ANÁLISIS DEL ESTADO DE CIBERSEGURIDAD EN LAS ORGANIZACIONES COLOMBIANAS Y LA EFECTIVIDAD DE LAS POLÍTICAS GUBERNAMENTALES DE SEGURIDAD DIGITAL.

DIANA PAOLA ORTIZ GALEANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2023

ANÁLISIS DEL ESTADO DE CIBERSEGURIDAD EN LAS ORGANIZACIONES COLOMBIANAS Y LA EFECTIVIDAD DE LAS POLÍTICAS GUBERNAMENTALES DE SEGURIDAD DIGITAL.

DIANA PAOLA ORTIZ GALEANO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Yenny Stella Nuñez Álvarez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este trabajo a Dios, porque me ha otorgado la oportunidad de estudiar y presentar esta monografía. A mis padres, mi más profundo agradecimiento por su apoyo incondicional y amor constante a lo largo de mi camino académico. Han sido mi roca y apoyo, enseñándome el valor de la calma y dedicación para enfocarme en mis estudios. Este logro es también suyo.

AGRADECIMIENTOS

Agradezco a los tutores por su dedicación y tiempo, por ser parte fundamental en este camino. A la Universidad Nacional Abierta y a Distancia UNAD, agradezco su innovadora metodología de estudio virtual que me ha permitido equilibrar el trabajo y los estudios. Además, agradezco enormemente el apoyo incondicional de mis amigos y mi pareja; su aliento y comprensión fueron un pilar fundamental para culminar este trabajo. Su respaldo ha significado todo en este proceso.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZA CIBERNETICA: Es una acción que busca explotar vulnerabilidades dentro de los sistemas informáticos con el objetivo de afectar la confidencialidad, disponibilidad e integridad de la información.

AUTENTICACION: Es el proceso de verificación de identidad de un usuario o dispositivo para poder acceder a los recursos que contiene un sistema.

CIBERSEGURIDAD: Es un conjunto de procedimientos que buscan proteger la información que este almacenada en diferentes sistemas, redes o equipos, por eso existen diferentes herramientas para poder evitar posibles amenazas cibernéticas.

CIBERDELINCUENCIA: Son actividades ilegales que se llevan a cabo por medio del uso de diferentes tecnologías para cometer delitos tales como: robo de información, fraude, espionaje cibernético etc.

CONFIDENCIALIDAD: Es la protección de los datos o información sensible para que la información no se vea comprometida por accesos no autorizados en los diferentes sistemas.

DISPONIBILIDAD: Se refiere a que la información esté disponible a los usuarios autorizados para cuando se requiera el acceso.

INTEGRIDAD: La información debe mantenerse intacta por lo cual no debe ser modificada por usuarios no autorizados que pueden alterar los datos.

MALWARE: Es un código malicioso que sirve para dañar sistemas o robar información.

VULNERABILIDAD: Es una debilidad que puede ser encontrada en los sistemas informáticos y puede ser explotada por los atacantes para causar daños o aprovechar el fallo con el fin de obtener acceso a la información.

SEGURIDAD DE LA INFORMACIÓN: Medidas que tienen como objetivo la protección de la integridad, disponibilidad y confidencialidad de la información en una organización.

SEGURIDAD INFORMATICA: Son medidas para proteger la información y los sistemas que se manejen en una organización.

RESUMEN

En la actualidad las organizaciones sufren de constantes ciberataques y se han vuelto en un objetivo para los ciberdelincuentes debido a que buscan robar la información de las organizaciones ya sea para modificarla, secuestrar los datos o dañar su reputación ante las partes interesadas.

Es necesario que en las organizaciones se le dé prioridad a la ciberseguridad en el punto de vista interno y externo porque se debe buscar que los datos de clientes, empleados o proveedores que se almacenen en los diferentes sistemas estén protegidos.

