Universidad CENFOTEC

MAESTRÍA EN CIBERSEGURIDAD

Documento final de Proyecto de Investigación Aplicada 2

Tema:

PROPUESTA PARA MEJORAR LA SEGURIDAD DE LA COMUNICACIÓN DE DATOS DE LAS ORGANIZACIONES DE COSTA RICA A TRAVÉS DE INTERNET.

Estudiante:
Solano Romero, Jeffry David

Abril, 2024

Declaratoria de derechos de autor

Yo, Jeffry David Solano Romero, autor del presente documento, presentado para obtener el grado de Maestría en Ciberseguridad en la Universidad Cenfotec, declaro que soy el autor de este documento. Las ideas, doctrinas, resultados y conclusiones a las que he llegado son de mi absoluta responsabilidad.

Se autoriza la consulta del documento con fines académicos y se prohíbe cualquier uso no autorizado de la tesis para su comercialización.

Dedicatorias

Dedico este proyecto final de graduación a:

A Dios, quien ha sido mi guía y me ha dado la fortaleza y confianza para poder realizar un proyecto de investigación exitoso.

A Stephanie Rocha Saborío, mi novia, quien siempre creyó en mí y me ha brindado un apoyo incondicional para lograr todos mis objetivos.

A Gilbert Solano Camacho, mi padre, en este proyecto, encuentro la oportunidad de expresar mi gratitud por su apoyo constante. Su presencia ha sido una fuente de inspiración para mí, y cada logro que he alcanzado se debe en gran parte a su sabiduría y orientación.

PROPUESTA PARA MEJORAR LA SEGURIDAD DE LA COMUNICACIÓN DE DATOS DE LAS ORGANIZACIONES DE COSTA RICA A TRAVÉS DE INTERNET.

Ing.Jeffry Solano Romero[1], MSc. Miguel Pérez Montero[2]
[1] jsolanor@ucenfotec.ac.cr
[2] mperez@ucenfotec.ac.cr

RESUMEN El aumento de la interconexión digital ha convertido la seguridad de las redes informáticas en un componente esencial para proteger los datos críticos de las organizaciones. Con el crecimiento de amenazas cibernéticas como *hackers*, *malware* e intrusiones internas, mantener la integridad y confidencialidad de los datos es un desafío constante. La seguridad de redes busca garantizar la confidencialidad, integridad y disponibilidad de los datos mediante medidas como cortafuegos, detección de intrusiones y políticas de acceso. Las organizaciones deben ser proactivas, capacitando a los empleados en seguridad cibernética, actualizando sistemas y aplicaciones, monitoreando amenazas y utilizando soluciones avanzadas. Las brechas de seguridad pueden tener consecuencias graves, desde la pérdida de datos hasta daños en la reputación y sanciones legales, por lo que la inversión en seguridad de redes es crucial. En un entorno digital complejo, la comunicación de la información es vital y compleja, comprender los desafíos, implementar soluciones efectivas y fomentar una cultura de seguridad son fundamentales para el éxito continuo de las organizaciones.

ABSTRACT *The increase in digital interconnection has made computer network security an essential component to protect organizations' critical data. With the growth of cyber threats such as hackers, malware, and insider intrusions, maintaining data integrity and confidentiality is a constant challenge. Network security seeks to guarantee the confidentiality, integrity, and availability of data through measures such as firewalls, intrusion detection and access policies. Organizations must be proactive, training employees in cybersecurity, updating systems and applications, monitoring threats, and using advanced solutions. Security breaches can have serious consequences, from data loss to reputational damage and legal penalties, making investment in network security crucial. In a complex digital environment, understanding the challenges, implementing effective solutions, and fostering a culture of security are critical to the continued success of organizations.*

PALABRAS CLAVE Ataques a la ciberseguridad, Autoevaluación, Infraestructura crítica, empresas en Costa Rica.

