 2022).

Por otro lado, estos ataques pueden tener diversas formas y motivaciones, desde la obtención de información confidencial hasta el sabotaje de operaciones comerciales tal como se menciona a continuación,

> Los ataques interrumpieron numerosos servicios gubernamentales, incluidos, las plataformas de impuestos y aduanas del país, los servicios digitales de tesorería y al

> menos un proveedor de energía. La Cámara de Exportadores de Costa Rica afirmó que los ataques causaron que el país perdiera USD 200 millones de dólares, debido a la falta de los sistemas aduaneros. Luego de estos ataques, el Departamento de Estado de los Estados Unidos anunció una recompensa de hasta USD 10 millones de dólares por información que ayude a identificar o localizar a algún individuo o grupo de personas que lideren el grupo Conti, así como hasta USD 5 millones de dólares por información sobre cualquier persona que intente o conspire para participar en las actividades de este grupo cibercriminal. (Pérez, 2022).

Las personas pueden ser la línea de defensa más fuerte y actuar como señales de advertencia frente al ciberespionaje y los ciberataques. Según los expertos, la idea sería enfocar la seguridad centrada en el ser humano, de acuerdo con el comportamiento cibernético de éste y así podría emitir una alerta y permitir a los encargados actuar, ya sea previniendo o mitigando la pérdida de datos importantes.

> Lo dicho anteriormente se puede explicar de la siguiente manera: debido a que los equipos de seguridad reciben miles de alertas en un día y no pueden prestarle atención a todas, como resultado pierden la batalla cibernética.
>
> Por lo tanto, estudiando el comportamiento humano y a la vez, analizando los riesgos, los expertos en ciberseguridad podrán identificar rápidamente las anomalías y obtener el contexto necesario para analizar las alertas de actividad de redes maliciosas. Además, los equipos de seguridad tendrían la capacidad de comprender, predecir y actuar ante posibles amenazas a medida que se desarrollan.
>
> Al darle este nuevo enfoque a la seguridad informática, se le está dando mayor importancia al ser humano que está delante de la pantalla y no al ciberdelincuente.

> Cambiar el enfoque del modelo tradicional de la seguridad informática al entendimiento del comportamiento humano, permite una mayor eficacia en la seguridad dentro de una organización y también se compromete con el personal de la empresa como primera línea de defensa de la organización.
>
> Obviamente el factor humano incide en la seguridad informática, ya que son personas quienes forman parte de la seguridad de los sistemas, son personas las que los diseñan, desarrollan, despliegan y configuran, y, por otro lado, son las personas quienes los utilizan, pero las personas no son máquinas, son seres humanos que cometen errores. Por esto es más difícil controlar, mitigar y prevenir el factor humano en la seguridad digital. (Instituto Internacional de Estudios en Seguridad Global, 2020).

La ingeniería social empezó a utilizarse a una escala mayor a finales de los años 80, hoy en día todavía sigue siendo una de las formas más eficaces para vulnerar una empresa, algo que solo se puede solucionar realizando, en primer lugar, una auditoría de ingeniería social para saber hasta qué punto las personas de la empresa son vulnerables, y en segundo lugar mediante una formación y establecimiento de protocolos para concienciar y solucionar dichos fallos.

A finales de la década del 2000 empezó un nuevo y gran desafío de la ciberseguridad que fue cuando se empezó a implantar Internet de las Cosas (“Internet of Things” o IoT). Esto supuso un problema debido a que se tratan de dispositivos domésticos, cámaras o incluso juguetes capaces de conectarse a internet (para obtener nuevas ventajas y comodidades) lo que se convirtió en una puerta de entrada para los ciberdelincuentes con la que tenían la oportunidad de acceder a los hogares, así como un incremento de los dispositivos que los ciberdelincuentes pueden utilizar para realizar sus ataques.

Aunque se ha avanzado mucho en la ciberseguridad de estos dispositivos, todavía hoy existen noticias sobre hackeos masivos de estos tipos de dispositivos, por lo que sigue siendo necesario ser precavidos con su uso.

> La inteligencia artificial y el Machine Learning están empezando a aplicarse al uso ofensivo de la ciberseguridad, y parece ser una tendencia bastante preocupante para los próximos años, dada su capacidad de evolucionar y tomar decisiones incluso de manera no supervisada por una persona. (Cybersecurity, 2020).

La tecnología es un aspecto fundamental de la vida humana actual, brindando muchos beneficios. En primer lugar, se encuentra el fácil acceso a la información con que se cuenta actualmente. En el 2013, la Organización de Estados Americanos indicó que "el acceso a la información es una herramienta clave para fomentar mayor eficiencia y eficacia en las acciones del estado, especialmente en el manejo de recursos públicos, la rendición de cuentas y la transparencia de sus operaciones" (Organización de Estados Americanos, 2013, pág. 9).

Previo a la invención del Internet, era imposible encontrar información, relacionada a cualquier tema, en cuestión de segundos. La masificación de esta red le ha permitido acceder a esta oportunidad a millones de personas alrededor del mundo.

Otro beneficio capital consiste en la conexión con el mundo que ofrece la tecnología.

Casi 4 mil millones de personas utilizan las redes sociales para consumir noticias de manera regular. Ahora, los usuarios no están limitados a las noticias de su medio local, como ocurría cuando la única forma de encontrarlas era a través de las emisoras de radio y televisión nacionales. Actualmente, cualquier persona en Internet puede suscribirse a noticieros de cualquier país del mundo, conectando así con regiones previamente aisladas. (Haider Th.Salim & Hussein Tuama, 2021).

Sin embargo, como ocurre con cualquier oficio, se deben ponderar los riesgos que implica la tecnología. Los peligros relacionados a la privacidad generan especial preocupación.

> La pérdida de privacidad en nuestros tiempos es algo frecuente. Hemos inundado el ciberespacio con toda la información que vamos almacenando consciente o inconscientemente. El espionaje ya no necesita de personas, el celular sabe todo de ti, y próximamente muchos dispositivos también lo harán. Esto no es un futuro lejano, ya está pasando, y se requerirán cada vez más expertos en tecnología que hagan frente a esta situación con desarrollos seguros y programas que no afecten a terceros. (Palacios Echeverría, 2021).

Los riesgos tecnológicos son ahora tan diversos y frecuentes que se ha definido una categoría para agrupar varias actividades relacionadas a ellos: delitos informáticos. Los llamados delitos informáticos, que constituyen actos delictivos que se cometen con la ayuda de las TIC y que aumentan los riesgos en el ciberespacio y ponen en entredicho la seguridad informática, se han ido multiplicando en los últimos años de manera exponencial. Son numerosas las formas y los ámbitos en que se presentan los ciberdelitos. En términos generales se reconocen cuatro grandes categorías: fraudes cometidos mediante la manipulación de computadoras, las falsificaciones informáticas, las modificaciones de programas o datos computarizados, y el acceso no autorizado a servicios y sistemas informáticos. (Universidad de Costa Rica, 2010).

El rápido acceso a la información también puede ocasionar desastres. La seguridad (del latín securitas) se puede referir a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo al que haga referencia en la seguridad. En términos generales, la seguridad se define como “el estado de bienestar que el ser humano percibe y disfruta. (Real Academia Española. 23° Edición, 2022).

En el campo de la seguridad en tecnología, interesa sobremanera la prevención de ataques cibernéticos. Para ello, se deben enumerar los riesgos a los que se exponen los usuarios de ella. La identificación de riesgos consiste en identificar cuáles situaciones podrían afectar el cumplimiento de un determinado proyecto y su respectiva documentación. El qué, por qué y cómo pueden surgir las cosas como base para un análisis posterior. Aunado a esta detección de amenazas, existen técnicas que pueden disminuir el impacto de ataques. Una de ellas es la creación de respaldos o backups. (Instituto Tecnológico de Costa Rica, 2020). “El respaldo de información es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general” (Romero Castro, y otros, 2018, pág. 18).

2.2.2 Ataques cibernéticos

Han transcurrido casi doscientos años desde que se detectó el primer ciberataque de la historia, ocurrido en Francia, en el año 1834. El ingeniero e inventor francés, Claude Chappe, había creado el telégrafo óptico. Este dispositivo era un sistema de transmisión mecánica para largas distancias, el cual era utilizado exclusivamente para el Gobierno francés. Sin embargo, en 1834, dos banqueros galos llamados François y Joseph Blanc, perpetraron el primer ataque cibernético del que se tiene constancia.

> El primer ciberataque registrado en la historia ocurrió en 1834, cuando el inventor francés Claude Chappe creó un telégrafo óptico que tenía dos brazos móviles, cuando querían comunicarse cambiarían de posición y mirarían a través del telescopio. El telegrama era exclusivamente del gobierno hasta que dos banqueros sobornaron al operador para obtener información sobre los movimientos de los mercados nacionales e internacionales que llegaron primero, mientras se peleaban entre los banqueros por información. Para lograrlo el operador que estaba cargo emitía caracteres errados y luego al final agregaba

> un carácter como señal de que se debía eliminar un campo, había un operador que sabía sobre los mensajes y era quien interpretaba la información. Esta situación se descubrió dos años después pero no hubo sanción, ya que no había ninguna ley que sancionara tal conducta. Morales Rojas, J. G. (2022)

Casi 200 años han transcurrido desde ese primer ciberdelito, el cual significó el inicio de una amenaza global que ataca indiscriminadamente. Por esta razón, distintas reglamentaciones y gobiernos, como es el caso del Reglamento General de Protección de Datos (GDPR) en Europa, priorizan la seguridad de la información mediante leyes y estándares normativos. Sin embargo, los ciberdelincuentes reinventan, día a día, sus tácticas digitales para vulnerar los sistemas más sofisticados.

Con el pasar del tiempo, la tecnología ha creado nuevas áreas que, junto con sus impactos positivos a la sociedad, conllevan también nuevos peligros. Las tecnologías emergentes, como la inteligencia artificial, el aprendizaje automático, el 5G o la computación cuántica, y las que están en evolución, como la nube, los vehículos autónomos y los dispositivos conectados al Internet de las Cosas, son blancos cuya seguridad debe resguardarse.

Así como incrementan los medios de transmisión para los ataques tecnológicos, aumentan también sus objetivos. Ya no solo existe el peligro hacia un individuo, sino la amenaza latente hasta para, incluso, países. Por ejemplo, tal como publicó el diario El país.com, en el año 2016 el gobierno de Estados Unidos denunció que Rusia intentó influir en las elecciones presidenciales mediante ciberataques.

Este mismo diario, publicaba en 2017, la noticia sobre el ataque a la firma estadounidense Equifax que puso en peligro la información de 143 millones de personas. Más recientemente, en el año 2022, la BBC News daba cuenta del robo de millones de correos electrónicos y documentos confidenciales del ejército mexicano. También indicaba ese mismo medio que se espera que los delitos cibernéticos le cuesten al mundo US$10,5 billones para 2025, según la firma de investigación de seguridad cibernética Cyber Ventures.

Costa Rica no se escapa de esa realidad. Una publicación del Financiero de abril de 2022 indicaba que los cibercriminales han estado atacando a las entidades públicas y empresas de Costa Rica desde hace años. Un reporte de la firma PwC indica que desde 2019 identificó al menos 180 víctimas en el sector gubernamental atacadas por 26 grupos cibercriminales; sin embargo, este número ha aumentado en los últimos años.

En abril del 2022, Telediario.cr publicaba que los ministerios de Hacienda y de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), así como Caja Costarricense de Seguro Social (CCSS) habían sido hackeadas. Ese mismo mes, el periódico El Financiero daba cuenta de nuevas empresas afectadas por hackeos, a saber: Radiográfica Costarricense S.A. (Racsa), el Instituto Meteorológico Nacional (IMN), el Fondo de Desarrollo Social y Asignaciones Familiares (FODESAF) y el Ministerio de Trabajo y Seguridad Social (MTSS).

Para mayo de ese mismo año, el diario La República informaba que los ataques cibernéticos en Costa Rica habían alcanzado a 27 instituciones estatales; así mismo informó que el presidente de la República, Rodrigo Chaves, reconoció un impacto "enorme" en el comercio exterior y la recaudación de impuestos y afirmó, en su discurso de toma de posesión el 8 de

mayo que: "*Estamos en guerra y eso no es una exageración. Costa Rica está sufriendo un ataque terrorista cibernético y por eso hemos decretado estado de emergencia"*.

A inicios del 2023, el diario La República publicaba que un informe de la Contraloría General de la República daba cuenta de que a raíz del ataque informático al Ministerio de Hacienda en abril de 2022 provocó la pérdida de 25 mil expedientes de cobro digitalizado y más de 18 mil expedientes de cobro asignados a los fiscales, lo que representa un déficit de unos ¢341 mil millones en perjuicio de las finanzas públicas de nuestro país.

2.2.3 Modus operandi

Los tipos de ataques cibernéticos han cambiado a lo largo de los años. En sus inicios de la época más reciente (es decir, alrededor de la década de los ochenta), el objetivo principal de los ataques era la computadora personal de un individuo. Por ello, en esta década se inició con el desarrollo de los programas antivirus, para contrarrestar el accionar ilícito de la época.

Seguidamente, en los noventa con el advenimiento y popularización de Internet, los ataques sobre esta red cobraron más fuerza. Como medida preventiva, se crearon los *firewalls* (en español, *muros de fuego*), los cuales permitían filtrar el tráfico sospechoso proveniente de Internet y, de esta manera, permitir únicamente conexiones legítimas entre la computadora personal y el mundo interconectado del exterior.

Un cambio en el objetivo de los atacantes cibernético ha ocurrido en el pasar del tiempo. A partir del nuevo milenio, los ciberdelincuentes se interesaron en vulnerabilidades específicas de los programas utilizados por los usuarios. En esta época, se pueden encontrar estrategias de suplantación de identidad, donde el atacante se hace pasar por un actor legítimo para perpetrar su actividad. A partir de entonces, el *modus operandi* se volvió cada vez más técnico y complejo,

involucrando tecnologías como computación en la nube, redes multi vectores y objetivos de nivel más macro como gobiernos y empresas.

A continuación, se enumeran algunos de los tipos más comunes de ataques cibernéticos:

- ✓ Ejecución de código remota y arbitraria: Los atacantes pueden correr piezas de código en la computadora afectada, para tener acceso a información sensible o dañar seriamente el equipo. Incluso, pueden llegar a obtener el control completo del mismo.
- ✓ Suplantación de ARP: La suplantación del *Address Resolution Protocol* (en español, *protocolo de resolución de direcciones*), redirige la comunicación entre dos dispositivos hacia un tercero, controlado por el atacante. En este caso, la víctima cree que ha establecido una conexión legítima, cuando en realidad el dispositivo al otro lado de la red fue suplantado por un ciberdelincuente.
- ✓ Desborde de pila: Ocurre típicamente cuando un programa informático recibe más datos que los que puede manejar. Esto puede llevar al equipo a un estado irrecuperable de los datos.
- ✓ Cookies: Las *cookies* son una parte fundamental de la navegación actual en Internet. Sin embargo, almacenan información sensible (como nombres de usuario y contraseñas), que pueden ser la base de un ataque informático.
- ✓ Denegación de Servicio: Conocido como *Denial of Service (DoS)* en inglés, corresponde a un ataque que busca colapsar la conectividad o ancho de banda de una red, evitando que otros usuarios tengan acceso a dicho recurso.
- ✓ Registro de pulsaciones: Un ataque del tipo *key logger* almacena las teclas que presiona un usuario, permitiéndole al atacante obtener contraseñas u otra información sensible.
- ✓ Malware: su definición consiste en,

> El concepto de malware, hace alusión a cualquier tipo de software malicioso que trata de infectar un sistema informático (ordenador) o un dispositivo móvil (smartphone). La finalidad del malware, es sustraer dinero del usuario ilegalmente. Para llevar a cabo esta tarea, el malware puede robar, cifrar o borrar datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en este sin el conocimiento o permiso del usuario. Sánchez, J. F. E. (2019).