En las organizaciones se debe contar con procedimientos que permitan tener una autenticación segura para garantizar los accesos autorizados en los diferentes sistemas que se manejen, es fundamental que los sistemas o software se encuentren actualizados para evitar tener vulnerabilidades que puedan ser detectadas por los ciberdelincuentes y explotadas causando graves daños en la información.

Es importante y necesario que se cuente con medidas de seguridad adecuadas, cabe recordar que la ciberseguridad es un tema crucial y que está en constante evolución por eso las organizaciones deben contar con copias de seguridad para el respaldo de la información, manejar un control de acceso en las plataformas o sistemas que manejen servicios críticos o datos sensibles y realizar un monitoreo de las amenazas que se pueden presentar para mitigar el impacto.

ABSTRACT

Currently organizations suffer from constant cyber attacks and have become a target for cybercriminals because they seek to steal information from organizations either to modify it, hijack the data or damage their reputation with stakeholders.

It is necessary that organizations give priority to cybersecurity in the internal and external point of view because it must seek to ensure that the data of customers, employees or suppliers stored in different systems are protected.

In organizations must have procedures that allow secure authentication to ensure authorized access to the different systems that are handled, it is essential that the systems or software are updated to avoid vulnerabilities that can be detected by cybercriminals and exploited causing serious damage to information.

It is important and necessary to have adequate security measures, it is important to remember that cybersecurity is a crucial issue and is constantly evolving so organizations must have backup copies to back up information, manage access control in platforms or systems that handle critical services or sensitive data and monitor the threats that may occur to mitigate the impact.

INTRODUCCIÓN

Actualmente es indispensable para las organizaciones el uso de las tecnologías, de la misma manera aumenta la preocupación por los ciberataques de acuerdo con Ospina[1] , la tecnología es una dependencia y una vulnerabilidad que pueden afectar el correcto funcionamiento del servicio en una organización y de los sistemas implementados debido a que la información se encuentra almacenada o gestionada en la nube o directamente en los dispositivos dependiendo del alcance de las organizaciones, de tal modo es un objetivo para el ciber atacante que busca robar, modificar o dañar la reputación e información de las organizaciones.

Por esta razón es necesario revisar en diversas fuentes bibliográficas sobre la implementación de buenas prácticas, controles, normatividades y métodos correspondientes a la ciberseguridad, ya que resulta vital que las organizaciones cuenten con medidas actualizadas para mitigar los riesgos y amenazas.

En esta monografía se abordará el tema de ciberseguridad en las organizaciones de todos los tamaños y sectores para identificar los riesgos y amenazas más comunes que se presentan debido a que nadie está exento de ser atacado, de la misma forma se analizara como se puede implementar políticas y estrategias que permitan proteger la información.

En definitiva, se brindará una visión actualizada de la ciberseguridad y porque la importancia de esta para proteger la información de las organizaciones con el objetivo de que pueda servir como base para conocimiento de medidas efectivas de seguridad.

[1] OSPINA DÍAZ, M. R., & SANABRIA RANGEL, P. E. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista criminalidad. Disponible en: https://biblat.unam.mx/hevila/Revistacriminalidad/2020/vol62/no2/5.pdf

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Es frecuente la presencia ataques cibernéticos en los diferentes sectores a los que pertenecen las organizaciones privadas o públicas, cómo indica Ulloa [2], un ataque cibernético puede llegar a afectar a corto o largo plazo a una organización donde deja secuelas de forma negativa para las partes interesadas, sin importar si es mediana o grande empresa, siempre y cuándo cuente con información sensible, sistemas vulnerables o personal poco capacitado para el manejo correcto de la información, permitiendo ser vulnerable a amenazas y ataques cibernéticos.