I. **INTRODUCCIÓN:** La seguridad de la comunicación de datos en internet es un aspecto crítico para cualquier organización en la era digital. La creciente dependencia de la red para la transmisión de información confidencial, financiera y estratégica ha dado lugar a una creciente preocupación por la protección de estos datos contra amenazas cibernéticas. La exposición a riesgos, como el robo de información, la interceptación de comunicaciones y el acceso no autorizado a sistemas, ha llevado a una búsqueda constante de soluciones para mejorar la seguridad en línea. En este contexto, se hace necesario abordar de manera efectiva los desafíos relacionados con la seguridad de la comunicación de datos en internet. Según el informe de la Promotora de Comercio Exterior (Procomer) "Perfil del uso y potencial de la ciberseguridad en empresas costarricenses", en 2020 en Costa Rica se detectaron alrededor de 201 millones de ciberataques, especialmente de *Phishing* y algunos nuevos métodos de hackeo basados en Inteligencia Artificial (IA) y en el Internet de las Cosas (IoT). Se estima que cada 10 segundos se producen pérdidas de casi USD$2 millones y en una hora hay casi 23.000 ataques a empresas e instituciones del país y esto ha ido creciendo exponencialmente conforme pasan los años. [1]

Según se muestra en la ilustración 1, en el gráfico se puede ver como los ciberataques han ido creciendo en los últimos años.

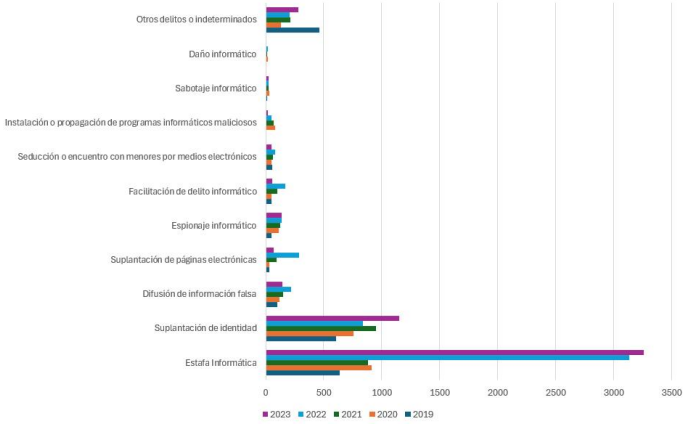

Ilustración 1 Crecimiento de los ciberataques
Fuente: Procomer, 2020

En este sentido, en este documento se presenta una propuesta integral que busca fortalecer la protección de la información transmitida en línea por las organizaciones. Esta propuesta se basa

en enfoques y tecnologías avanzadas que permiten garantizar la confidencialidad, integridad y autenticidad de los datos en tránsito, asegurando que la información sensible de las organizaciones no caiga en manos equivocadas. El objetivo principal de esta propuesta es proporcionar a las organizaciones en Costa Rica una serie de estrategias y mejores prácticas que les permitan enfrentar con éxito los desafíos actuales en materia de seguridad de la comunicación de datos en internet, y así garantizar la confianza de sus clientes, socios y empleados en un entorno digital cada vez más interconectado y expuesto a amenazas cibernéticas. Para lograrlo, se exploran diversas soluciones tecnológicas y políticas que fortalezcan la ciberseguridad de las organizaciones en la era de la información.

II. MÉTODOS Y MATERIALES:

Analizar la infraestructura de red crítica es fundamental en ciberseguridad por varias razones clave. En primer lugar, proporciona una comprensión profunda de los sistemas y dispositivos críticos que están interconectados, lo que permite identificar posibles vulnerabilidades y puntos de entrada para posibles ataques cibernéticos. Además, al comprender la topología y la arquitectura de la red, los equipos de seguridad pueden diseñar estrategias efectivas de defensa y respuesta ante incidentes.

Otro aspecto crucial es la detección temprana de amenazas. Al analizar la infraestructura de red crítica de manera regular, es posible detectar patrones inusuales o comportamientos sospechosos que podrían indicar la presencia de intrusiones o actividades maliciosas. Esta capacidad de detección temprana es fundamental para mitigar los riesgos al minimizar el impacto de los ataques cibernéticos.

Para este estudio, se empleó una metodología mixta que combinó análisis cualitativo y cuantitativo de datos, junto con una investigación exploratoria. El propósito fue recopilar información detallada sobre los tipos de ciberataques más comunes que enfrentan las empresas en Costa Rica.

En primer lugar, se llevó a cabo un análisis cualitativo para explorar las características y patrones subyacentes de los ciberataques. Esto implicó examinar casos específicos, entrevistas con expertos en ciberseguridad y revisión de informes de incidentes previos.

Por otro lado, se realizó un análisis cuantitativo para obtener datos numéricos sobre la frecuencia y la magnitud de los ciberataques en la región. Esto incluyó el análisis de estadísticas proporcionadas por instituciones gubernamentales, empresas de seguridad cibernética y otros organismos pertinentes.