2.2.4 Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)

Esta organización corresponde al ente rector del sector de ciencia, innovación, tecnología, telecomunicaciones y gobernanza digital del Gobierno de la República de Costa Rica. De acuerdo a su sitio web, su misión consiste en "generar e impulsar el cumplimiento de las políticas públicas en materia de ciencia, innovación, tecnología y telecomunicaciones del país mediante el ejercicio de la rectoría sectorial y la ejecución efectiva de sus procesos sustantivos y de gestión, para mejorar la competitividad en beneficio del bienestar social, la igualdad y la prosperidad de la sociedad costarricense en el marco de la transformación digital y la cuarta revolución." (¿Qué es MICITT?, s. f.).

De esta forma, esta entidad recalca la importancia de la ciberseguridad en la actualidad debido al creciente papel que la tecnología y el internet desempeñan en todos los aspectos de nuestras vidas, tanto a nivel personal como empresarial y gubernamental. Entre las razones más importantes para destacar la necesidad de mantener los sistemas con información de datos seguros se encuentran los siguientes:

- ✓ Protección de la información: La ciberseguridad protege la información confidencial y sensible, como datos personales, datos financieros, información comercial y gubernamental. Un

ciberataque exitoso puede llevar al robo o la divulgación no autorizada de datos, lo que puede tener graves consecuencias económicas y de privacidad.

- ✓ Seguridad financiera: La ciberseguridad protege las transacciones financieras en línea, evitando fraudes y estafas electrónicas. Garantiza que las transacciones y los datos financieros estén protegidos durante la navegación en internet o la realización de operaciones en línea.
- ✓ Continuidad del negocio: Para muchas organizaciones, especialmente las empresas, la ciberseguridad es esencial para garantizar la continuidad del negocio. Un ataque cibernético significativo puede interrumpir las operaciones, provocar pérdidas financieras y dañar la reputación de la empresa.
- ✓ Protección de infraestructura crítica: La ciberseguridad es crucial para proteger las infraestructuras críticas, como redes de energía, suministro de agua, sistemas de transporte y servicios de salud. Un ciberataque dirigido a estos sectores puede tener consecuencias devastadoras para la sociedad y la seguridad pública.
- ✓ Privacidad y confianza: La ciberseguridad promueve la privacidad y la confianza en el uso de la tecnología. Los usuarios deben sentirse seguros al utilizar dispositivos conectados y servicios en línea, sabiendo que sus datos están protegidos.
- ✓ Protección contra ciberataques: La ciberseguridad es esencial para defenderse de ciberataques cada vez más sofisticados y persistentes. Los atacantes emplean diversas técnicas, como ransomware, phishing, malware y ataques de denegación de servicio (DDoS). La ciberseguridad proporciona las herramientas y medidas necesarias para prevenir, detectar y responder a estos ataques.
- ✓ Cumplimiento legal y regulaciones: En muchos países, existen leyes y regulaciones que obligan a las organizaciones a proteger la privacidad y seguridad de los datos de sus clientes y

empleados. La ciberseguridad es esencial para cumplir con estos requisitos legales y evitar sanciones y multas.

De acuerdo con el MICITT, se está realizando una propuesta para que los sectores que tengan interés en este campo se pueden alinear a una estrategia nacional, este es un documento público con el fin de que las personas e instituciones interesadas tomen las recomendaciones que más se adapten a su infraestructura previa a oficializar el proceso, de esta forma se menciona que:

> La Estrategia Nacional de Ciberseguridad se ha construido a través de una metodología participativa, ya establecida para la elaboración de política pública y considera el involucramiento de múltiples voces y sectores, en estrecha coordinación con el Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), bajo la instrucción de la Presidencia de la República y la rectoría del MICITT. (Avanza Proceso de implementación de la Estrategia Nacional de Ciberseguridad, 2023)

De esta forma, la ciberseguridad es fundamental para proteger la información, salvaguardar los activos digitales y mantener la confianza en el uso de la tecnología. Es un desafío en constante evolución, ya que los ataques cibernéticos se vuelven más sofisticados, por lo que es esencial que las personas, empresas y gobiernos estén comprometidos a mantenerse actualizados y adoptar medidas efectivas para protegerse en el mundo digital.

2.2.5 Legislación actual y responsabilidad empresarial

El aumento en el uso de la tecnología ha dado cabida al desarrollo de legislaciones específicas para los delitos en esta materia. En el contexto nacional, es de particular importancia el Código Penal. “El código penal es un documento que reúne un conjunto de normas imperativas que regulan los comportamientos que constituyen delitos y sus penas”. (Coll Morales, Francisco, 2020).

El Código Penal de Costa Rica ha recibido incorporaciones que detallan la legislación vigente cuando de ataques informáticos se trata, de acuerdo con el articulo 236 se indica lo siguiente:

> Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios. (Sistema Costarricense de Información Jurídica, 2015).

En el presente trabajo de investigación, interesa estudiar la seguridad tecnológica en el contexto empresarial.

"Una empresa es un grupo social en el que, a través de la administración del capital y el trabajo, se producen bienes y/o servicios tendientes a la satisfacción de las necesidades de la comunidad". (Munch Galindo & García Martínez, 2017).

Dentro de las obligaciones de una corporación empresarial, se encuentra la de adherirse a los estándares internacionales que le atañen. "La estandarización es el proceso mediante el que una serie de procesos se ajustan o se adecúan a un estándar". (Coll Morales, Francisco, 2020).

En este sentido, adaptar los procesos a un modelo que se considera de referencia. Esto es de vital importancia en el campo de la seguridad informática, pues el modelo de referencia provee indicaciones que disminuyen el riesgo de sufrir un ataque cibernético.

Por su parte, algunos de los recursos típicos con los que cuenta una empresa son el tecnológico y el humano. Estos tipos de insumo son "un medio que se vale de la tecnología para cumplir con su propósito. Los recursos tecnológicos pueden ser tangibles (como una

computadora, una impresora u otra máquina) o intangibles (un sistema, una aplicación virtual)". (Pérez Porto & Merino, 2021).

En el contexto de la seguridad de la información, se define la importancia de la seguridad informática como:

> La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad. Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., & Castillo Merino, M. (2018)

Seguidamente, se tiene el recurso humano de la empresa. Los colaboradores juegan un papel importante en la seguridad de cada compañía, por lo que es necesario fomentar una cultura de ciberseguridad. Esta cultura, se encuentra de la siguiente manera:

> "Contextualizada con el comportamiento de los humanos en un contexto organizacional para proteger información procesada por la empresa, através del cumplimiento con los reglamentos de la seguridad de la información y un entendimiento de cómo implementar requerimientos de una manera cautelosa y atenta, embebida a través de comunicación regular, consciencia, e iniciativas de capacitación y educación."(Alshaikh, M, 2020, pág.4).

La vulnerabilidad humana se puede explotar de diversas formas, siendo el phishing y la ingeniería social dos de las más conocidas en el mundo digital. La ingeniería social es la práctica de engañar a una persona, de manera presencial, por teléfono o en línea, para que realicen algo

que los deja vulnerables ante ataques futuros. En el mundo digital, resulta más fácil engañar a las personas para que sean objeto de trampas en línea que hacerlo en la vida real, logrando convertir a la ingeniería social en una práctica peligrosa y prevalente. (Acronis.Cyber Protect Cloud, 2021).

Esta práctica, en diversas ocasiones, se realiza para obtener información que pueda facilitar el éxito de un ataque de phishing. El phishing es una técnica de engaño que utilizan los piratas informáticos para robar nuestros datos personales y bancarios a través de la página web falsa de alguna institución oficial como la Agencia Tributaria, nuestro banco o cualquier empresa o tienda que consideraríamos de total confianza. (Malwarebytes, 2021).

Ante un presente repleto de amenazas, es crucial velar por el cumplimiento de las buenas prácticas en ciberseguridad por parte del personal de la empresa. Algunas de estas mejores prácticas se fundamentan en respetar la confidencialidad de la información. De acuerdo con Sangaiah, A. K., Medhane, D. V., Han, T., Hossain, M. S., & Muhammad, G. (2019). “Se entiende por confidencialidad la garantía de que únicamente las personas concernientes puedan acceder a la información o datos recolectados, en la medida que sus responsabilidades para con la investigación lo requieran, y no más allá.” (p.15)

Capítulo 3: Diagnóstico del Estado Actual

3.1 Instrumentos Utilizados, Muestra, Variables

A continuación se presentan las herramientas utilizadas para la recopilación de datos en una investigación, así como la referencia al grupo de individuos que fueron seleccionados para ser parte del trabajo y por último, se definen las características que se estudian en la investigación por medio de las variables.

De acuerdo con Torres, M., Salazar, F. G., & Paz, K. (2019), las fuentes de información se definen como "todos aquellos medios de los cuales procede la información, que satisfacen las necesidades de conocimiento de una situación o problema presentado, que posteriormente será utilizado para lograr objetivos esperados." (p. 3). De esta forma, se presentan los instrumentos utilizados para la recolección de los datos utilizados en la investigación.

3.1.1 Instrumentos utilizados

Los datos son un pilar fundamental de cualquier investigación. Con ellos, se puede conocer el estado actual del problema a estudiar, establecer conclusiones y, en algunos casos, realizar predicciones sobre el futuro del contexto estudiado. La presente investigación utiliza datos como insumo principal para realizar el trabajo investigativo y hallar conclusiones que puedan beneficiar a la empresa en el escenario descrito. Al proveer el plan de implementación de mejoras, se espera que las recomendaciones allí planteadas fortalezcan la seguridad de la información de los datos de la empresa, de igual forma al capital humano que aquí labora.

Para estudiar la infraestructura tecnológica a nivel de empresa, se llevará a cabo una entrevista al personal a cargo de la administración de la red de la empresa con el fin de identificar vulnerabilidades de la infraestructura actual contra estándares de la industria encontrados en la norma ISO 27001. Una entrevista implica coordinar una sesión con el

administrador de la red y realizar la recolección de datos en el lugar propio donde se encuentra el objeto de estudio; en este caso, la empresa Sonda.

Se eligió este instrumento para recabar información directamente de una persona experta en el tema quien está en contacto diariamente con los dispositivos en estudio que forman parte de la infraestructura tecnológica. Gracias a esta herramienta de recolección de datos, se permite una comprensión más profunda y detallada sobre el tema en investigación. Además, al interactuar directamente con los participantes, es posible obtener información abundante en detalles, perspectivas y experiencias que no serían capturadas fácilmente mediante otros métodos de recolección de datos

Por su parte, para el análisis de las prácticas de ciberseguridad en los colaboradores, se les facilitará una encuesta con base en un cuestionario. Una encuesta contiene una serie de preguntas relacionadas con alguna materia en particular; en este caso, ciberseguridad. La encuesta se elaborará según el conocimiento técnico de la persona investigadora, aunado a estándares de la industria que se recomiendan en la seguridad informática, determinados a partir de una revisión de literatura.

Se eligió una encuesta como instrumento de investigación debido a la facilidad que ofrece para recolectar una cantidad significativa de respuestas. De acuerdo con Torres, M., Salazar, F. G., & Paz, K. (2019),

> Constituye el término medio entre la observación y la experimentación. En ella se pueden registrar situaciones que pueden ser observadas y en ausencia de poder recrear un experimento se cuestiona a la persona participante sobre ello. Por ello, se dice que la encuesta es un método descriptivo con el que se pueden detectar ideas, necesidades, preferencias, hábitos de uso, etc. (p.4).

Además, debido al interés en conocer el nivel de proficiencia en ciberseguridad de los colaboradores, la encuesta emerge como un vehículo para evaluar dicha capacidad, preguntando directamente a las personas encuestadas sobre el tema. Con los instrumentos seleccionados, se pretende obtener una visión holística del problema a tratar. Combinando la entrevista al personal experto en telecomunicaciones, con la voz propia de los colaboradores, hecha manifiesta mediante la encuesta, se tendrán insumos suficientes para llevar a cabo la presente investigación.

3.1.2 Población y muestreo

Las estadísticas no tienen sentido por sí solas, es necesario relacionarlas o considerarlas dentro del contexto que se va a estudiar, de ahí la importancia de comprender la definición de población y muestra. Los sujetos son las personas objeto de estudio, “ (Barrantes, 2005, pág. 135).

De esta forma, en este trabajo de investigación se establece la unidad de análisis delimitando la población al personal de la empresa Sonda Costa Rica. En la presente investigación, la población a estudiar corresponde a una muestra del total del personal de la empresa seleccionada, es decir, 27 personas. De acuerdo con Montgomery (2019), se define población como “Una población se define como una colección cualquiera, finita o infinita, de unidades u objetos individuales.” (p. 758).

Para el análisis de la muestra, es necesario definir si es probabilística o no probabilística, la diferencia entre ambas radica en que en las muestras probabilísticas todos los elementos de la población tienen posibilidad de salir en el estudio, es decir, no depende de ningún factor externo; “para una muestra probabilística se necesita conocer dos aspectos fundamentales: el tamaño de la muestra y la forma de seleccionar los elementos que la confirmarán”. (Barrantes, 2005, pág. 136).

Adicionalmente a esto, la muestra representa un subconjunto de la población en la que se llevará a cabo la investigación. De esta forma, se elige probabilísticamente, al personal de la compañía para dicho estudio, según Navid, “los métodos estadísticos se basan en la idea de analizar una muestra elegida a partir de una población. Para que esta idea funcione, se debe elegir el tipo de muestreo de manera apropiada, así como las unidades de muestreo u observación (p.3).

De esta manera, en el marco muestral para esta investigación, las unidades o elementos que facilitan la selección aleatoria de la muestra son las personas colaboradoras de la empresa pertenecientes a todos los departamentos sin distinción. La unidad de observación será la misma que posee el marco muestral pues se trabaja con las personas como elemento sobre el cual se realiza la medición. En cuanto tipo de muestreo, un muestreo irrestricto aleatorio para Navidi (2020) “Un muestreo irrestricto aleatorio ocurre cuando la muestra es elegida por un método en el cual cada colección de elementos en la población tiene la misma probabilidad de ser elegida.” (p.3).

Una vez definidos los parámetros anteriores, siendo un nivel de confianza 90% aceptable para este estudio y con un margen de error del 10%, se selecciona un tamaño de la muestra de 27 colaboradores, estos se seleccionan de manera aleatoria para formar parte de la investigación.

3.1.3 Variables

A continuación, se mostrará el cuadro operativo de variables definidas por objetivos, con sus respectivas características de conceptualización, operalización, instrumentalización, alcances y limitaciones.

Tabla 1

Variables

Problemas específicos	Objetivos específicos	Variables	Conceptualización	Operalización	Instrumentalización	Alcances	Limitaciones
¿Cómo conocer las vulnerabilidades tecnológicas que tiene Sonda Costa Rica respecto al estándar ISO 27001?	Identificar el nivel de cumplimiento de la empresa Sonda con respecto a la norma ISO 27001, mediante una evaluación informática que considere las prácticas de seguridad aplicadas en la actualidad.	Variable independiente: nivel de cumplimiento de la empresa Sonda con respecto a la norma ISO 27001. Variable interviniente: evaluación informática Variable dependiente: prácticas de seguridad aplicadas en la actualidad	Identificar el nivel de cumplimiento de la empresa Sonda en temas de ISO 27001.	Método analítico	Análisis de complimiento de las prácticas de la empresa con lo dictado en la norma ISO 27001.	Se limita el estudio a la información de las configuraciones que proveen los equipos instalados en la empresa Sonda Costa Rica.	Los procesos relacionados a desarrollo de software no serán considerados para realizar la evaluación de ciberseguridad en SONDA.