Para una organización debe ser importante conocer que ataques cibernéticos se presentan y cuál es su origen, la principal causa de los problemas de seguridad es el desconocimiento de los riesgos que se encuentran en los diferentes sistemas. las empresas deben tener conocimiento de los riesgos más comunes cómo: la falta de implementación de medidas adecuadas de Ciberseguridad y concientización del personal con el fin de proteger la información.[3]

A todo esto, el ciberdelincuente aprovecha las vulnerabilidades que tiene una organización para robar sus datos o dañar la reputación de la misma por falta de implementación de políticas, generando daños en la integridad, confidencialidad y disponibilidad de la información.

“Colombia ha presentado grandes riesgos producidos por ciberataques, el más reciente fue en 2018 al registrarse 28.000 ataques de robots a las páginas de la registraduría nacional en jornada electoral. en 2019 se registraron 48 billones de intentos de ciberataques a un sistema bancario. después en 2021 se registro 11.200 millones de intentos de ciberataques datos informados por Fortinet y por último en 2022 nuevamente se recibió 400.000 ataques en una semana a la página de la registraduría nacional.”[4]

---

[2] ULLOA MORA, Jimmy. Automatización, ciberseguridad y ciencia de datos: la nueva estrategia empresarial. [en línea]. p.36

[3] OLAYA OLIVEROS, Alexander. Ataques cibernéticos. [en línea]. 2021. pp.15-36

[4] SOLANO, Brigadier General Ricardo Charry. El riesgo de los ciberataques para Colombia. [en línea]. 2022. Disponible en Internet: https://esici.edu.co/wp-content/uploads/2023/02/Boletin_05_V4.pdf

Durante el año 2022 Colombia a pesar de que cuenta con ciberdefensa y Estrategia nacional de ciberseguridad es considerado como un país vulnerable a los ciberataques siendo uno de los más atacados en los últimos años.

Dado que se presenta esta situación es necesario profundizar sobre las estrategias de ciberseguridad que se están utilizando en las organizaciones y cómo se está implementando las políticas y procedimientos para que sean eficaces para prevenir o mitigar los riesgos de ataques cibernéticos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se implementa la ciberseguridad en las organizaciones colombianas y cuáles son las medidas efectivas para proteger los datos contra los riesgos cibernéticos?

2. JUSTIFICACIÓN

En las organizaciones se considera que el activo más vulnerable son las personas debido a que se vuelven un objetivo para el robo de información, siendo usada la ingeniería social de acuerdo con Fernández[5], la ingeniera social se basa en ganar la confianza de una persona, utilizar un perfil falso y aprovecharse de la ingenuidad de las personas. En este sentido las organizaciones necesitan comenzar a implementar metodología para gestionar la seguridad de la información por medio de políticas de seguridad, herramientas de control y monitoreo, adicionalmente capacitar al personal interno sobre la importancia de la seguridad cibernética ya que en la mayoría de ocasiones dentro de la misma organización puede existir las vulnerabilidades, se puede sufrir ataques por ingeniería social, accesos no autorizados o suplantación de identidad.

"En la actualidad todas las organizaciones necesitan estar al tanto de las amenazas cibernéticas porque estás han crecido de manera exponencial y se debe evitar que estos puedan dejar daños de alto impacto que afecten a la prestación de servicios".[6]

De modo que es necesario comenzar a implementar herramientas o metodologías que existen hoy en día para prever un ataque o mitigar los riesgos, por eso se realizara una investigación por medio de diferentes fuentes de búsqueda para conocer cómo proteger la información y contar con seguridad cibernética en las organizaciones con el fin de aplicar buenas prácticas para evitar ser parte del riesgo.