Además, se llevó a cabo una investigación exploratoria para identificar posibles tendencias emergentes en el panorama de ciberseguridad de Costa Rica. Esto implicó la revisión de literatura especializada, la consulta de fuentes confiables en línea y la búsqueda de información en bases de datos relevantes.
En conjunto, esta metodología mixta permitió obtener una visión integral de los ciberataques más frecuentes en empresas costarricenses, proporcionando *insights* valiosos para fortalecer las estrategias de ciberseguridad y mitigar los riesgos asociados.

Además, se determinó que el análisis de la infraestructura de red crítica es fundamental para garantizar el cumplimiento de los estándares y regulaciones de ciberseguridad. Muchas industrias están sujetas a normativas específicas que requieren controles de seguridad robustos en sus sistemas críticos. Al analizar la infraestructura de red, las organizaciones pueden identificar posibles brechas de cumplimiento y tomar medidas correctivas para garantizar que se cumplan los requisitos legales y regulatorios.

III. PRINCIPALES AMENAZAS Y VULNERABILIDADES EN LAS EMPRESAS DE COSTA RICA:

Las principales amenazas y vulnerabilidades en las empresas de Costa Rica pueden incluir una variedad de factores, tanto internos como externos. Algunos de los más comunes son:

Ciberataques: Las empresas en Costa Rica están expuestas a una amplia gama de ciberataques, que pueden incluir *malware, ransomware, phishing,* ataques de denegación de servicio (DDoS) y ataques de ingeniería social. Estos ataques pueden resultar en la pérdida de datos, interrupción de servicios, daño a la reputación y pérdidas financieras.
Falta de conciencia y formación en seguridad: Muchas empresas pueden enfrentar vulnerabilidades debido a la falta de conciencia y formación en seguridad cibernética entre su personal. Los empleados pueden ser engañados por ataques de *phishing* o no estar al tanto de las mejores prácticas de seguridad, lo que puede llevar a brechas de seguridad.
Infraestructura de TI obsoleta: La utilización de sistemas y software desactualizados puede dejar a las empresas vulnerables a ataques y explotaciones de vulnerabilidades conocidas. La falta de actualizaciones de seguridad y parches puede exponer la infraestructura de TI a riesgos significativos.
Falta de políticas de seguridad claras: La ausencia de políticas de seguridad claras y robustas puede dejar a las empresas vulnerables a amenazas internas y externas. La falta de controles de acceso, políticas de contraseñas débiles y la negligencia en la gestión de cuentas de usuario pueden aumentar el riesgo de violaciones de

seguridad.

Riesgos relacionados con el cumplimiento normativo: Las empresas pueden enfrentar riesgos significativos relacionados con el cumplimiento normativo, especialmente en sectores regulados como la banca, la salud y las finanzas. El incumplimiento de regulaciones de protección de datos como la Ley de Protección de Datos Personales puede resultar en sanciones y multas.

Dependencia de proveedores de servicios: La tercerización de servicios a proveedores externos puede introducir riesgos adicionales de seguridad, especialmente si estos proveedores no cumplen con los estándares de seguridad adecuados o si se produce una brecha en sus sistemas.

Estas son solo algunas de las principales amenazas y vulnerabilidades a las que se enfrentan las empresas. Es importante que las organizaciones comprendan estos riesgos y tomen medidas proactivas para mitigarlos y proteger sus activos y datos críticos.

IV. TIPO DE HERRAMIENTAS QUE OFRECE EL MERCADO PARA LA EVALUACIÓN DE RIESGOS:

El mercado de la ciberseguridad ofrece una amplia gama de herramientas especializadas para la evaluación de riesgos y vulnerabilidades. Estas herramientas ayudan a identificar posibles amenazas, puntos débiles en la infraestructura de TI y posibles brechas de seguridad. Algunas de las categorías principales de herramientas incluyen:

Escáneres de vulnerabilidades: Estas herramientas escanean la infraestructura de TI en busca de vulnerabilidades conocidas en sistemas operativos, aplicaciones y servicios. Identifican posibles puntos de entrada para los atacantes y proporcionan recomendaciones para solucionar las vulnerabilidades encontradas. Ejemplos de escáneres de vulnerabilidades incluyen Nessus, *OpenVAS y Qualys*. [2]

Herramientas de pruebas de penetración: También conocidas como "pentesting tools", estas herramientas simulan ataques cibernéticos para identificar y explotar vulnerabilidades en sistemas y redes. Los *pentesters* pueden utilizar estas herramientas para evaluar la seguridad de una organización desde la perspectiva de un atacante real. Ejemplos incluyen *Metasploit, Burp Suite y Nmap*. [3]