Problemas específicos	Objetivos específicos	Variables	Conceptualización	Operalización	Instrumentalización	Alcances	Limitaciones
¿Cómo diagnosticar vulnerabilidades tecnológicas y categorizar su riesgo, dentro de Sonda Costa Rica?	Analizar los riesgos informáticos, de infraestructura y personal, identificando la severidad de cada vulnerabilidad encontrada.	Variable independiente: riesgos informáticos, de infraestructura y personal Variable interviniente: severidad de cada vulnerabilidad encontrada.	Diagnosticar vulnerabilidades tecnológicas en la empresa.	Método comparativo.	Identificación de amenazas y vulnerabilidades.	Se limita el estudio a la información de las configuraciones que proveen los equipos instalados en la empresa Sonda Costa Rica.	No se evaluará el cumplimiento de algún estándar de seguridad digital en específico, sino métricas recopiladas y seleccionadas según las referencias consultadas.

Problemas específicos	Objetivos específicos	Variables	Conceptualización	Operalización	Instrumentalización	Alcances	Limitaciones
¿Cómo identificar el nivel de conocimiento del personal de Sonda Costa Rica en aspectos de ciberseguridad?	Realizar una encuesta para conocer los hábitos de seguridad de la información en el personal, para determinar su nivel de experticia.	Variable independiente: conocer los hábitos de seguridad de la información en el personal Variable interviniente: una encuesta Variable dependiente: nivel de experticia	Conocer los hábitos de seguridad del personal.	Método analítico	Encuesta	Se limita a 27 personas encuestadas por medio de correo electrónico institucional, en un máximo de un mes a partir del año 2023 para analizar las prácticas en materia de ciber seguridad y terminará cuando se haya encuestado el 100% de la muestra.	No se solicitará información sensible ni confidencial sobre los clientes u otros actores relacionados a SONDA.

Problemas específicos	Objetivos específicos	Variables	Conceptualización	Operalización	Instrumentalización	Alcances	Limitaciones
¿Qué herramienta debe utilizar el personal de Sonda para minimizar el impacto de un ataque cibernético?	Elaborar un plan de acción que considere los lineamientos establecidos en el documento ISO 27001 y los hallazgos de la encuesta.	Variable independiente: plan de acción Variable interviniente: lineamientos establecidos en el documento ISO 27001 y los hallazgos de la encuesta.	Realizar un plan de acción con lineamientos y hallazgos.	Método deductivo.	Confección de plan de un plan de acuerdo a los hallazgos.	Se limita el estudio a unas recomendaciones de mejores prácticas y no a cambios a nivel de reglamentos internos.	No se realizarán cambios a nivel de políticas ni reglamentos de la empresa Sonda.

Fuente: elaboración propia (2023).

3.2 Enfoque de la Investigación

La ciberseguridad se ha convertido en un aspecto crítico en el mundo empresarial actual, donde la dependencia de la tecnología y la digitalización de los procesos han aumentado exponencialmente. La creciente sofisticación de los ciberataques y la constante evolución de las amenazas cibernéticas han resaltado la necesidad urgente de garantizar la protección integral de los sistemas, datos y activos de las empresas. En este contexto, este trabajo se centra en llevar a cabo un análisis de la ciberseguridad de la empresa Sonda Costa Rica, explorando su estado actual, vulnerabilidades potenciales y estrategias de mitigación.

De esta forma, el enfoque de la investigación debe centrarse en la definición de un paradigma específico, para de Franco, M. F., & Solórzano, J. L. V. (2020) “el paradigma se define como un modelo, sistema de convicción, creencias que posee el investigador en relación al componente ontológico, axiológico, epistemológico y metodológico, lo cual conlleva a la búsqueda del camino o vía de acceso a la generación de conocimiento científico.” (pág. 6).

De esta manera, el paradigma delimita un margen que indica cómo recolectar y razonar los datos recolectados, relativos a un fenómeno de interés que, a su vez, se encuentra inscrito en un grupo o escenario relevante para el trabajo. Es importante mencionar que esta investigación puede utilizar diferentes enfoques a la vez, los cuales no son excluyentes unos de otros.

La presente investigación tomará un enfoque naturalista, el cual “busca conocimiento medible, sistemático y comprobable. Además, su objeto de estudio consiste únicamente en fenómenos observables, pues busca encontrar las causas que responden a dichos fenómenos mediante la generalización de los datos observados”. (Pérez Porto & Merino, 2021)

Se eligió de esta forma debido a la observabilidad intrínseca de la tecnología, que permite estudiar fenómenos observables, pues busca encontrar las causas de los procesos digitales que interesen.

Al seguir este paradigma, el conocimiento emerge naturalmente a partir de la generalización realizada por la persona investigadora sobre los insumos obtenidos. En este caso, el conocimiento surge a partir de la interpretación de las encuestas y el estudio de campo realizado, siempre combinado con el conocimiento y juicio técnico adquirido previamente.

El enfoque de la investigación determina la dirección que tomará la obra investigativa. Si bien algunos escritos tienen una fuerte inclinación hacia los números y datos crudos, otros se apoyan con mayor fuerza en las interpretaciones de la discusión teórica actual. Definir el enfoque es vital para conocer hacia dónde debe dirigir su esfuerzo la persona investigadora, así como los insumos que debe conseguir para llevar a cabo su labor de investigación.

La presente investigación seguirá un enfoque mixto, ya que combina tanto métodos cuantitativos como cualitativos, de esta forma se pretende obtener una visión completa y profunda del tema en estudio. Primeramente, se tomará, como punto de partida, la encuesta como instrumento de recolección de datos enfocado en el método cuantitativo, pues ofrece cifras comparables y explícitas sobre el conocimiento en ciberseguridad del personal entrevistado, así como el cumplimiento a nivel de empresa de los estándares técnicos elegidos. “El enfoque cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos “brincar” o eludir pasos”. (Hernández Sampieri, Fernández, & Baptista Lucio, 2018, pág. 5). Luego, se realizará una interpretación de los resultados obtenidos, ofreciendo así mayor profundidad en el análisis ejecutado.

Seguidamente, basado en el enfoque cualitativo, se realizará una entrevista al personal encargado del área de redes de la empresa Sonda con el fin de recabar información relevante para la investigación y obtener datos importantes sobre la infraestructura instalada en la compañía. “La acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien “circular” en el que la secuencia no siempre es la misma, pues varía con cada estudio.” (Hernández Sampieri, Fernández, & Baptista Lucio, 2018, pág. 7)

Este enfoque se ajusta a los proyectos investigativos relacionados a la tecnología, pues existen diversas unidades numéricas que se utilizan en el campo. Términos técnicos como latencia, transferencia efectiva o bits son comunes en la informática, y pueden ser fácilmente estudiados con métodos cuantitativos. La investigación mixta es especialmente útil cuando se abordan preguntas de investigación complejas o cuando se desea obtener una visión holística de un fenómeno.

> En el Enfoque Mixto, dada la naturaleza del problema, se podría concebir un estudio de carácter híbrido. El investigador se podría aproximar al problema, por medio de ambas rutas. Por una parte, el enfoque cuantitativo permite asignar valores numéricos para analizar datos a través de la estadística, verificación de hipótesis y poder incluso generalizar resultados (si la muestra es representativa). Sin embargo, en muchos casos se requiere profundizar e interpretar el fenómeno, y es allí cuando se complementa con la ruta Cualitativa. (Padilla-Avalos, C. A., & Marroquín-Soto, C, 2021, pág. 338).

Al combinar la riqueza de los datos cualitativos (que se enfocan en la comprensión en profundidad y el contexto) con la objetividad y generalización de los datos cuantitativos, los investigadores pueden obtener una perspectiva más completa y sólida de sus investigaciones.

3.3 Tipos de Investigación

La investigación, en cualquier ámbito, permite resolver problemas precisos y prácticos sobre cualquier acontecimiento social o histórico. Además, aporta un criterio propio con fundamentación científica. De esta manera, se pretende que, por medio de la investigación, se den soluciones a problemas reales apoyándose en la ciencia.

Las personas que realizan una investigación logran alcanzar no solamente sus objetivos propuestos, sino también entender de una mejor forma el proyecto en el que se encuentran involucrados. De acuerdo con Bardales, J. M. D. (2021), “La investigación científica en los diferentes campos de las ciencias, es un pilar fundamental porque contribuye a la calidad de vida y bienestar de las personas, en la formación de nuevos profesionales y en el desarrollo de los profesionales que se encaminan hacia la investigación.”(p.234).

Al ser el presente un trabajo de investigación de tipo aplicada utiliza información obtenida de los colaboradores de la empresa Sonda que se encuentran desempeñando sus funciones en los departamentos de administración, servicios, ventas y monitoreo. De esta forma, se partirá de conocimientos técnicos previos para evaluar el estado de la ciberseguridad en la empresa seleccionada. Con esto, se pretende encontrar puntos de mejora, para así enumerar y entregar recomendaciones a la compañía y sus colaboradores, con el fin de asegurar controles más robustos en la materia. Según Bardales, J. M. D. (2021), “La investigación aplicada ha de ser aquella que aporte soluciones a los individuos directamente relacionados con ella” (pág. 236).

De igual forma, el trabajo será de tipo descriptivo, donde las variables no serán manipuladas, se observan tal cual están en su ambiente natural valiéndose de datos cuantitativos y cualitativos.

> Los diseños transaccionales descriptivos tienen como objetivo indagar la incidencia y los valores en que se manifiestan una o más variables (dentro del enfoque cuantitativo) o ubicar, categorizar y proporcionar una visión de una comunidad, un evento, un contexto, un fenómeno o una situación (describirla, como su nombre lo indica, dentro del enfoque cualitativo). (Hernández Sampieri, Fernández, & Baptista Lucio, 2018, pág. 218)

Siendo esta investigación enfocada al tipo mixto, su diseño será de tipo explicativo, basado en el apoyo de datos cualitativos para ampliar los resultados de los datos cuantitativos. Encargándose de puntualizar las características de la población en estudio, en este caso, el personal de la empresa Sonda Costa Rica. De acuerdo con Navidi (2020), el objetivo de este tipo de investigación se puede enfocar de la siguiente manera "La investigación mixta tiene como fin último la descripción y representación conceptual de los fenómenos en su estado natural, sin ahondar en relaciones de causalidad, correlación u otros tipos de asociación que expliquen dicho comportamiento." (pág. 56). De esta manera, se busca describir, con este enfoque, las relaciones del objeto de estudio con otros objetos o asociaciones entre las variables definidas.

En cuanto a los métodos de investigación, hacen referencia al conjunto de herramientas y estrategias utilizadas con el fin de llegar a un objetivo concreto. El método analítico es uno de los que se va a utilizar en esta investigación, de esta manera, se hará una descomposición de todos los elementos básicos que conlleva la ciberseguridad a lo interno de una empresa, se observarán las prácticas que mantienen los colaboradores de la compañía y se analizarán sus efectos, obteniendo así resultados precisos para realizar recomendaciones de mejora en las prácticas. El método analítico según Navidi (2020) se define como "El método analítico se basa, fundamentalmente, en la consideración y estudio individual de cada sección particular de un

sistema, para explicar el fenómeno en cuestión como un todo a partir de sus elementos más básicos.” (pág.27).

Otro método que será utilizado en esta investigación es el método deductivo, siendo este un procedimiento de investigación que usa un tipo de pensamiento más allá de la razón general y la lógica convencional, todo esto basado en un hecho concreto o en leyes y principios, de esta manera sirve para obtener conclusiones a partir de estos hechos.

> Las investigaciones cuantitativas, cuyo método es el deductivo sí formulan hipótesis, siempre y cuando se defina desde el inicio que su alcance será correlacional o explicativo, o en caso de un estudio descriptivo, que intente pronosticar una cifra o un hecho. (Hernández Sampieri, Fernández, & Baptista Lucio, 2018, pág. 111)

De esta forma, se planea obtener las recomendaciones en cuanto a la ciberseguridad para la empresa Sonda Costa Rica.

3.4 Fuentes de Información

Para lograr obtener todos los insumos necesarios que permitan llevar a cabo esta propuesta metodológica para el análisis de las prácticas en materia de ciberseguridad es necesario definir las variables sobre las cuales se va a trabajar. Se denomina variable a todo aquello que posee características propias, con esto pueden distinguirse de lo demás, también es posible controlarla, medirla o estudiarla en una investigación. De acuerdo con Montgomery (2019), "Una variable corresponde a una función que relaciona un número, discreto o real, con la magnitud de la característica estudiada en el objeto de análisis." (pág.58).

De acuerdo con la Tabla 1. Variables, presentada anteriormente, podemos definir las variables para esta investigación de la siguiente manera, para el primer objetivo específico que es "determinar las áreas más vulnerables en el campo de la ciberseguridad en Sonda Costa Rica, a través de una revisión de la infraestructura tecnológica instalada, identificando las mejores prácticas recomendadas en los estándares informáticos." La variable independiente son las áreas más vulnerables en el campo de la ciberseguridad, la variable interviniente es la revisión de la infraestructura tecnológica instalada, mientras que la variable dependiente son las mejores prácticas recomendadas en los estándares informáticos.

Seguidamente, según la definición de las variables presentadas en la tabla 1 de esta investigación, para el segundo objetivo específico, el cual corresponde a "diagnosticar las posibles causas de un ataque de ciberseguridad, mediante el análisis de las prácticas de seguridad de la información del personal, estableciendo las variables existentes en relación con la práctica y la teoría." La variable independiente consiste en las posibles causas de un ataque de ciberseguridad, por otro lado, la variable interviniente es el análisis de las prácticas de seguridad

de la información del personal, mientras que las variables dependientes son las variables existentes en relación con la práctica y la teoría.

Por último, de acuerdo con la tabla 1. Variables, para el tercer objetivo específico que corresponde a “establecer recomendaciones que permitan mejorar los hábitos de la seguridad de la información, mediante el análisis de los lineamientos en materia de aseguramiento de la información, desarrollando una propuesta de ejecución.” La variable independiente consiste en las recomendaciones que permitan mejorar los hábitos de la seguridad de la información. Por otro lado, la variable interviniente es el análisis de los lineamientos en materia de aseguramiento de la información y la variable dependiente es el desarrollo de una propuesta de ejecución.

Una vez identificadas las variables por objetivos, es posible iniciar con la elaboración de los instrumentos de medición con el fin de recolectar los datos necesarios para el análisis de la información recabada por persona en temas de ciberseguridad para la empresa Sonda Costa Rica

3.5 Análisis de Resultados

En la siguiente sección se presenta el análisis de los resultados obtenidos por medio de las distintas herramientas de recolección de datos implementadas durante el trabajo de investigación, las mismas fueron aplicadas en la empresa Sonda, durante el segundo cuatrimestre del año 2023.