"Los ciberdelincuentes usan diferentes tácticas tecnológicas para infiltrarse a los puntos débiles que tienen las organizaciones dejando en evidencia el desconocimiento de la ciberseguridad, por eso algunas organizaciones han promovido el uso de estrategias para afrontar las amenazas de ciberseguridad."[7]

---

[5] FERNÁNDEZ, Luis Jonalber, et al. Incidencia del factor humano en la seguridad de la información de las organizaciones públicas de categoría 6. p.29

[6] REALPE, M.; CANO, J. Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. [en línea]. 2020. Disponible en Internet: https://www.researchgate.net/profile/Jeimy-Cano-M/publication/340465740_Amenazas_Ciberneticas_a_la_Seguridad_y_Defensa_Nacional_Reflexiones_y_perspectivas_en_Colombia/links/5e8fb6dc92851c2f52910dce/Amenazas-Ciberneticas-a-la-Seguridad-y-Defensa-Nacional-Reflexiones-y-perspectivas-en-Colombia.pdf

[7] MONTOYA, Yan Cornejo; VERDEZOTO, Víctor Hugo; RAMÍREZ, Andrea Villacis. Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad. [en línea]. 2019. Disponible en Internet: http://www.imjst.org/wp-content/uploads/2019/02/IMJSTP29120135.pdf

Además, que son necesarias estas estrategias para proteger su información y evitar verse afectados por el robo de sus datos y lo que puedan lograr hacer los ciber atacantes con esta información, esta investigación se realizara de forma global de los diferentes casos presentados de ciberataques y ciberseguridad, donde se han presentado aumento de incidentes cibernéticos cómo en:

España, en 2020 se dio un reporte por parte de INCIBE-CERT donde indican que gestionaron 133.155 incidentes de ciberseguridad entre los cuales de organizaciones y ciudadanos fueron 106.466 incidentes, operadores estratégicos 1.190 incidentes y a la red académica e investigación 25.499, de tal manera que el 35% era malware, 32% otro tipo de ataques y 17.39% sistemas vulnerables [8].

El resultado de este trabajo contribuirá a que las organizaciones comprendan la importancia de la ciberseguridad en las organizaciones para fortalecer las medidas de seguridad, en definitiva, se busca dar a conocer cómo mejorar políticas y procedimientos, y que estas sean ajustadas o evaluadas para que se hagan conocer a los usuarios de una organización, cómo a sus clientes y proveedores.

[8] INCIBE [Sitio web]. INCIBE gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020. Disponible en Internet: https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-130000-incidentes-ciberseguridad-durante-el-ano-2020

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el estado de ciberseguridad de las organizaciones colombianas y la efectividad de las políticas y normativas gubernamentales para la seguridad digital a través de la consulta documental y el análisis de fuentes especializadas.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar, a través de informes de seguridad, los riesgos y amenazas más frecuentes que han afectado a las organizaciones en Colombia y evaluar su impacto en la continuidad del negocio.
- Determinar la efectividad de las políticas, normativas y lineamientos generados por el gobierno nacional de Colombia para garantizar la seguridad digital en las organizaciones.
- Identificar los métodos y estrategias de ciberseguridad que puedan fortalecer y complementar las políticas de seguridad digital en Colombia.
- Evaluar y presentar mecanismos y buenas prácticas para la gestión de riesgos, la prevención y la defensa de la seguridad digital en organizaciones.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Importancia de la ciberseguridad en las organizaciones

La ciberseguridad es una parte de la seguridad informática, la ciberseguridad está enfocada al ciber espacio por lo que permite que se tenga reducción de riesgos de la información que se maneja en los dispositivos o plataformas y está centrada en el procesamiento, almacenamiento y transporte de la información.

Por otra parte, la ciberseguridad permite que se pueda garantizar la protección de la información, cumplir con los requisitos legales establecidos en diferentes sectores; siendo de gran importancia porque puede mejorar la continuidad del negocio de una organización minimizando los riesgos o amenazas cibernéticas que se puedan presentar.

Cómo indica Manrique[9] los pilares de protección de los activos son muy importantes como la disponibilidad ya que se debe contar con un acceso de usuarios autorizados para acceso a la información, garantizar la integridad para que la información no sea alterada o dañada y la confidencialidad para que no se divulgue procesos no autorizados.