Herramientas de análisis de código: Estas herramientas examinan el código fuente de aplicaciones y software en busca de posibles vulnerabilidades de seguridad, como errores de programación y prácticas inseguras. Ayudan a identificar y corregir problemas de seguridad en las fases de desarrollo y pruebas. Ejemplos incluyen

Veracode, Checkmarx y Fortify. [4]

Herramientas de gestión de vulnerabilidades: Estas herramientas permiten a las organizaciones gestionar y priorizar las vulnerabilidades identificadas, realizar un seguimiento del progreso de las correcciones y generar informes detallados sobre el estado de la seguridad de la infraestructura de TI. Ejemplos incluyen *Tenable.io, Rapid7 InsightVM y Nexpose.* [5]

Herramientas de gestión de riesgos: Estas herramientas ayudan a las organizaciones a evaluar y gestionar los riesgos de seguridad cibernética de manera integral, teniendo en cuenta factores como la probabilidad de ocurrencia, el impacto potencial y la mitigación de riesgos. Ejemplos incluyen *RSA Archer, RiskLens y FAIR.* [6]

Estas son solo algunas de las muchas herramientas disponibles en el mercado de la ciberseguridad para la evaluación de riesgos y vulnerabilidades. La elección de las herramientas adecuadas depende de las necesidades específicas de cada organización, el entorno tecnológico y los objetivos de seguridad. Es importante evaluar cuidadosamente las opciones disponibles y seleccionar las herramientas que mejor se adapten a las necesidades y recursos de la empresa.

V. TIPO DE DISPOSITIVOS EN EL MERCADO PARA LA PREVENCIÓN DE CIBER AMENAZAS:

En el mercado de la ciberseguridad, hay una variedad de dispositivos diseñados específicamente para la prevención de ciberamenazas. Estos dispositivos se utilizan para proteger las redes, sistemas y dispositivos contra una amplia gama de amenazas cibernéticas, como *malware*, ataques de denegación de servicio (DDoS), intrusiones y fugas de datos. Algunos de los tipos de dispositivos más comunes incluyen:

Hardware de red: Incluye *routers*, *switches*, *firewalls*, y dispositivos de detección de intrusiones (IDS) y prevención de intrusiones (IPS).

Software de seguridad: Como programas antivirus, cortafuegos, sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y software de cifrado de datos.

Dispositivos de autenticación: Como *tokens* de seguridad, tarjetas inteligentes, biométricos (lectores de huellas dactilares, reconocimiento facial) para garantizar la autenticación adecuada de usuarios.

Servicios de seguridad en la nube: Almacenamiento seguro, protección de correo electrónico, servicios de autenticación multifactor (MFA), etc.

Estos son solo algunos ejemplos de los dispositivos disponibles en el mercado para la prevención de ciber amenazas. La elección de dispositivos específicos dependerá de las necesidades de seguridad de la organización, el entorno tecnológico y el presupuesto disponible. Es importante evaluar cuidadosamente las opciones y seleccionar los dispositivos que mejor se adapten a las necesidades de seguridad y recursos de la empresa.

VI. MARCOS DE REFERENCIA Y ESTÁNDARES A SEGUIR:

Existen varios marcos y estándares ampliamente reconocidos en el campo de la ciberseguridad que pueden ayudar a las empresas a evitar riesgos y vulnerabilidades. Estos marcos y estándares proporcionan directrices y mejores prácticas para el diseño, implementación y gestión de programas de seguridad cibernética efectivos. Algunos de los más recomendados incluyen:

ISO/IEC 27001: Este estándar establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Proporciona un enfoque sistemático para identificar, gestionar y mitigar los riesgos de seguridad de la información en una organización. ISO/IEC 27001 es ampliamente reconocido internacionalmente y se puede adaptar a organizaciones de cualquier tamaño y sector. [8]

NIST *Cybersecurity Framework:* Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., este marco ofrece una serie de directrices, estándares y prácticas recomendadas para mejorar la ciberseguridad de una organización. Se basa en cinco funciones principales: identificar, proteger, detectar, responder y recuperarse, y puede adaptarse a diversos sectores y niveles de madurez en seguridad cibernética. [9]