3.5.1 Entrevista

A continuación, se muestran los resultados de la entrevista aplicada al responsable de la seguridad de la red en la empresa Sonda, esta persona es encargada de la administración, configuración y mantenimiento de los equipos de telecomunicaciones que se encuentran instalados en la empresa, cuenta con varios años de experiencia en el ámbito de la tecnología y mantiene actualizado su conocimiento en materia de seguridad de la información con capacitación constante que ha obtenido por cuenta propia. Como datos adicionales, labora para Sonda desde hace más de 5 años, conoce a cabalidad la red que aquí se encuentra, la entrevista se aplicó el día 7 de julio de 2023, en las oficinas de Sonda, a las 4:30p. m.

1. En cuanto a la seguridad de la red en la empresa, ¿Hay una configuración segura de los equipos para proteger la infraestructura de comunicaciones contra amenazas y vulnerabilidades?

   En cuanto a firewalls, existen reglas de filtrado de paquetes para permitir solamente el tráfico necesario y bloquear el tráfico no autorizado.

   Existen conexiones VPN para permitir el acceso remoto de los usuarios que realizan teletrabajo y puedan acceder a la red interna.

2. ¿Cuáles políticas de seguridad se aplican dentro de la empresa?

Se aplican políticas de usuarios y contraseñas de dominio, las cuales deben tener una cierta cantidad de caracteres y un cambio periódico.

Políticas de seguridad en las redes inalámbricas, principalmente con los usuarios que son visitantes de la empresa.

3. ¿Qué mecanismos utiliza la empresa para proteger la información en tránsito?

   Se utilizan mecanismos como túneles VPN para conexiones remotas y autenticación de dos factores con el objetivo de validar la identidad de los usuarios que están accediendo a la información en tránsito.

4. ¿Podría mencionar algunos de los protocolos seguros que utilizan en la empresa?

   Se utilizan protocolos seguros como IPsec, a través de las conexiones VPN y SSH para realizar conexiones a los equipos de comunicaciones de manera remota dentro de la red interna.

   También se utiliza el protocolo SFTP para transferencia de archivos en caso de requerirlo en los equipos de comunicaciones.

5. ¿Cómo se gestionan los accesos remotos dentro de la empresa?

   Los accesos remotos se gestionan por medio de conexiones VPN que se administran en un equipo de seguridad marca Cisco, modelo ASA.

6. Podría indicarnos, ¿qué tipo de prácticas utilizan para la autenticación y control de accesos?

   Entre las prácticas de autenticación están las contraseñas seguras, los usuarios deben establecer ciertos requisitos en sus contraseñas y la autenticación de doble factor de

identidad, donde se registra un número de teléfono y por medio de un mensaje de texto se envía un código de autorización para validar el acceso remoto.

7. En cuanto a la gestión de incidentes de seguridad ¿cómo los detecta la empresa?

   En este momento la empresa no cuenta con un sistema de detección de incidentes de seguridad.

8. ¿Podría mencionar algunos de esos procedimientos para la gestión de incidentes?

   En este momento la empresa no cuenta con un sistema de detección de incidentes de seguridad.

9. ¿Cuentan ustedes con estadísticas sobre accidentes, ataques, tiempos de respuesta a estos incidentes, entre otros?

   La empresa no cuenta con ningún sistema sobre accidentes o ataques a incidentes en este momento.

10. Finalmente, ¿qué opina de la actualización y parcheo de equipos de comunicaciones?

    Me parece una tarea importante que debe implementarse ya que esto depura la red sobre nuevas vulnerabilidades que encuentran los fabricantes, es una tarea que lleva tiempo y planificación ya que se recomienda se realice fuera de horario laboral, en caso de fallo es importante que los equipos cuenten con un contrato activo con el fabricante, en este caso, la mayoría de los equipos se encuentran obsoletos y fuera de contrato.

3.6 Principales Hallazgos

Los hallazgos obtenidos durante un trabajo investigativo son fundamentales porque brindan la posibilidad de dar a conocer nuevos conocimientos y constituyen el punto de partida para emitir un criterio, recomendar acciones correctivas u optimizar lo que ya existe.

En este apartado se presentan los principales hallazgos del trabajo de investigación, los cuales representan los resultados más significativos y relevantes obtenidos a lo largo del estudio. Durante el proceso de investigación, se han recopilado datos, analizado información y aplicado metodologías específicas para responder a cada una de las preguntas de investigación. Estos hallazgos proporcionan una visión profunda y detallada sobre el tema estudiado, y permiten responder a los objetivos planteados inicialmente.

3.6.1 Encuesta

Para analizar los resultados de la encuesta, se utilizarán gráficos circulares que muestran la proporción de cada respuesta en las preguntas aplicadas. Esta información será el sustento para discutir los principales hallazgos en la siguiente sección. El instrumento de medición fue aplicado a 27 personas colaboradoras de la empresa Sonda de diferentes departamentos para obtener una visión más amplia de los temas planteados en el cuestionario.

La encuesta fue aplicada del 3 al 10 de julio de 2023, esta fue enviada por correo electrónico al personal de la empresa, una vez obtenidas las 27 respuestas, se dio por concluido el proceso de recolección de datos con esa herramienta, esta se encuentra en el Anexo 1. “Instrumento de recolección de datos, encuesta”.

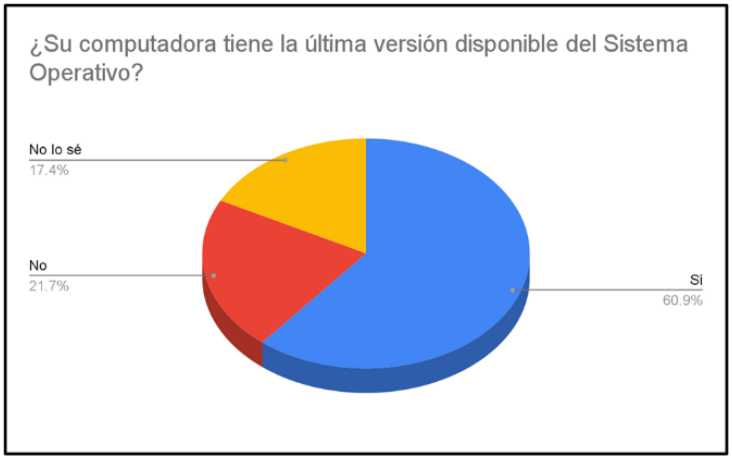
3.6.1.1 Conocimiento del personal sobre versión del sistema operativo disponible

Como se muestra en la Figura 2, más de la mitad del personal cuenta con la última versión del sistema operativo. Esto es de suma importancia, pues contar con las actualizaciones

más recientes previene ataques al sistema informático, que se aprovechan de fallas ya conocidas en versiones anteriores.

Figura 2

Personal según Versión Disponible del Sistema Operativo



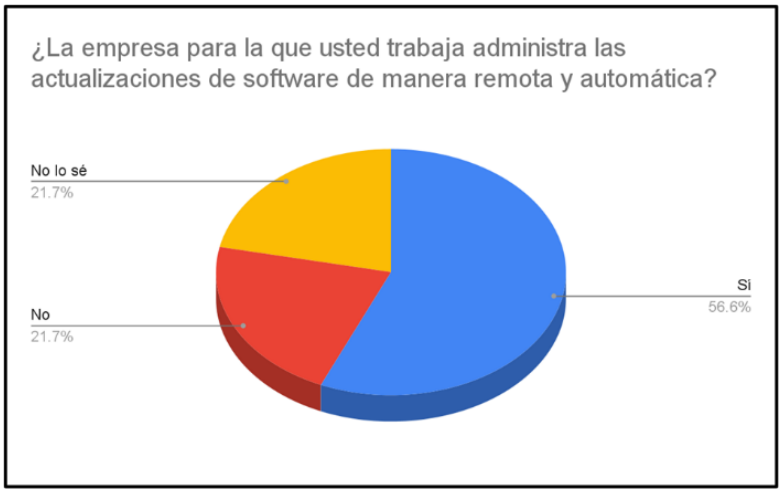
Nota. Datos obtenidos a partir de la encuesta

3.6.1.2 Conocimiento del personal sobre actualizaciones de software

De manera similar, en la Figura 3, se observa una diversidad de respuestas importante. Cerca de la quinta parte de los encuestados desconoce si las actualizaciones de software se realizan automáticamente, lo que supone una deficiencia clara en materia de capacitación al personal. se rescata el 56.6% que afirmó la actualización automática de software, actividad que fortalece la ciberseguridad.

Figura 3

Personal según Conocimiento de Actualizaciones de Software



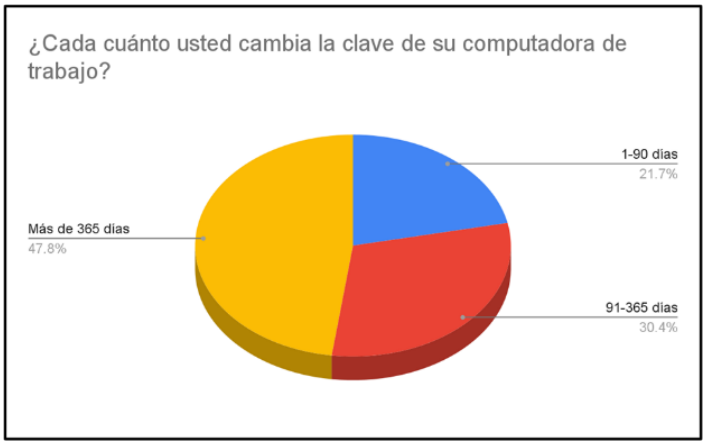
Nota. Datos obtenidos a partir de la encuesta

3.6.1.3 Información sobre cambio de contraseña

Según la Figura 4, casi la mitad del personal mantiene la misma contraseña por períodos mayores a un año. Lamentablemente, tan solo el 21.7% la cambia cada menos de 3 meses, el cual es el plazo recomendado para realizar cambios de este tipo. La adopción de medidas a nivel empresarial puede obligar a disminuir el tiempo entre actualizaciones de contraseña, práctica básica en la seguridad informática.

Figura 4

Personal según Periodicidad en Cambio de Contraseña



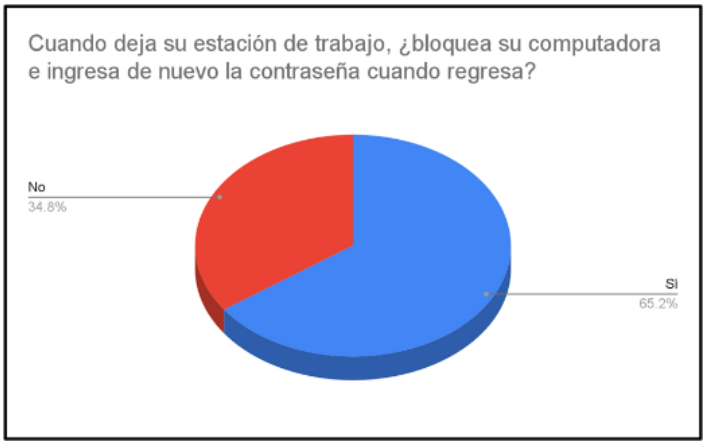
Nota. Datos obtenidos a partir de la encuesta

3.6.1.4 Información sobre bloqueo de la computadora

Como muestra la Figura 5, la mayoría del personal bloquea la computadora cuando la deja desatendida, pero el 34.8% no sigue esta práctica. Desafortunadamente, este rubro no se puede garantizar con medidas empresariales, por lo que se debe concientizar al personal sobre la importancia de bloquear los dispositivos tecnológicos cuando no se está cerca de ellos.

Figura 5

Personal según Costumbre en Bloqueo de Computadora



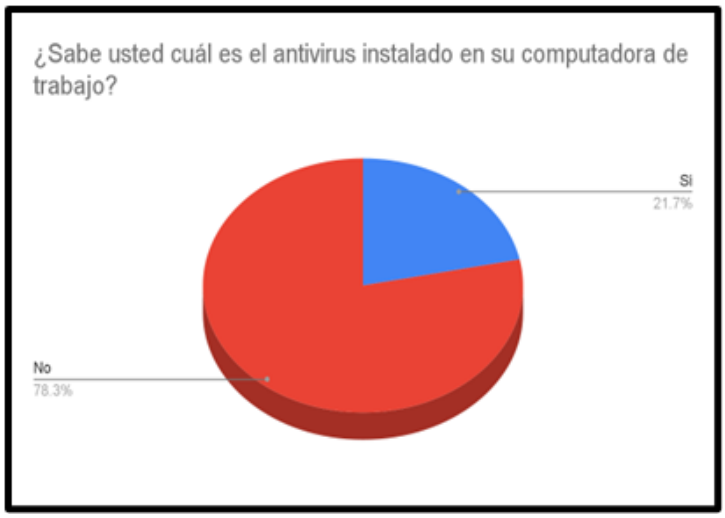
Nota. Datos obtenidos a partir de la encuesta

3.6.1.5 Conocimiento del personal sobre antivirus instalado

Con base en las Figuras 6 y 7, se observa una porción muy significativa del personal que desconoce respuestas básicas en materia de ciberseguridad. Nuevamente, es imperioso emplear recursos en fomentar las capacidades técnicas de esta población, pues son los que trabajan día a día con la tecnología de la empresa y, por consiguiente, son responsables de la robustez de su seguridad informática.

Figura 6

Personal según Conocimiento de Antivirus



Nota. Datos obtenidos a partir de la encuesta

Figura 7

Personal según Conocimiento de Información Encriptada

Nota. Datos obtenidos a partir de la encuesta

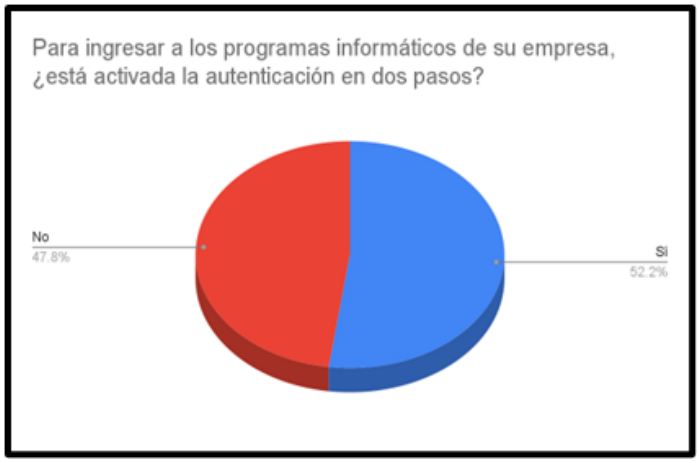
3.6.1.6 Conocimiento del personal sobre antivirus instalado

En la Figura 8, se puede apreciar una disyuntiva en el uso de autenticación de dos pasos. A partir de ella, se puede concluir que la adopción de esta práctica puede ser beneficiosa para la

empresa: por un lado, la mitad de los colaboradores están familiarizados con ella; por el otro, se protegería al 47.8% restante que no la utiliza en sus labores profesionales cotidianas.

Figura 8

Personal según Conocimiento de la Autenticación en dos Pasos



Nota. Datos obtenidos a partir de la encuesta

3.6.1.7 Información sobre capacitación en temas de ciberseguridad

De nuevo relacionado al tema de capacitación, en la Figura 9 se muestra que el 87% del personal no ha recibido entrenamiento alguno durante el último año. Probablemente, el 13% restante corresponde a un sector particular de la compañía, que se ha considerado como el más pertinente en esta materia. Sin embargo, conviene capacitar a la totalidad de los colaboradores, pues todos y cada uno de ellos son responsables de la seguridad informática.

Figura 9

Personal según Capacitación Recibida

Nota. Datos obtenidos a partir de la encuesta

3.6.1.8 Conocimiento del personal en caso de ataque cibernético

Un aspecto positivo se muestra en la Figura 10, donde casi tres cuartas partes del personal sabe a quién debe acudir en caso de un ataque informático.

Figura 10

Personal según Conocimiento sobre Qué Hacer en Caso de Ataque Informático

Nota. Datos obtenidos a partir de la encuesta

3.6.1.9 Utilización de un gestor de contraseñas

En concordancia con la Figura 11, una minoría del personal utiliza un gestor de contraseñas en su dispositivo de trabajo. Como se mostrará más adelante, una aplicación de este tipo puede mejorar grandemente la ciberseguridad de la compañía.

Figura 11

Personal según Utilización de Gestor de Contraseñas

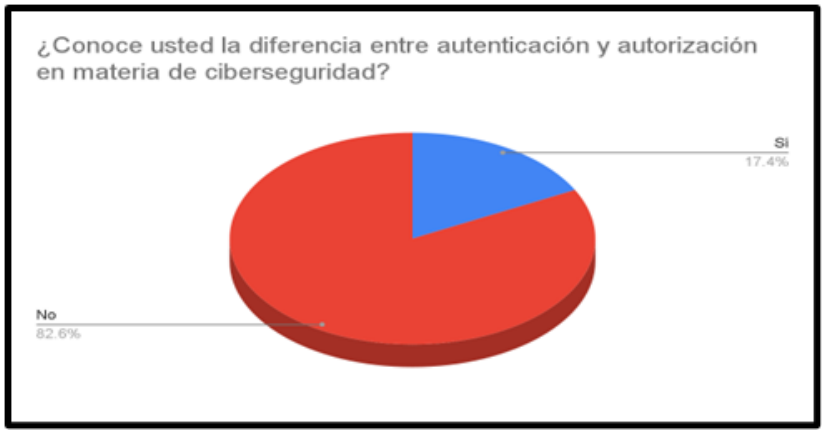
Nota. Datos obtenidos a partir de la encuesta

3.6.1.10. Conocimiento del personal sobre antivirus instalado

Retomando el tema de capacitación, la Figura 12 demuestra una falencia técnica de los encuestados, pues la gran mayoría desconoce la diferencia entre dos términos básicos de seguridad informática.

Figura 12

Personal según Conocimiento Términos Básicos de Seguridad Informática



Nota. Datos obtenidos a partir de la encuesta

3.6.1.11 Información sobre ataques informáticos

Finalmente, la Figura 13 expone un porcentaje muy alto del personal que no ha sufrido un ataque informático.

Figura 13

Personal según Incidencia de Ataque Informático

Nota. Datos obtenidos a partir de la encuesta

3.6.1.12 Responsabilidad en caso de ataque

Este porcentaje es similar al de la Figura 14, donde la mayoría del personal no se siente responsable de la seguridad informática en la empresa. Nuevamente, es necesario realizar esfuerzos que permitan al personal reconocer su papel e importancia en la lucha contra los ataques informáticos.

Figura 14

Personal según Percepción de Responsabilidad en la Seguridad Informática de la Empresa

Nota. Datos obtenidos a partir de la encuesta

3.6.2 Entrevista

A continuación, se muestra la interpretación de la entrevista aplicada:

1. En cuanto a la seguridad de la red en la empresa, ¿Hay una configuración segura de los equipos para proteger la infraestructura de comunicaciones contra amenazas y vulnerabilidades?

Si bien es cierto, se mantienen algunas prácticas comunes para la protección contra amenazas y vulnerabilidades, de acuerdo con la norma ISO 27001 se pueden aplicar algunos otros controles como, por ejemplo:

Establecer políticas claras y documentadas que definan los requisitos de seguridad para la configuración de los equipos. Estas deben ser comunicadas y entendidas por todos los miembros del personal involucrados en el manejo de los equipos.

Implementar mecanismos de autenticación robustos, como contraseñas fuertes, autenticación de múltiples factores y restricciones de acceso basadas en roles.

Mantener actualizados los sistemas operativos, aplicaciones y firmware de los equipos para incorporar las últimas correcciones de seguridad y mitigar las vulnerabilidades conocidas por los fabricantes.

Implementar soluciones de seguridad actualizadas, como antivirus y antimalware, en los equipos de comunicaciones para detectar y prevenir ataques en la red.

2. ¿Cuáles políticas de seguridad se aplican dentro de la empresa?

   En este ámbito y siendo Sonda una empresa de tecnología, es importante tener en cuenta políticas de acceso a la información, que incluya la autenticación de usuarios, la asignación de privilegios, el control de acceso físico y lógico a equipos de comunicaciones, y la gestión de contraseñas. Además de una parte fundamental que es la capacitación y concientización en seguridad de la información entre el personal de la organización. Esto incluye la formación en buenas prácticas de seguridad, la gestión de contraseñas y la protección de la información confidencial.

3. ¿Qué mecanismos utiliza la empresa para proteger la información en tránsito?

Algunos de los mecanismos para proteger la información en tránsito que se recomienda por la norma ISO 27001 que puede ser implementado en la empresa se encuentran la segmentación de redes, ya que se limita la propagación de la información en caso de un acceso no autorizado. Esto ayuda a proteger la información en tránsito al restringir su alcance a redes específicas y reducir la superficie de ataque.

También se podría implementar un sistema o software de monitoreo del tráfico de la red, como Whatsup Gold o PRTG con el fin de detectar y alertar sobre actividades sospechosas o anómalas, de esta forma también se pueden identificar intentos de intrusión o fugas de información durante la transmisión de datos.

4. ¿Podría mencionar algunos de los protocolos seguros que utilizan en la empresa?

   De acuerdo con el Grupo de Trabajo de Ingeniería de Internet (IETF), una organización encargada de promover estándares de Internet, incluyendo los protocolos de seguridad, en esta respuesta se nota un buen uso de los protocolos seguros, principalmente para el ingreso remoto de conexiones a la red interna de la empresa. ((IETF), s.f.)

5. ¿Cómo se gestionan los accesos remotos dentro de la empresa?

   Si bien es cierto, el control de los accesos remotos se mantiene a través de un equipo de seguridad robusto de marca Cisco, es importante mantener algunas recomendaciones adicionales como por ejemplo, la segmentación de usuarios por políticas de acceso, con el objetivo de que logren acceder a equipos de acuerdo a los grupos asignados, así como un sistemas de detección y prevención de intrusiones, para proteger contra amenazas y ataques cibernéticos, en este caso se recomienda la valoración de la implementación de una herramienta como Cisco ISE o similar que realice este tipo de funciones.

Además, establecer un proceso para garantizar que los dispositivos remotos se mantengan actualizados con los últimos parches y actualizaciones de seguridad. Esto reduce el riesgo de explotación de vulnerabilidades conocidas. A nivel del equipo de seguridad, una buena práctica es mantener el software de conexión remota actualizado a la última versión recomendada por el fabricante, en este caso Cisco, en el año 2022 lanzó un nuevo cliente llamado Cisco Secure Client, el cual viene a reemplazar al conocido Cisco AnyConnect, por lo cual se recomienda valorar la adaptación de este nuevo software a la versión actual del equipo Cisco ASA.

6. Podría indicarnos, ¿qué tipo de prácticas utilizan para la autenticación y control de accesos?

   Las técnicas utilizadas están dentro de las recomendaciones por la norma ISO 27001, sin embargo, como valor agregado se podría añadir una implementación de un sistema de registros de auditoría y monitoreo que registre y supervise las actividades de autenticación y acceso. Estos registros pueden ayudar a identificar actividades sospechosas o no autorizadas, y proporcionar una traza de auditoría para fines de investigación y cumplimiento.

7. En cuanto a la gestión de incidentes de seguridad ¿cómo los detecta la empresa?
   De acuerdo con la norma ISO 27001, se deben implementar medidas para detectar y gestionar los incidentes de seguridad de la información de manera efectiva, se recomienda tomar en cuenta los siguientes puntos:

   - ✓ Implementar una red de sensores de seguridad distribuidos en la infraestructura de TI para monitorear el tráfico de red y los eventos de sistemas en tiempo real. Los

sensores pueden ayudar a detectar actividad maliciosa, intrusiones y anomalías en la red.

- ✓ Estar al tanto de las amenazas y vulnerabilidades conocidas a través de la monitorización de fuentes confiables de inteligencia de amenazas y boletines de seguridad, esta tarea estaría a cargo del personal administrador de la red de la empresa.
- ✓ Contar con la capacidad de llevar a cabo análisis forenses en caso de que ocurran incidentes de seguridad. Para ello, es necesaria la recolección y preservación adecuada de evidencias digitales, el análisis de registros y el seguimiento de las acciones realizadas durante un incidente para identificar su causa y alcance, ya que muchas veces cuando ocurre un incidente y se soluciona, la documentación de este no parece relevante y se pierde trazabilidad para un futuro evento similar.

8. ¿Podría mencionar algunos de esos procedimientos para la gestión de incidentes?

   Es importante mencionar que los procedimientos para la gestión de incidentes son procesos continuos que se van adaptando a los riesgos e infraestructura de cada empresa y cliente.

   También, es importante contar con un plan de respuesta a incidentes que establezca los pasos a seguir una vez que se detecte un incidente, incluyendo la notificación, la contención, la investigación y la recuperación de este.

9. ¿Cuentan ustedes con estadísticas sobre accidentes, ataques, tiempos de respuesta a estos incidentes, entre otros?

   En este punto, de acuerdo con la norma ISO 27001, se recomienda la generación de informes periódicos sobre los incidentes de seguridad detectados, incluyendo estadísticas

y métricas relevantes. Estos informes pueden proporcionar información valiosa sobre la efectividad de las medidas de detección implementadas y ayudar a identificar áreas de mejora.

10. Finalmente, ¿qué opina de la actualización y parcheo de equipos de comunicaciones?

    El personal a cargo de la administración de la red de la empresa Sonda está consciente de la importancia y valoración de la seguridad de la información para la organización, lo cual facilita el proceso de mejora en cuanto a las debilidades encontradas. También comprenden que implementar siempre mejores prácticas basadas en estándares internacionales, ayudan a fortalecer y garantizar un entorno seguro para la empresa.

Capítulo 4: Propuesta de Cambio

4.1 Introducción a la Propuesta de Cambio

La seguridad informática es una disciplina en la cual tanto la empresa como sus colaboradores deben sentirse responsables. Ambas partes deben trabajar conjuntamente para alcanzar un sistema robusto y fiable en el mundo tecnológico. En esta sección, se presentará una propuesta de cambio, tanto a nivel de individuos como de la totalidad de la compañía, con el fin de ofrecer una ruta hacia una mejor seguridad informática.

Primeramente, se abordarán los resultados obtenidos a partir de la encuesta, instrumento que fue aplicado a una muestra de los colaboradores de Sonda Costa Rica. Se detallarán aspectos concretos y prácticos, aplicables en el contexto de la compañía y relevantes con su momento actual en el mercado tecnológico. Con esto, se robustece la primera línea de defensa cibernética de toda empresa, así como el eslabón más débil en la lista de medidas de protección: el factor humano.

Seguidamente, se utilizará la entrevista como insumo para enumerar las principales aristas en cuanto a seguridad a nivel empresarial concierne. Estas medidas, si bien no necesariamente serán advertidas por los colaboradores, aumentarán la ciberseguridad de la compañía y quienes trabajan en ella. Naturalmente, estos cambios serán de un carácter más técnico, por lo que requerirán personal especializado para poder llevarse a cabo.

Luego, se brindará un plan a seguir para incorporar los cambios expuestos, junto con sus responsables, fechas límite y resultados a evaluar. Además, se tomará en cuenta el presupuesto necesario para financiar dicho plan, con su respectivo análisis de costos y beneficios. Con estos entregables, se demostrará la concretitud y plausibilidad del plan a incorporar, para que pueda ser adoptado y ejecutado por las personas correspondientes.

Finalmente, se tomará en cuenta el criterio de expertos, quienes tienen experticia en el tema tratado, para conocer sus impresiones acerca del plan propuesto. Si bien es cierto no son las personas encargadas de llevar a cabo el proyecto, cuentan con un amplio bagaje técnico que les permite emitir juicios de valor sumamente valiosos para la investigación realizada.

4.2 Descripción del Escenario Deseado

En esta sección, se presentará el escenario deseado de la investigación, donde se explorarán las metas y objetivos que se buscan alcanzar en base a los resultados obtenidos en la encuesta y entrevista realizadas en este trabajo. Para analizar el problema expuesto, así como el plan detallado para su solución, se deben considerar las siguientes variables:

- ✓ Capacitación del personal en materia de ciberseguridad.
- ✓ Medidas empresariales para robustecer la seguridad del personal.
- ✓ Actualización de equipos de comunicaciones y sistemas operativos de los equipos que realizan especialmente conexiones remotas.
- ✓ Definir una segmentación de la red de acuerdo con los departamentos que son parte de la empresa.
- ✓ Implementar un sistema o software de monitoreo del tráfico de la red.

A continuación, se ahondará en cada una de ellas.

4.2.1 Capacitación del personal

Como se expuso en el Estado de la Cuestión y en el Marco Teórico, un sinnúmero de ataques informáticos ha ocurrido gracias al factor humano. Puesto que este es el eslabón más débil, es de vital importancia garantizar un compromiso e identificación de los colaboradores con la ciberseguridad de la empresa. Si cada persona se reconoce como responsable de la seguridad informática en su lugar de trabajo, el riesgo de sufrir las consecuencias de un ataque disminuye abruptamente.

Aunado a lo anterior, es pertinente también capacitar al personal en materia técnica, con el fin de expandir sus conocimientos relacionados al tema de ciberseguridad. Si no existe una

familiaridad con los términos tecnológicos, o si la capacidad de respuesta técnica es débil, la seguridad informática de la empresa, y sus colaboradores, estará en riesgo.

4.2.2 Medidas empresariales para robustecer la seguridad del personal

A nivel empresarial, se pueden gestionar medidas que aumenten la seguridad del personal. Por ejemplo, realizar actualizaciones automáticas y periódicas de sistemas operativos, utilizar autenticación en dos pasos para ingresar a las aplicaciones de la compañía, emplear gestores de contraseña para todo el personal, entre otros. Estas precauciones de carácter obligatorio incrementan significativamente la robustez de la seguridad en la empresa.

4.2.3 Actualización de equipos de comunicaciones y sistemas operativos de los equipos que realizan especialmente conexiones remotas.

La actualización de equipos de comunicaciones es de gran importancia según la norma ISO 27001 y las mejores prácticas de seguridad de la información en general debido a que los fabricantes lanzan parches que protegen de vulnerabilidades conocidas y ayudan a mejorar la protección de los dispositivos. De igual forma, ayuda a mitigar el riesgo de explotación de vulnerabilidades y minimiza las posibilidades de sufrir ataques cibernéticos.

Los equipos de comunicaciones desactualizados representan un riesgo significativo para la seguridad de la información de las empresas y las vulnerabilidades no corregidas pueden ser explotadas por atacantes, quienes evolucionan constantemente.

4.2.4 Definir una segmentación de la red de acuerdo con los departamentos que son parte de la empresa.

De acuerdo con lo indicado por la norma ISO 27001 se sugiere que las organizaciones deben identificar y definir dominios de seguridad en su infraestructura de red, en este caso, lo ideal es que la red de la empresa se divida subredes que agrupen sistemas y recursos similares y

tengan políticas de seguridad comunes, de esta forma, al dividirse en segmentos más pequeños, se reduce la exposición de los sistemas y la exposición de la información. De igual forma, si un segmento de red se ve comprometido, la segmentación ayuda a limitar el impacto al evitar que la amenaza se propague a otros segmentos de la red, lo que minimiza el daño potencial y facilita la contención y mitigación de incidentes.