COBIT *(Control Objectives for Information and Related Technologies)*: COBIT es un marco de gestión y control que proporciona un conjunto de prácticas y objetivos para la gobernanza de TI y la gestión de riesgos. Ayuda a las organizaciones a alinear sus objetivos de negocio con la tecnología de la información y a garantizar un uso adecuado y seguro de los recursos tecnológicos.[10]

CIS *Controls:* Desarrollados por el Center for Internet Security (CIS), estos controles son un conjunto de prácticas recomendadas para mejorar la ciberseguridad de una organización. Se dividen en tres

grupos: controles básicos, controles clave y controles avanzados, y cubren áreas como la seguridad de redes, sistemas, datos y usuarios. [11]

PCI DSS *(Payment Card Industry Data Security Standard):* Este estándar establece los requisitos para proteger la información de tarjetas de pago y garantizar la seguridad de las transacciones con tarjeta de crédito. Es aplicable a cualquier organización que almacene, procese o transmita datos de tarjetas de pago, y ayuda a prevenir el fraude y el robo de datos de tarjetas de crédito. [12]

GDPR *(General Data Protection Regulation):* Este reglamento de la Unión Europea establece normas para proteger la privacidad y los datos personales de los ciudadanos de la UE. Se aplica a todas las organizaciones que recopilan, procesan o almacenan datos personales de individuos en la UE, y establece requisitos estrictos para la protección de datos y la notificación de violaciones de seguridad. [13]

Estos marcos de trabajo no son excluyentes entre si e implementar y cumplir con estos marcos y estándares puede ayudar a las empresas a fortalecer su postura de seguridad cibernética, reducir los riesgos y mitigar las vulnerabilidades. Es importante evaluar las necesidades específicas de seguridad de cada organización y seleccionar los marcos y estándares más adecuados para sus objetivos y requisitos de cumplimiento.

VII. DISEÑO DE UN PLAN PARA MEJORAR LA SEGURIDAD DE LA COMUNICACIÓN DE DATOS A TRAVÉS DE INTERNET

Para empezar a diseñar un plan efectivo para mejorar la seguridad informática dentro de las empresas, es esencial seguir un enfoque estructurado y holístico.

Antes de comenzar a elaborar el plan de ciberseguridad de la empresa, es crucial comprender su situación actual en cuanto a seguridad cibernética. Esto implica examinar detenidamente los protocolos y políticas de seguridad existentes, así como identificar cualquier servicio de tecnología de la información (TI) externalizado. Además, es importante conocer qué software de seguridad se está utilizando actualmente y cómo se están implementando las medidas de protección de datos y sistemas. Este proceso proporciona una visión clara de las prácticas de seguridad actuales de la empresa y establece una base sólida para desarrollar un plan de ciberseguridad efectivo y adaptado a sus necesidades específicas.

Se debe empezar realizando una evaluación exhaustiva de la infraestructura de red y sistemas de la organización para identificar

vulnerabilidades y riesgos en la comunicación de datos Esto puede incluir la revisión de políticas de seguridad existentes, análisis de vulnerabilidades, pruebas de penetración y evaluación del cumplimiento normativo.

Algunos métodos que se pueden utilizar para obtener una visión completa de la postura de seguridad y desarrollar estrategias efectivas para proteger los activos de información de las empresas contra las amenazas cibernéticas son los siguientes:

Análisis de riesgos: Este método identifica y evalúa los riesgos potenciales para los activos de información de la empresa. Se examinan amenazas, vulnerabilidades y posibles impactos para determinar la probabilidad de ocurrencia y la gravedad de los riesgos. Es de las primeras labores a realizar pues la gestión efectiva de riesgos prioriza las áreas que deben atenderse primero pues resultan más críticas para la organización.

Pruebas de penetración: Estas pruebas implican simular ataques cibernéticos contra los sistemas de la empresa para identificar vulnerabilidades y evaluar la eficacia de las medidas de seguridad.

La utilización de herramientas de evaluación de seguridad continua ofrece una serie de beneficios y es de gran importancia para garantizar la protección efectiva de los activos y datos de una organización.

Estas herramientas pueden identificar de manera proactiva posibles vulnerabilidades en la infraestructura de TI y en las aplicaciones, antes de que puedan ser explotadas por los atacantes. Esto permite a las organizaciones tomar medidas preventivas para mitigar los riesgos antes de que se conviertan en problemas mayores.

Auditorías de seguridad: Las auditorías de seguridad involucran una revisión exhaustiva de las políticas, procedimientos y controles de seguridad implementados en la empresa. Se comparan las prácticas de seguridad con estándares y regulaciones establecidos para identificar posibles áreas de mejora.

Análisis de vulnerabilidades: Este método implica escanear la infraestructura tecnológica en busca de vulnerabilidades conocidas, como fallos de software o configuraciones inseguras. Se utiliza software especializado para identificar y clasificar las vulnerabilidades encontradas.

Evaluación de cumplimiento: Se centra en garantizar que la empresa cumpla con las regulaciones y estándares de seguridad relevantes en su industria. Se revisan las políticas, procedimientos y

controles de seguridad para asegurarse de que estén alineados con los requisitos legales y regulatorios.

El desarrollo de políticas y procedimientos de seguridad es muy importante, se deben crear políticas y procedimientos de seguridad robustos que aborden aspectos clave de la comunicación de datos en el Internet, como el cifrado de datos, la autenticación de usuarios, el control de acceso y la gestión de incidentes.

Muchos estándares y regulaciones de seguridad, como ISO/IEC 27001, PCI DSS y GDPR, requieren la implementación de controles de seguridad continuos y la evaluación regular de la postura de seguridad de una organización. El uso de herramientas de evaluación continua puede ayudar a las empresas a cumplir con estos requisitos y evitar posibles sanciones y multas.

Revisión de arquitectura de seguridad: Esta evaluación se enfoca en examinar la arquitectura de la red y los sistemas de la empresa para identificar posibles debilidades en el diseño que puedan ser explotadas por los atacantes.

Se deben implementar controles técnicos y organizativos para proteger la comunicación de datos en línea. Esto puede incluir la instalación de *firewalls*, sistemas de detección de intrusiones (IDS/IPS), *software* antivirus, cifrado de datos y autenticación multifactor.

Por otro lado, si se cuenta con estos dispositivos se deben mantener actualizados, esto es crucial para garantizar la seguridad, el rendimiento y la fiabilidad de las operaciones de una organización.

Las actualizaciones de software y firmware frecuentes suelen incluir correcciones de seguridad que abordan vulnerabilidades conocidas. Mantener los sistemas actualizados ayuda a proteger contra ataques cibernéticos y *malware* al cerrar brechas de seguridad y parchear posibles puntos de entrada para los atacantes.

Lo anterior debe ir de la mano con una efectiva inteligencia de amenazas para que la organización esté al tanto de las tendencias de los ataques recientes alrededor del mundo.

Simulacros de incidentes: Estos ejercicios simulan situaciones de crisis, como un ciberataque o una violación de datos, para evaluar la capacidad de respuesta de la empresa y su capacidad para gestionar y mitigar el impacto de tales eventos.

También se debe proporcionar formación regular sobre seguridad de la información a todos los empleados, incluyendo buenas prácticas

para la comunicación segura de datos en línea y cómo reconocer y responder a posibles amenazas.

Es de igual importancia establecer sistemas de monitorización continua para detectar y responder rápidamente a posibles incidentes de seguridad en la comunicación de datos. Desarrollar un plan de respuesta a incidentes detallado que describa los pasos a seguir en caso de una brecha de seguridad.

Luego se deben establecer objetivos claros y alcanzables para mejorar la seguridad de la empresa. Estos objetivos deben alinearse con las necesidades específicas de la organización, teniendo en cuenta su tamaño, industria y nivel de riesgo.

Basados en la información recopilada en las fases anteriores, es crucial establecer los objetivos que se deben alcanzar con el plan de ciberseguridad. Entre los objetivos comunes de un plan de ciberseguridad para empresas se incluyen minimizar los riesgos, implementar sistemas de respuesta rápida, utilizar métodos efectivos de detección de amenazas y establecer un proceso de mejora continua que garantice que la empresa siempre esté buscando formas de mejorar e incrementar su nivel de ciberseguridad. Estos objetivos son fundamentales para fortalecer la postura de seguridad de la empresa y proteger sus activos y datos críticos contra las crecientes amenazas cibernéticas.

Luego se deben definir las acciones específicas que se deben realizar para alcanzar los objetivos de ciberseguridad establecidos previamente. Estas medidas pueden ser de corto, mediano y largo plazo, adaptándose a las necesidades y particularidades de cada servicio o proceso. Estas acciones deben tener un inicio y un fin y deben ser medibles para poder analizar su implementación y mejora continua. Algunas de las acciones a definir incluyen:

- Implementación de protocolos de ciberseguridad, como la aplicación de contraseñas seguras y la gestión adecuada de permisos de usuario.
- Actualización y parcheo regular de sistemas y software para cerrar posibles vulnerabilidades.
- Instalación y configuración de *firewalls* y sistemas de detección

de intrusiones para proteger la red empresarial.