4.2.5 Implementar un sistema o software de monitoreo del tráfico de la red

Con respecto al monitoreo del tráfico de la red, su importancia radica en establecerse como una medida de seguridad para proteger la información y los sistemas de una organización, ya que por medio de estas herramientas se pueden registrar eventos, monitorear en tiempo real actividades sospechosas que interfieran con el funcionamiento normal de la red de la empresa. Además, de implementar la detección de intrusos por medio de estas herramientas para monitorear y alertar sobre posibles intentos de acceso no autorizado o actividades maliciosas en la red.

4.2.6 Implementar de nuevos procedimientos dentro de la empresa

La implementación de políticas de seguridad de la red dentro de una empresa es un proceso crucial para proteger los activos digitales, salvaguardar la información confidencial y prevenir ciberataques. Estas políticas deben abordar temas como el acceso a la red, el uso de contraseñas seguras, la protección de datos confidenciales, el uso de dispositivos personales en la red corporativa, entre otros.

De igual forma, es idóneo el unificar todas las políticas que están relacionadas con la seguridad de la red con la casa matriz de la empresa, con el objetivo de brindar una protección más robusta para el aseguramiento de la información y brindar una respuesta rápida y efectiva en caso de un ataque y minimizar el impacto que actividades sospechosas o maliciosas tengan en la

organización. La implementación efectiva de políticas de seguridad de la red requiere un enfoque integral y proactivo para proteger la infraestructura de la empresa y los datos confidenciales.

4.3 Plan para el Cambio

Primeramente, se debe llevar a cabo una campaña de concientización sobre la importancia de los colaboradores en materia de ciberseguridad. Luego, se impartirán talleres técnicos sobre seguridad informática, para profundizar y adquirir competencias nuevas en esta disciplina. Sin embargo, puesto que el factor humano es de vital importancia, se recomienda realizar actividades similares continuamente y no excepcionalmente, como se detalla en el cronograma al final de esta sección. El departamento de Tecnología será el encargado de elaborar y aplicar el material que se utilizará con los colaboradores, así como regular y revisar los resultados de dichas capacitaciones. Adicionalmente, el departamento de Relaciones Humanas podrá colaborar en esta sección.

Para llevar a cabo esta capacitación del personal, se clasificará a los colaboradores en dos grupos: “técnicos” y “no técnicos”, donde los colaboradores técnicos son todas aquellas personas que desarrollan, mantienen, dan soporte, o trabajan de manera directa con la infraestructura de software y hardware propia de la empresa. Por ejemplo, profesionales de ingeniería telemática, software, sistemas, electrónica, entre otros. Todos los demás colaboradores pertenecerán al grupo “no técnico”.

Una vez seccionada la fuerza laboral, se brindará capacitación personalizada a cada grupo. En particular, los profesionales no técnicos recibirán talleres sobre seguridad informática básica en la empresa, orientados a prevenir ataques de terceros fuera de la compañía, ofrecidos por la compañía KnowBe4. Además, contarán con información de los recursos y personas de apoyo con quienes cuentan en la empresa, a fin de poder contactarlas en caso de algún siniestro informático.

Por otro lado, los tópicos que se brindarán a los profesionales técnicos estarán ligados a las mejores prácticas de la industria en cuanto desarrollo y mantenimiento de infraestructura tecnológica concierne. Puesto que estos colaboradores son los mayores responsables del bienestar cibernético de la empresa, su capacitación debe ser más técnica y detallada. Por ende, además de llevar los mismos talleres de seguridad informática básica de KnowBe4 mencionados anteriormente, realizarán también el entrenamiento técnico de la empresa Veracode, especializada en ciberseguridad para profesionales de ingeniería. Tanto KnowBe4 como Veracode fueron elegidas debido a su trayectoria en el mercado de capacitación en ciberseguridad, así como los reconocimientos que ambas empresas han obtenido.

Seguidamente, la empresa deberá realizar inversiones económicas para adquirir servicios de hardware y software que robustecen la seguridad informática de la compañía. En particular una licencia del gestor de contraseñas OnePassword para cada colaborador, y una licencia del software de gestión de dispositivos Jamf, para cada computadora en la organización. El departamento de Finanzas será el responsable de esta tarea, mientras que el equipo de Tecnología podrá brindar asesoría técnica.

Finalmente, se implementarán medidas técnicas que mejoren la seguridad informática de la empresa, a saber: habilitar y exigir la autenticación en dos pasos en las aplicaciones de software utilizadas en la compañía; instalar OnePassword y Jamf en los dispositivos de los colaboradores; establecer actualizaciones de los equipos de comunicaciones periódicamente y sistemas operativos que ingresen por medio de conexiones remotas; definición de una adecuada segmentación de la red y por último la implementación de un software de monitoreo de la red contra vulnerabilidades externas.

Para evaluar el avance del plan, se contabilizará la cantidad de colaboradores que han concluido su capacitación y comenzado a utilizar tanto el gestor de contraseñas como la autenticación en dos pasos. Puesto que el plan se llevará a cabo durante 4 meses, al finalizar cada mes se espera que un 25% de los colaboradores haya cumplido con este objetivo. De esta manera, al finalizar el cuatrimestre, el 100% de la empresa deberá haber cumplido con las disposiciones planteadas en la propuesta de cambio.

Adicionalmente, una vez finalizados los cuatro meses, el departamento de Tecnología podrá realizar ataques de prueba para corroborar la efectividad de las medidas tomadas. En particular, se enviarán correos simulando "phishing", elaborados por el propio equipo de Tecnología de la empresa, a colaboradores de Sonda para determinar si son víctimas de esta amenaza informática. De igual manera, se podrán realizar pruebas de naturaleza similar para evaluar la efectividad del plan aplicado.

4.3.1 Cronograma

A continuación, se presenta el cronograma propuesto que forma parte del plan de cambio luego de un análisis exhaustivo de los datos recolectados.

Tabla 2 *Cronograma de Trabajo*

Fase	Actividad	Mes de implementación				
		Agosto	Septiembre	Octubre	Noviembre	Diciembre
Fase I: planificación y aprobación.	Presentación del plan al personal a cargo de la división de Data Center y Cloud.					
	Aprobación del presupuesto por parte de la Gerencia General.					
Fase II: implementación de capacitaciones.	Capacitación de todo personal de la empresa de manera general sobre temas de ciberseguridad.					
	Capacitación del personal especializado para administradores de la infraestructura.					
Fase III: implementación de mejoras de seguridad en la red.	Incorporación del gestor de contraseñas por parte del personal especializado.					
	Incorporación de autenticación en dos pasos.					
Fase IV: auditoría y control.	Definir los departamentos de la empresa para aplicar una simulación de “phishing”					
	Preparar y personalizar los correos electrónicos de phishing y los enlaces maliciosos					
	Implementar la simulación y analizar los datos recopilados durante la simulación.					
	Evaluación de resultados tras aplicar el plan de cambio.					
	Comunicar los resultados a las gerencias y jefaturas involucradas.					

Fuente: elaboración propia (2023).

4.4 Presupuesto de Cambio

En esta sección, se abordarán aspectos cruciales del presupuesto de cambio del trabajo de investigación. Como parte del estudio, se ha identificado la necesidad de implementar cambios y mejoras en diferentes áreas para lograr los objetivos. Sin embargo, es necesario identificar los costos asociados con las actividades de cambio propuestas, así como los recursos y el financiamiento requeridos.

En la siguiente tabla, se detalla el coste de cada inversión necesaria para llevar a cabo el plan de cambio. Los cálculos se realizaron con 70 colaboradores, poco más de los 50 con los que cuenta actualmente la empresa Sonda Costa Rica. Con esto, se desea crear un margen económico para realizar el cambio, así como tomar en cuenta de antemano las posibles futuras contrataciones que se realizarán.

Tabla 3

Presupuesto de cambio. Costos generales

Detalle	Costo anual (1 usuario)	Costo anual (70 usuarios)
Licencia OnePassword	$95.00	$6,650
Licencia Jamf	$163.80	$11,466.00
PRTG	$1,899.00	$1,899.00
Capacitación KnowBe4	$2.75	$7,192.50
TOTAL	$2,160.55	$27,207.05

Fuente: elaboración propia (2023).

*Nota: Los montos corresponden a la información brindada por las siguientes empresas: OnePassword, Jamf, PRTG y KnowBe4. (knowbe4.com, s.f.)

A continuación, se presentan los gastos específicos para los profesionales de ingeniería. En Sonda Costa Rica, laboran cerca de 40 personas de esta especialidad.

Tabla 4

Presupuesto de cambio específico para profesionales de ingeniería

Detalle	Costo anual (1 profesional)	Costo anual (40 profesionales)
Capacitación Veracode	$100.00	$4,000.00
TOTAL	$100.00	$4,000.00

Fuente: elaboración propia (2023).

*Nota: Los montos corresponden a la información brindada por la empresa Veracode. (eLearning, s.f.)

La compañía KnowBe4, que ofrece servicios de capacitación en seguridad informática básica, tiene una tarifa de $2.75 por usuario anualmente. Con esto, se instruirá a todo el personal en materia de ciberseguridad. Adicionalmente, la empresa Veracode cuenta con capacitaciones específicas para profesionales de ingeniería. Puesto que Sonda Costa Rica cuenta con 40 colaboradores de este tipo, el costo de brindar dicha capacitación a la totalidad de este grupo es de $4000 anuales.

El gestor de contraseñas OnePassword, en su línea de productos para empresas, ofrece servicios a $95.88 por usuario anualmente. Con este servicio, todos los colaboradores de Sonda Costa Rica no tendrán que almacenar sus contraseñas de manera física o digital, pues la aplicación realizará el trabajo por ellos. De esta forma, el riesgo de una filtración de contraseñas se reduce dramáticamente.

Por su parte, el software de gestión de dispositivos Jamf, cuenta con su línea para negocios a $163.80 por usuario anualmente. Al utilizarlo, se podrán realizar actualizaciones de

sistema operativo automáticas, así como bloquear el dispositivo en caso de robo o extravío. Adicionalmente, se obtendrán notificaciones y alertas sobre posibles riesgos de seguridad en las aplicaciones instaladas en el equipo.

En cuanto a software para monitoreo de red, se eligió el programa Paessler Router Traffic Grapher (PRTG), pues ofrece un servicio adecuado para las necesidades de la empresa. Debido a su modelo de facturación, el costo por 1 usuario o toda la compañía es el mismo, por lo que abarcar a toda la empresa no corresponde a un gasto adicional.

Para incorporar la autenticación en dos pasos en los programas de la compañía, se recomienda la aplicación de Google Authenticator. Este software no tiene costo alguno, por lo que representa una inversión en ciberseguridad sin costo.

Si bien es cierto los costos anuales pueden parecer elevados de entrada, el beneficio de contar con ellos es sumamente benéfico para la ciberseguridad de la empresa. Un ataque informático puede tener consecuencias nefastas, que se pueden prevenir con una inversión atinada en robustecer los sistemas defensivos de la compañía. Por esta razón, se recomienda pagar el precio económico de la prevención, en lugar de esperar a que suceda un incidente y verse obligado a pagar el precio de la desatención en seguridad.

4.4.1 **Información sobre las capacitaciones**

En un mundo en constante evolución, la adquisición de nuevos conocimientos y habilidades es esencial para el crecimiento personal y profesional. En esta sección, se proporciona información detallada sobre los temas a impartir en las capacitaciones tanto “técnicas” como “no técnicas” de cada una de las academias seleccionadas previamente, proporcionando una visión detallada del conocimiento ofrecido y diseñado para fortalecer el entendimiento en temas de ciberseguridad de los colaboradores de la empresa Sonda Costa Rica.

A continuación, se muestra el contenido de la capacitación que será impartida por la empresa KnowBe4 y la duración de cada uno de los temas, divididos en 3 sesiones de aproximadamente 6 horas cada una, preparada para el personal “técnico” y “no técnico” de la empresa Sonda, con el objetivo de fortalecer el conocimiento general en el área de la ciberseguridad:

Tabla 6

Contenido capacitación KnowBe4

Capacitación – KnowBe4		
Tema	**Duración**	**Sesión**
Introducción a la protección de datos	1 hora	I Sesión
Introducción al ransomware	1 hora	
Introducción a la ingeniería social	1 hora	
Introducción al phishing	1 hora	
Principales claves de la protección contra ransomware	1.5 horas	
Ciberseguridad en el lugar de trabajo I: Correo electrónico	2 horas	II Sesión
Ciberseguridad en el lugar de trabajo II: Trabajo remoto	2 horas	
Ciberseguridad en el lugar de trabajo III: Información confidencial	2 horas	
Contraseñas seguras: Ocho formas de aumentar su seguridad	3 horas	III Sesión
Redes sociales: cómo protegerse en un mundo conectado	2 horas	
Total	16.5 horas	

Fuente: elaboración propia (2023).

En la siguiente tabla, se muestra el contenido de la capacitación que será impartida por la empresa Veracode y la duración de cada una de las tareas, dividida en 3 sesiones de aproximadamente 8 horas cada una, preparada para el personal de los departamentos de la empresa Sonda que se encuentran en contacto directo con la tecnología como parte de sus funciones diarias, con el objetivo de fortalecer el conocimiento en el área de la ciberseguridad y blindar el factor humano en caso de un posible ataque:

Tabla 7

Contenido capacitación Veracode

Capacitación Técnica – Veracode		
Tema	**Duración**	**Sesión**
Inyección de código SQL	2 horas	I Sesión
Autenticación rota	2 horas	
Entidades XML externas (XXE)	2 horas	
Pérdida de control de acceso	2 horas	II Sesión
Scripting entre sitios (XSS)	2 horas	
Mejores prácticas en las configuraciones seguras de red	3 horas	
Inteligencia Artificial ética: un camino hacia la sensibilidad	3 horas	
Logging: prácticas seguras en la empresa	2 horas	III Sesión
Criptografía I: Fallas criptográficas más comunes	3 horas	
Criptografía II: Garantizando privacidad en tránsito y en reposo	3 horas	
Total	24 horas	

Fuente: elaboración propia (2023).

4.5 Valoración del Plan Cambio

Para valorar el plan del cambio, se entrevistaron a profesionales de las áreas de Tecnología y Finanzas, que no son colaboradores de Sonda Costa Rica, y que poseen amplia experiencia en el tema de implantar mejoras de ciberseguridad en las empresas. A continuación, se detallan las principales ideas expuestas por dichas expertas.

Con respecto a los esfuerzos a realizar por el departamento de Tecnología, se consideraron como un buen punto de inicio para mejorar la ciberseguridad de la empresa. Tanto el programa gestor de contraseñas, como el gestor de dispositivos, son prácticas estándar en otras compañías de tecnología. La experta técnica mencionó, incluso, que la elección de OnePassword y Jamf ha sido utilizada en varias de sus experiencias profesionales anteriores.

Sin embargo, se cuestionó el impacto sobre los colaboradores no técnicos en la empresa. De manera particular, se hizo hincapié en la importancia de concientizar correcta y continuamente a esta población, pues es la más expuesta a permitir ataques cibernéticos. Por ende, se recomendó considerar una diferenciación en el entrenamiento a brindar a los colaboradores, para tener especial atención con aquellos menos familiarizados con la tecnología.

Por su parte, la experta en finanzas sostuvo que, a nivel empresarial, los montos a pagar no son excesivamente altos. Por el contrario, comparados con otros gastos típicos de una compañía, no representan la porción más elevada de cuentas por pagar. Por tratarse de una inversión en seguridad, se estimó como apropiada y factible, pues sus beneficios sobrepasan grandemente sus riesgos.