- Establecimiento de políticas de acceso y control de datos para garantizar la confidencialidad y la integridad de la información.
- Realización de copias de seguridad periódicas y almacenamiento seguro de datos críticos.
- Implementación de medidas de prevención y detección de *malware*, como software antivirus y antimalware.
- Capacitación y concienciación regular del personal sobre prácticas seguras de navegación y manipulación de datos.
- Establecimiento de un proceso de gestión de incidentes para responder de manera efectiva a posibles violaciones de seguridad.
- Evaluación periódica de la infraestructura de seguridad y realización de pruebas de penetración para identificar posibles vulnerabilidades.
- Colaboración con proveedores externos de servicios de seguridad cibernética cuando sea necesario para reforzar la protección.

Estas acciones deben ser detalladas y adaptadas a las necesidades específicas de la empresa, considerando factores como el tamaño de la organización, el sector de la industria y el nivel de riesgo percibido. Deben establecer roles y responsables de las acciones, así como toda la infraestructura de comunicación efectiva de ejecución y reacción ante ataques.

Hay que tomar en cuenta que, antes de pasar a la implementación, es necesario priorizar acciones necesarias, basada, en el grado de riesgo al que se enfrenta la empresa. Por ejemplo, es prioritario implementar un sistema de copias de seguridad periódicas y automatizadas, ya que garantiza la recuperación y el acceso a la información crítica de la empresa en caso de incidentes.

La etapa de implementación es donde se llevan a cabo todas las acciones definidas previamente y priorizadas en el plan de ciberseguridad. En esta fase, se materializa en la operación tecnológica el trabajo realizado anteriormente. Es esencial designar a los responsables de cada proyecto o implementación para garantizar una mejor organización y asegurar que se disponga de los recursos necesarios para una implantación eficiente. Esto permite una ejecución ordenada y efectiva de las medidas de seguridad planificadas, asegurando que se implementen correctamente y se alcancen los objetivos establecidos en el plan de ciberseguridad.

Una vez finalizada la implementación, es crucial contar con un sistema de monitoreo y control que permita realizar un seguimiento preciso y en tiempo real. Esto facilita la detección temprana de problemas o desviaciones del plan de ciberseguridad, lo que permite

tomar medidas correctivas de manera oportuna para resolverlos. Este sistema de monitoreo y control garantiza que la seguridad de la empresa se mantenga efectiva y adaptada a cualquier cambio en el entorno cibernético, asegurando así la protección continua de los activos y datos críticos de la organización.

Por último, realizar evaluaciones periódicas de la seguridad de la comunicación de datos y revisar y actualizar regularmente las políticas y procedimientos de seguridad. Utilizar los resultados de estas evaluaciones para identificar áreas de mejora y fortalecer aún más la seguridad de la comunicación de datos en línea.

Al construir y seguir un plan de seguridad de este tipo, las organizaciones pueden mejorar significativamente la seguridad de su comunicación de datos a través de Internet y mitigar los riesgos y vulnerabilidades asociados.

VIII. Conclusiones

Los crecientes ataques de ciberseguridad en Costa Rica representan una preocupación significativa para empresas, instituciones y ciudadanos por igual. En los últimos años, el país ha experimentado un aumento en la frecuencia y la sofisticación de los ataques cibernéticos, que van desde el *phishing* y el *ransomware* hasta intrusiones más complejas en sistemas informáticos.

Estos ataques pueden tener diversas consecuencias negativas, como la pérdida de datos confidenciales, interrupciones en las operaciones comerciales, daños a la reputación de las empresas y pérdidas financieras. Además, los ataques cibernéticos pueden afectar a sectores críticos como la salud, las finanzas y el gobierno, lo que plantea preocupaciones adicionales sobre la seguridad nacional y la privacidad de los ciudadanos.

Para hacer frente a esta creciente amenaza, es fundamental que las organizaciones y las autoridades gubernamentales en Costa Rica tomen medidas proactivas para mejorar su postura de ciberseguridad. Esto incluye la implementación de medidas de seguridad robustas, la educación y concienciación del personal sobre las mejores prácticas de seguridad cibernética, y la colaboración con socios internacionales para compartir información y recursos en la lucha contra el cibercrimen.