Empero, la experta mencionó también el clima económico actual. Ante factores como la incertidumbre en el tipo de cambio, guerras en otras latitudes, recesiones económicas a la vista y demás, algunos ejecutivos de finanzas pueden mostrarse reacios a permitir gastos

extraordinarios. Sobre esta línea, precisó la importancia de mostrar claramente los riesgos a los que se está expuesto en el mundo tecnológico, así como el valor que aportará adoptar las soluciones aquí expresadas. Esto será, en palabras de la experta, el factor principal que decidirá la puesta en marcha de la propuesta de cambio.

Conclusiones y Recomendaciones

La ciberseguridad se ha convertido en un componente vital en el mundo cada vez más interconectado y digitalizado. A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas, lo que requiere una respuesta proactiva y sólida para salvaguardar la información y los sistemas. Esta investigación realizada ha permitido comprender la importancia de la conciencia de seguridad que debe mantener el personal de la empresa Sonda, la implementación de medidas de protección adecuadas en los equipos de comunicaciones y la correcta colaboración entre los actores involucrados con los temas sobre ciberseguridad.

Para el objetivo específico 1 *identificar el nivel de cumplimiento de la empresa Sonda con respecto a la norma ISO 27001, mediante una evaluación informática que considere las prácticas de seguridad aplicadas en la actualidad* se concluye que:

- ✓ Basándose en los resultados de la evaluación informática aplicada en la empresa Sonda, se confirma el cumplimiento de este objetivo, debido a que se puede afirmar que las prácticas de seguridad aplicadas en la actualidad demuestran un nivel razonable de madurez en la protección de los accesos remotos y políticas de seguridad aplicadas al personal de la organización. Sin embargo, se identificaron áreas de mejora, como la actualización de software y la implementación de medidas de seguridad adicionales en cuanto al monitoreo del tráfico de la red, que deben abordarse para fortalecer de una mejor forma la postura de seguridad de la empresa.
- ✓ Gracias a la evaluación informática realizada se revela que las prácticas de seguridad aplicadas en la actualidad en la empresa Sonda son efectivas para detectar y responder a posibles amenazas y ataques cibernéticos. El monitoreo

constante del tráfico de red, la implementación de soluciones de detección y prevención de intrusiones, y la respuesta rápida a las alertas de seguridad son aspectos clave para mantener la integridad y confidencialidad de información importante para la organización.

Para el objetivo específico 2 analizar los riesgos informáticos, de infraestructura y personal, identificando la severidad de cada vulnerabilidad encontrada se concluye que:

- ✓ De acuerdo con los resultados del análisis de riesgos informáticos, se determinó que las vulnerabilidades informáticas presentan un riesgo moderado para la organización. La falta de parches y actualizaciones de seguridad en los equipos de comunicaciones, la inexistencia de herramientas de detección de intrusos y la falta de monitoreo de tráfico en la red son las principales áreas que requieren atención inmediata para reducir la probabilidad de incidentes de seguridad, de esta forma se cumple con el objetivo planteado identificando los riesgos y vulnerabilidades.
- ✓ El análisis de riesgos también revela la importancia de abordar las vulnerabilidades relacionadas con el factor humano. La falta de conciencia en seguridad y permisos inadecuados de acceso a la red por la falta de segmentación representan riesgos significativos para la organización. Es fundamental implementar programas de concienciación y capacitación en seguridad, así como establecer una reestructuración de la red para mitigar estos riesgos y promover una cultura de seguridad en toda la compañía.

Para el objetivo específico 3 realizar una encuesta para conocer los hábitos de seguridad de la información en el personal, para determinar su nivel de experticia se concluye que:

- ✓ La investigación sobre los hábitos de seguridad de la información en el personal revela que existen diferentes niveles de experticia en cuanto a prácticas de seguridad en la empresa. Algunos colaboradores muestran un alto nivel de conocimiento y adoptan buenas prácticas de seguridad, como la actualización periódica del sistema operativo y el uso de contraseñas fuertes en su ingreso a sistemas. Sin embargo, se identificaron deficiencias en ciertos aspectos, como la falta de conocimiento sobre ataques informáticos y la importancia de la seguridad de la información para la empresa. Estos hallazgos resaltan la necesidad de programas de capacitación y concienciación para mejorar los hábitos de seguridad de todo el personal y fortalecer la postura de seguridad de la compañía en caso de un posible ataque cibernético, de esta manera se cumple con el objetivo planteado.
- ✓ Con base en los hallazgos de la evaluación informática, se recomienda que la empresa Sonda continúe fortaleciendo sus prácticas de seguridad mediante la adopción de enfoques proactivos. Esto implica la implementación de programas de concienciación y capacitación en seguridad para el personal, la realización de evaluaciones periódicas de riesgos, y la mejora continua de los controles de seguridad existentes para mantenerse al tanto de las últimas amenazas y vulnerabilidades en los sistemas informáticos.
- ✓ Con relación a la experiencia en seguridad de la información, existen algunos colaboradores que aplican medidas de seguridad recomendadas, como la autenticación de dos factores y la utilización de redes VPN para conexiones

remotas, otros aún no comprenden aspectos como la identificación de enlaces sospechosos en correos electrónicos y el manejo de dispositivos personales en el entorno laboral. Estos resultados resaltan la necesidad de programas de capacitación personalizados y la implementación de controles adicionales para elevar la experticia en seguridad de toda la empresa.

Para el objetivo específico 4 Elaborar un plan de acción que considere los lineamientos establecidos en el documento ISO 27001 y los hallazgos de la encuesta se concluye que:

- ✓ Basado en los lineamientos establecidos en la norma ISO 27001, se elaboró un plan de acción que aborda aspectos clave de seguridad de la información para la empresa. Este plan de acción incluye la implementación de herramientas de control de tráfico en la red, autenticación por medio de dos factores, actualizaciones periódicas en los equipos de comunicaciones y la concienciación y capacitación del personal en temas de seguridad. La implementación de este plan permitirá a la empresa mitigar los riesgos y aumentar la protección eficaz de la información valiosa.
- ✓ El plan de acción elaborado brinda una guía sólida para mejorar la seguridad de la información en la empresa, de acuerdo con el análisis de las vulnerabilidades encontradas por medio de los instrumentos anteriormente aplicados en la investigación.

Con base en las conclusiones anteriores, se detallan las siguientes recomendaciones para la empresa Sonda Costa Rica y, de manera general, cualquier empresa que desee robustecer su seguridad informática:

- ✓ Dedicar una parte importante de los recursos, tanto en tiempo y en dinero, a concientizar a los colaboradores en materia de ciberseguridad. Este rubro dará los mayores frutos, tanto para la compañía como para el personal.
- ✓ Reconocer la diferencia entre los colaboradores técnicos y no técnicos, así como sus distintas necesidades en cuanto a capacitación concierne.
- ✓ Identificar a los responsables de llevar a cabo las distintas secciones del plan de cambio, con el fin de optimizar las habilidades y recursos de cada persona o departamento.
- ✓ Elaborar un plan concreto, detallado y plausible para presentar con los responsables financieros de la empresa. El apoyo a un futuro plan de cambio depende de la claridad con la que se transmita el valor que aportan las distintas inversiones a realizar.

En última instancia, la ciberseguridad es una responsabilidad compartida que involucra a individuos y organizaciones como tal. Al trabajar por un mismo objetivo, promoviendo buenas prácticas de seguridad, invirtiendo en tecnologías robustas y fomentando la educación y conciencia en los colaboradores, es posible construir un entorno digital más seguro y resistente frente a las amenazas cibernéticas enfrentadas día a día en el mundo actual.

Referencias Bibliográficas

Instituto Internacional de Estudios en Seguridad Global. (14 de enero de 2020). *Iniseg.* Obtenido de Iniseg: www.iniseg.es/blog/ciberseguridad/factor-humano-y-ciberseguridad/

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2022). *Diagnóstico Sector Telecomunicaciones.* Obtenido de Diagnóstico Sector Telecomunicaciones: https://www.micitt.go.cr/wp-content/uploads/2022/04/diagnostico_sector_telecomunicaicones_pndt_2022-2027_version_final.pdf

Avanza Proceso de implementación de la Estrategia Nacional de Ciberseguridad. (2023, 27 abril). https://www.micitt.go.cr/2023/04/27/avanza-proceso-de-implementacion-de-la-estrategia-nacional-de-ciberseguridad/

Acronis.Cyber Protect Cloud. (24 de junio de 2021). *Acronis.Cyber Protect Cloud*. Obtenido de Acronis.Cyber Protect Cloud: https://www.acronis.com/es-mx/blog/posts/social-engineering/

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Álvarez, D. C. (2022, April 19). Estas son las plataformas del Gobierno que han sido hackeadas. Telediario Costa Rica. https://www.telediario.cr/nacional/estas-son-las-plataformas-del-gobierno-que-han-sido-hackeadas

Bardales, J. M. D. (2021). La investigación científica: su importancia en la formación de investigadores. Ciencia Latina Revista Científica Multidisciplinar, 5(3), 2385-2386.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669.

Castro Bermúdez, Y., Muñoz Guerrero, L., & Solarte Martínez, G. (2019). *Planificación, Gestión y Control de la Calidad del Software.*

Castro, J. (30 de julio de 2020). Costa Rica ocupa el quinto puesto de América en ciberseguridad. *La República. net.*

Clavellina Miller, J., & Domínguez Rivas, M. (s.f. de Marzo de 2020). *Implicaciones económicas de la pandemia por COVID-19 y opciones de política.* Obtenido de bibliodigitalibd.senado.gob.mx: http://bibliodigitalibd.senado.gob.mx/handle/123456789/4829

Coll Morales, Francisco. (1 de mayo de 2020). *economipedia*. Obtenido de economipedia: https://economipedia.com/definiciones/estandarizacion.html

Comisión Nacional de Emergencias. (s.f. de junio de 2022). *www.cne.go.cr*. Obtenido de www.cne.go.cr: https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf

Contreras, R. (16 de octubre de 2022). *Digital 360. Los 10 ciberataques más grandes de la década.* Obtenido de Digital 360. Los 10 ciberataques más grandes de la década: https://www.computing.es/seguridad/los-10-ciberataques-mas-grandes-de-la-decada/

Cybersecurity, S. (2020). *La breve historia de la ciberseguridad*. Obtenido de La breve historia de la ciberseguridad: https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

de Franco, M. F., & Solórzano, J. L. V. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. Mundo Recursivo, 3(1), 1-24.

Galeano, S. (26 de enero de 2023). *Marketing Ecommerce*. Obtenido de Marketing Ecommerce: https://marketing4ecommerce.net/usuarios-de-internet-mundo/

Global, I. I. (14 de enero de 2020). *Factor humano y ciberseguridad, un riesgo en crecimiento.* Obtenido de Factor humano y ciberseguridad, un riesgo en crecimiento: www.iniseg.es/blog/ciberseguridad/factor-humano-y-ciberseguridad/

Haider Th.Salim , A., & Hussein Tuama, H. (2021). Enhanced Data Security of Communication System Using Combined Encryption and Steganography. *International Journal of Interactive Mobile Technologies*, 1.

Hernández Armenta, M. (18 de abril de 2020). *forbes.co.* Obtenido de forbes.co: https://forbes.co/2020/04/28/tecnologia/google-detecta-18-millones-de-correos-maliciosos-al-dia-relacionados-con-covid-19

Hernández Sampieri, R., Fernández, C. C., & Baptista Lucio, P. (2018). *Metodología de la Investigación.* México: McGraw-Hill Interamericana.

Instituto Tecnológico de Costa Rica. (2020). *Unidad Especializada de Control Interno*. Obtenido de Unidad Especializada de Control Interno: https://www.tec.ac.cr/valoracion-riesgo

Kaspersky.com. (2023). *latam.kaspersky.com*. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Malwarebytes. (13 de diciembre de 2021). *Malwarebytes*. Obtenido de Suplantación de identidad (phishing): https://www.malwarebytes.com/blog/news/2021/12/spear-phish-whale-phish-regular-phish-whats-the-difference

Montgomery, D. C., & Runger, G. C. (2019). Applied Statistics and Probability for Engineers sixth edition. https://perpustakaan.itera.ac.id/slims/index.php?p=show_detail&id=2131

Morales Rojas, J. G. (2022). Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial.

Navidi, W. (2019). Statistics for engineers and scientists. http://ci.nii.ac.jp/ncid/BB01850726

Padilla-Avalos, C. A., & Marroquín-Soto, C. (2021). Enfoques de investigación en odontología: cuantitativa, cualitativa y mixta. Revista estomatologica herediana, 31(4), 338-340.

Palacios Echeverría, A. (1 de octubre de 2021). La pérdida de la privacidad. *El País.cr*, pág. 2.

Pérez Porto, J., & Merino, M. (24 de mayo de 2021). *Recursos tecnológicos - Qué son, en el hogar, definición y concepto.* Obtenido de Definición.de: https://definicion.de/recursos-tecnologicos/

Pérez, C. C. (2022, April 21). Ataques cibernéticos aumentaron contra empresas e instituciones en Costa Rica durante esta semana. El Financiero. https://www.elfinancierocr.com/tecnologia/ataques-ciberneticos-aumentaron-contra-empresas-e/3UKWNFT67RABXOS6MLXBUDEGM4/story/

¿Qué es la seguridad de datos? Definición y descripción general de la seguridad de datos | IBM. (n.d.). https://www.ibm.com/es-es/topics/data-security

¿Qué es MICITT? (s. f.). https://www.micitt.go.cr/que-es-micitt/

Ramos Galarza, C. A. (2020). Los alcances de una investigación. *Revista CienciAmérica*, 6. Obtenido de dialnet.unirioja.es: https://dialnet.unirioja.es/servlet/articulo?codigo=7746475

Real Academia Española. 23° Edición. (2022). *Diccionario Real Academia Española*. Obtenido de Diccionario Real Academia Española: https://dle.rae.es/

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., & Castillo Merino, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante: Editorial Área de Innovación y Desarrollo,S.L.

Sánchez, J. F. E. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. La Razón histórica: revista hispanoamericana de historia de las ideas políticas y sociales, (44), 153-173.

Sangaiah, A. K., Medhane, D. V., Han, T., Hossain, M. S., & Muhammad, G. (2019). Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics. IEEE Transactions on Industrial Informatics, 15(7), 4189-4196.

Sistema Costarricense de Información Jurídica. (22 de abril de 2015). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal*. Obtenido de Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal: http://www.pgrweb.go.cr.

Sonda. (2023). *Sonda.com*. Obtenido de Sonda.com: https://www.sonda.com/

Torres, M., Salazar, F. G., & Paz, K. (2019). Métodos de recolección de datos para una investigación.

Universidad de Costa Rica. (2010). *Ciberseguridad en Costa Rica.* San José: PROSIC.

Anexo 1. "Instrumento de recolección de datos, encuesta".

Evaluación sobre Seguridad Informática

Porque su opinión es importante, solicitamos su colaboración para responder la siguiente encuesta sobre su percepción acerca de la seguridad informática en su empresa.

La información que nos suministre será confidencial.

Muchas gracias.

1. ¿Su computadora tiene la última versión disponible del Sistema Operativo?

   Sí ___ No___ No lo sé___

2. ¿La empresa para la que usted trabaja administra las actualizaciones de software de manera remota y automática?

   Sí ___ No___ No lo sé___

3. ¿Cada cuánto usted cambia la clave de su computadora de trabajo?