Además, es importante que los individuos y las empresas tomen medidas para protegerse contra los ataques cibernéticos, como mantener sus sistemas y software actualizados, utilizar contraseñas seguras, evitar hacer clic en enlaces o archivos adjuntos sospechosos, y realizar copias de seguridad regulares de sus datos importantes.

El diseño e implementación de un plan de ciberseguridad efectivo es fundamental para proteger los activos y datos críticos de una empresa en un entorno cibernético cada vez más complejo y dinámico.

Estos planes son esenciales para la protección integral de una organización en el entorno digital actual. Proporcionan una estructura sólida para salvaguardar los activos digitales de la empresa, así como para mitigar los riesgos asociados con las crecientes amenazas cibernéticas. Además, garantiza la continuidad de las operaciones empresariales al reducir la probabilidad de interrupciones graves causadas por incidentes de seguridad. Asimismo, ayuda a la empresa a cumplir con las regulaciones y estándares de seguridad pertinentes, lo que a su vez protege su reputación y evita posibles sanciones legales. En última instancia, permiten a la organización adaptarse y responder de manera proactiva a las amenazas emergentes, asegurando su resiliencia en un entorno digital en constante evolución.

En resumen, la importancia de un plan de ciberseguridad efectivo radica en su capacidad para proteger los activos críticos de la empresa, asegurar las comunicaciones de datos críticos, garantizar la continuidad del negocio, cumplir con las regulaciones, promover una cultura de seguridad y proporcionar un marco claro para la gestión de la seguridad cibernética.

IX. Referencias

[1] Summa, R. (2023, 8 febrero). *7 de cada 10 empresas costarricenses ha invertido o invierte actualmente en ciberseguridad - Revista Summa*. Revista Summa. https://revistasumma.com/7-de-cada-10-empresas-costarricenses-ha-invertido-o-invierte-actualmente-en-ciberseguridad/

[2]]Chavez, J. J. S. (2024, 13 febrero). *Escáneres de vulnerabilidades: ¿Cuáles son los mejores?* https://www.deltaprotect.com/blog/mejores-escaneres-de-vulnerabilidades

[3] Rootstack. (s. f.-b). *Las 5 mejores herramientas de pruebas de penetración*. Rootstack. https://rootstack.com/es/blog/las-5-mejores-herramientas-de-pruebas-de-penetracion

[4] *¿Cómo funcionan las herramientas de seguridad DAST, SAST y SCA? – Codster*. (s. f.-b). https://codster.io/blog/herramientas-de-seguridad-dast-sast-y-sca/

[5] *La plataforma Insight de Rapid7 unifica la gestión de vulnerabilidades con el análisis del comportamiento del usuario*.

(s. f.). Ingecom. https://www.ingecom.net/es/prensa/104/la-plataforma-insight-de-rapid7-unifica-la-gestion-de-vulnerabilidades-con-el-analisis-del-comportamiento-del-usuario/

[6] Su organización necesita una mejor gestión de riesgos. ¿Qué software puede ayudarte a conseguirlo? (2024, 26 enero). https://es.linkedin.com/advice/0/your-organization-needs-better-risk-management-5ze3f?lang=es

[7] Kosutic, D. (s. f.). ¿Qué es norma ISO 27001? 27001Academy. https://advisera.com/27001academy/es/que-es-iso-27001/

[8] ¿Qué es el Marco de Ciberseguridad del NIST? | IBM. (s. f.). https://www.ibm.com/es-es/topics/nist#:~:text=El%20Instituto%20Nacional%20de%20Est%C3%A1ndares,en%20metrolog%C3%ADa%2C%20normas%20y%20tecnolog%C3%ADa.

[9] Nextech, S. (2021, 12 mayo). ¿Qué es COBIT y para qué sirve? Nextech. https://nextech.pe/que-es-cobit-y-para-que-sirve/https://nextech.pe/que-es-cobit-y-para-que-sirve/

[10] ManageEngine. (s. f.). ¿Qué son y cómo implementar los Controles de CIS? | Definición de Controles CIS o CIS Controls (Cis Ciberseguridad) - ManageEngine. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

[11] Acosta, D. (s. f.). ¿Qué es PCI DSS? | PCI Hispano. https://www.pcihispano.com/que-es-pci-dss/

[12] GDPR: Lo que debes saber sobre el reglamento general de protección de datos. (s. f.). https://www.powerdata.es/gdpr-proteccion-datos