   1-90 días___ 90-365 días___ Más de 365 días_____

4. Cuando deja su estación de trabajo (por ejemplo, para ir a almorzar), ¿bloquea su computadora e ingresa de nuevo la contraseña cuando regresa?

   Sí___ No___

5. ¿Sabe usted cuál es el antivirus instalado en su computadora de trabajo?

   Sí___ No___

6. La información confidencial o sensible almacenada en su computadora de trabajo, ¿está encriptada?

   Sí ___ No___ No lo sé___

7. Para ingresar a los programas informáticos de su empresa (por ejemplo: correo electrónico, servicios de mensajería informática, aplicaciones de llamadas en tiempo real, entre otros), ¿está activada la autenticación en dos pasos?

Sí___ No___

8. En el último año, ¿ha recibido capacitación en ciberseguridad por parte de su empresa?

Sí___ No___

9. En caso de sufrir un ataque informático en su computadora de trabajo, ¿sabe usted a quién acudir para solicitar ayuda?

Sí___ No___

10. ¿Utiliza usted algún gestor de contraseñas (ejemplo:. Google Contraseñas, BitGuardian, OnePassword, entre otras) para almacenar sus contraseñas en el lugar de trabajo?

Sí___ No___

11. ¿Conoce usted la diferencia entre autenticación y autorización en materia de ciberseguridad?

Sí___ No___

12. ¿Ha sido usted víctima de algún ataque informático?

Sí___ No___

13. ¿Se siente usted responsable de la seguridad informática en su empresa?

Sí___ No___

Anexo 2. “Información recopilada a través de la encuesta”.

Tabla 8

Resultados de los datos recopilados a través del cuestionario.

		Sí	No	No sé
Pregunta #1	¿Su computadora tiene la última versión disponible del Sistema Operativo?	4	5	14
Pregunta #2	¿La empresa para la que usted trabaja administra las actualizaciones de software de manera remota y automática?	5	5	13
Pregunta #6	La información confidencial o sensible almacenada en su computadora de trabajo, ¿está encriptada?	3	3	17
		1-90 días	91-365 días	>365 días
Pregunta #3	¿Cada cuánto usted cambia la clave de su computadora de trabajo?	5	7	11
		Sí	No	
Pregunta #4	Cuando deja su estación de trabajo (por ejemplo, para ir a almorzar), ¿bloquea su computadora e ingresa de nuevo la contraseña cuando regresa?	15	8	
Pregunta #5	¿Sabe usted cuál es el antivirus instalado en su computadora de trabajo?	5	18	
Pregunta #7	Para ingresar a los programas informáticos de su empresa (por ejemplo: correo electrónico, servicios de mensajería informática, aplicaciones de llamadas en tiempo real, entre otros), ¿está activada la autenticación en dos pasos?	12	11	
Pregunta #8	En el último año, ¿ha recibido capacitación en ciberseguridad por parte de su empresa?	3	20	
Pregunta #9	En caso de sufrir un ataque informático en su computadora de trabajo, ¿sabe usted a quién acudir para solicitar ayuda?	6	17	
Pregunta #10	¿Utiliza usted algún gestor de contraseñas (ejemplo:. Google Contraseñas, BitGuardian, OnePassword, entre otras) para almacenar sus contraseñas en el lugar de trabajo?	3	20	
Pregunta #11	¿Conoce usted la diferencia entre autenticación y autorización en materia de ciberseguridad?	4	19	
Pregunta #12	¿Ha sido usted víctima de algún ataque informático?	2	21	
Pregunta #13	¿Se siente usted responsable de la seguridad informática en su empresa?	2	21	

Fuente: elaboración propia (2023).

Anexo 3. “Entrevista al personal encargado del área de redes en Sonda Costa Rica”

Entrevista

Mejores prácticas de la norma ISO 27001 aplicadas a los equipos de comunicaciones

1. En cuanto a la seguridad de la red en la empresa, ¿Hay una configuración segura de los equipos para proteger la infraestructura de comunicaciones contra amenazas y vulnerabilidades?

En cuanto a firewalls, existen reglas de filtrado de paquetes para permitir solamente el tráfico necesario y bloquear el tráfico no autorizado.

Existen conexiones VPN para permitir el acceso remoto de los usuarios que realizan teletrabajo y puedan acceder a la red interna

2. ¿Cuáles políticas de seguridad se aplican dentro de la empresa?

Se aplican políticas de usuarios y contraseñas de dominio, las cuales deben tener una cierta cantidad de caracteres y un cambio periódico.

Políticas de seguridad en las redes inalámbricas, principalmente con los usuarios que son visitantes de la empresa.

3. ¿Qué mecanismos utiliza la empresa para proteger la información en tránsito?

Se utilizan mecanismos como túneles VPN para conexiones remotas y autenticación de dos factores con el objetivo de validar la identidad de los usuarios que están accediendo a la información en tránsito.

4. ¿Podría mencionar algunos de los protocolos seguros que utilizan en la empresa?

Se utilizan protocolos seguros como IPsec, a través de las conexiones VPN y SSH para realizar conexiones a los equipos de comunicaciones de manera remota dentro de la red interna.

También se utiliza el protocolo SFTP para transferencia de archivos en caso de requerirlo en los equipos de comunicaciones.

5. ¿Cómo se gestionan los accesos remotos dentro de la empresa?

Los accesos remotos se gestionan por medio de conexiones VPN que se administran en un equipo de seguridad marca Cisco, modelo ASA.

6. Podría indicarnos, ¿qué tipo de prácticas utilizan para la autenticación y control de accesos?

Entre las prácticas de autenticación están las contraseñas seguras, los usuarios deben establecer ciertos requisitos en sus contraseñas y la autenticación de doble factor de identidad, donde se registra un número de teléfono y por medio de un mensaje de texto se envía un código de autorización para validar el acceso remoto.

7. En cuanto a la gestión de incidentes de seguridad ¿cómo los detecta la empresa?

En este momento la empresa no cuenta con un sistema de detección de incidentes de seguridad.

8. ¿Podría mencionar algunos de esos procedimientos para la gestión de incidentes?

En este momento la empresa no cuenta con un sistema de detección de incidentes de seguridad.

9. ¿Cuentan ustedes con estadísticas sobre accidentes, ataques, tiempos de respuesta a estos incidentes, entre otros?

La empresa no cuenta con ningún sistema sobre accidentes o ataques a incidentes en este momento.

10. Finalmente, ¿qué opina de la actualización y parcheo de equipos de comunicaciones?

Me parece una tarea importante que debe implementarse ya que esto depura la red sobre nuevas vulnerabilidades que encuentran los fabricantes, es una tarea que lleva tiempo y planificación ya que se recomienda se realice fuera de horario laboral, en caso de fallo es importante que los equipos cuenten con un contrato activo con el fabricante, en este caso, la mayoría de equipos se encuentran obsoletos y fuera de contrato.

Anexo 4. Carta de aprobación de la empresa Sonda.

San Pedro, Agosto, 2023

Señores

Comité de Trabajos Finales de Graduación

Escuela de Ingeniería

Universidad Latina de Costa Rica

Estimados señores:

Por este medio certifico que estoy de acuerdo con la propuesta elaborada por Marianela Isabel Marín Masís, estudiante de su universidad, para la empresa Sonda Costa Rica, en su Trabajo Final de Graduación.

Considero que es factible aplicar dichas recomendaciones en nuestra empresa y quedo a la orden para cualquier otra consulta.

Suscribe cordialmente

X VLADIMIR CHACON HERRERA (FIRMA)

Firmado digitalmente por VLADIMIR CHACON HERRERA (FIRMA)
Fecha: 2023.08.18 14:10:00 -06'00'

Ing. Vladimir Chacón Herrera
Supervisor de Operaciones CDC

Glosario

A

Antivirus: Programas especializados en la detección y, si es posible, en la destrucción de virus informáticos. Dada la velocidad con que aparecen nuevos y más sofisticados de estos programas "infecciosos", el mayor problema es la actualización continua, teniendo en cuenta los bajos rendimientos conseguidos en cuanto a la detección de virus desconocidos.

Aprendizaje automático: El aprendizaje automático es un subconjunto de inteligencia artificial que permite que un sistema aprenda y mejore de forma autónoma mediante redes neuronales y aprendizaje profundo, sin tener que ser programado explícitamente, a través de la ingesta de grandes cantidades de datos.

Ataque cibernético: Son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos.

Ataque distribuido de denegación de servicio (DDoS): Un ataque DDoS, o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.

C

Ciberdelincuente: El ciberdelincuente es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware.

Ciberdelito: Delito cometido mediante el uso de métodos informáticos o a través de Internet o las redes virtuales.

Ciberespacio: El término inglés cyberspace llegó al castellano como ciberespacio. Así se denomina al entorno artificial que se desarrolla mediante herramientas informáticas.

Ciberespionaje: El ciberespionaje es un tipo de ciberdelito en el que los piratas informáticos obtengan acceso inadvertido a sistemas digitales que siempre están conectados a Internet. Usando tácticas oscuras, los malos actores en su mayoría roban datos personales y profesionales que podrían generar dinero en la web oscura, obtener ganancias competitivas sobre los rivales comerciales o empañar la reputación de los rivales políticos.

Cibernauta: Es la persona que navega por el ciberespacio, que no es otra cosa que "el mundo generado mediante la conexión a Internet", es decir que no se amarra a un único dispositivo.

Ciberseguridad: La ciberseguridad o seguridad en Internet hace referencia al conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas computables.

Computación cuántica: Esta rama de la informática se basa en los principios de la superposición de la materia y el entrelazamiento cuántico para desarrollar una computación distinta a la tradicional. En teoría, sería capaz de almacenar muchísimos más estados por unidad de información y operar con algoritmos mucho más eficientes a nivel numérico, como el de Shor o el temple cuántico. Esta nueva generación de superordenadores aprovecha el conocimiento de la mecánica cuántica —la parte de la física que estudia las partículas atómicas y subatómicas— para superar las limitaciones de la informática clásica. Aunque la computación cuántica presenta

en la práctica problemas evidentes de escalabilidad y decoherencia, permite realizar multitud de operaciones simultáneas y eliminar el efecto túnel que afecta a la programación actual en la escala nanométrica.

Confidencialidad: La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información.

Conti Group: Banda cibernética Conti que se especializaba en el robo y encriptado de datos sensibles, que usaba para extorsionar "a grandes presas", como corporaciones o gobiernos. Múltiples instituciones latinoamericanas han sido víctimas de este tipo de extorsión, gracias al atraso en sus prácticas de seguridad informática

Cookies: Cuando se visita una página Web, es posible recibir una Cookie. Este es el nombre que se da a un pequeño archivo de texto, que queda almacenado en el disco duro del ordenador. Este archivo sirve para identificar al usuario cuando se conecta de nuevo a dicha página Web.

D

Delitos informáticos: El delito informático se define como el acto delictivo en el que se hace uso de la informática para su comisión, bien sea como medio o como fin de este.

Denegación de Servicio (denial of service (DOS)): Un ataque de denegación de servicio (DoS) es un tipo de ciberataque en el que un actor malicioso tiene como objetivo que un ordenador u otro dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el funcionamiento normal del mismo.

Desborde de pila: Un desbordamiento de pila es un error de tiempo de ejecución que ocurre cuando un programa se queda sin memoria en la pila de llamadas. El desbordamiento de la pila generalmente indica un problema en el aprovisionamiento de recursos y tiene que repararse para permitir que el programa se ejecute y use la memoria correctamente.

F

Firewalls (en español, muros de fuego): Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

H

Hacker: Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes.

Hacktivismo: El hacktivismo se define como la realización de actos, normalmente maliciosos, en Internet para promover unas ideas políticas, religiosas o sociales.

I

Ingeniería social: consisten en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. Generalmente engañan a la gente para obtener información sensible como contraseñas, números de cuentas bancarias, tarjetas de créditos, etc.

Inteligencia artificial: Ciencia que investiga la posibilidad de que un ordenador simule el proceso de razonamiento humano. Pretende también que el ordenador sea capaz de modificar su programación en función de su experiencia y que «aprenda».

Internet: Es la red global compuesta de limes de redes de área local (LAN) y de redes de área extensa (WAN) que utiliza TCP/IP para proporcionar comunicaciones de ámbito mundial a hogares, negocios, escuelas y gobiernos.

Internet de las Cosas: El término IoT, o Internet de las cosas, se refiere a la red colectiva de dispositivos conectados y a la tecnología que facilita la comunicación entre los dispositivos y la nube, así como entre los propios dispositivos. Gracias a la llegada de los chips de ordenador de bajo coste y a las telecomunicaciones de gran ancho de banda, ahora tenemos miles de millones de dispositivos conectados a Internet. Esto significa que los dispositivos de uso diario, como los cepillos de dientes, las aspiradoras, los coches y las máquinas, pueden utilizar sensores para recopilar datos y responder de forma inteligente a los usuarios.

M

Machine Learning: El Machine Learning es una disciplina del campo de la Inteligencia Artificial que, a través de algoritmos, dota a los ordenadores de la capacidad de identificar patrones en datos masivos y elaborar predicciones (análisis predictivo). Este aprendizaje permite a los computadores realizar tareas específicas de forma autónoma, es decir, sin necesidad de ser programados.

Malware: Malware es un término general para referirse a cualquier tipo de «malicious software» (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento y causar daños e interrupciones en el sistema o robar datos

N

Norma ISO 27001: La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

Norma ISO 27002: La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

Nube: Tecnología destinada a utilizar a distancia recursos de ejecución o almacenamiento.

P

Phishing: Es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. Normalmente, se utiliza con fines delictivos enviando SPAM e invitando acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios.

R

Ransomware: El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.

Redes informáticas: Una red informática es un conjunto de equipos o dispositivos interconectados que comparten recursos e intercambian información. Dentro de una red informática, encontramos los roles del emisor y del receptor a través de los cuales fluye la información. Estos roles se van intercambiando a menudo, produciéndose así un flujo de la información de manera bidireccional

Redes sociales: Las redes sociales son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes.

Registro de pulsaciones (key loger): El registro de pulsaciones de teclas es un método mediante el que se realiza el seguimiento y se registra cada tecla que el usuario pulsa en el teclado del ordenador, a menudo sin la autorización del usuario y sin que este se dé cuenta.

Respaldos o backups: La copia de seguridad, también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe.

S

Seguridad digital: La seguridad digital es un término amplio que se refiere a todas las diferentes formas de protección de datos e información en línea para que no sean robados, dañados o comprometidos.

Software: l término inglés original define el concepto por oposición a hardware: blando-duro, en referencia a la intangibilidad de los programas y corporeidad de la máquina. Software es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.

Spyware: Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos.

Suplantación de ARP: La suplantación de ARP (en inglés ARP spoofing) es enviar mensajes ARP falsos a la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo1 (el nodo atacado), como por ejemplo la puerta de enlace predeterminada. Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo). El atacante puede incluso lanzar un ataque de tipo DoS (denegación de servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

Suplantación de identidad: La suplantación o robo de identidad en internet consiste en hacerse pasar por otra para cometer actividades delictivas, tales como fraude o estafas, obtener datos o información sensible o confidencial.

T

Tecnología 5 G: 5G es la quinta generación de tecnología celular inalámbrica, que ofrece mayores velocidades de carga y descarga, conexiones más consistentes y una capacidad mejorada que las redes anteriores.

Tecnologías de la información: La tecnología de la información (TI) es el proceso de creación, almacenamiento, transmisión y percepción de la información y los métodos de aplicación de dichos procesos. Muchos equiparan el concepto con la tecnología informática porque ésta se ha desarrollado más rápidamente junto con ella.