Tabla 1. Mecanismo de la ciberseguridad

Mecanismo	Descripción
Seguridad de la información	• Confidencialidad • Integridad • Disponibilidad
Seguridad de las aplicaciones	• Procesos • Componentes • Software • Resultados • Datos
Seguridad de la red	• Diseño • Implementación • Operación

[9] MANRIQUE Reyna, V. H. Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un instituto superior tecnológico público. pp.20-30

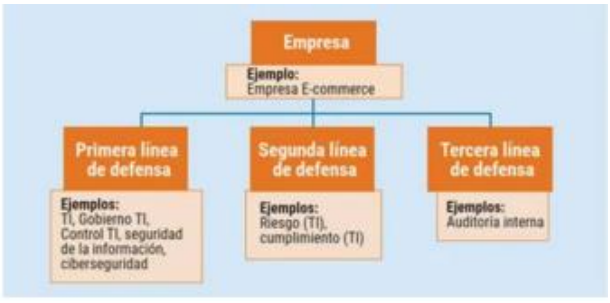
Seguridad de internet	• Servicios en internet seguro • Redes • Disponibilidad de servicios • Fiabilidad de servicios
Seguridad en la infraestructura	• Datacenter • Condiciones ambientales • Acceso Físico • Sitios Alternos

Fuente: MANRIQUE Reyna, V. H. (2022) Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un instituto superior tecnológico público. 26 p. https://repositorio.ucv.edu.pe/handle/20.500.12692/84954

En las organizaciones se debe comenzar a aplicar las diferentes metodologías o marcos de ciberseguridad con el fin de poder brindar aseguramiento tecnológico para poder tener la capacidad al evaluar los riesgos, definir políticas y procedimientos con el fin de mantener un plan de continuidad. Como indica Hernández[10] las organizaciones deben ir alineadas con los avances de la tecnología por lo que se debe buscar buenas prácticas de ciberseguridad como: COBIT, ITIL, NIST 800, 27001 entre otras.

Por otra parte, se debe tener en cuenta cómo funciona las líneas de defensa para aplicar en una organización con el fin de contar con aseguramiento de la infraestructura, contar con apoyo para identificación de riesgos y dar cumplimiento en las diferentes normatividades y por último contar con auditorias que permitan que se mejoren los procesos que se manejen en una organización.

Figura 1. Estructura de líneas de defensa.



Fuente: HERNANDEZ Holbert. (2022). Importancia de estructurar un Gobierno de

[10] HERNÁNDEZ GONZÁLEZ, Holber Steven. Importancia de Estructurar un Gobierno de Seguridad y Ciberseguridad en las Organizaciones. pp.1-6

Seguridad y Ciberseguridad en las organizaciones. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/12278

Cómo indica ISACA[11] existen diferentes roles para la seguridad de la información, todo depende de cada organización el rol que puede asignar, la cuál va de la mano con la ciberseguridad y gobierno, por lo que nos da un ejemplo cómo la siguiente estructura en la figura 2, donde se refleja la estructura que se puede manejar en un departamento de TI para poder trabajar en conjunto y poder dividir las diferentes tareas correspondientes para la administración del riesgo, analizar las infraestructuras y mantener monitoreo constante.

Figura 2. Estructura de un área TI

Fuente: ISACA. (2019). Roles de las tres líneas de defensa para la seguridad de la información y gobierno. Disponible en: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

4.1.2 Riesgos de una organización frente a ataques cibernéticos

Las organizaciones deben dar la prioridad a la ciberseguridad debido a los avances tecnológicos, de la misma forma como va avanzando los ataques cibernéticos. la ciberseguridad es considerada importante para todo tipo de organización de tal manera que es necesaria para poder evitar los riesgos por el gran impacto que estos dejan después de un ataque, se debe preparar a las partes interesadas para que tengan el conocimiento de cómo enfrentar un riesgo cibernético, cómo indica

[11] ISACA. [Sitio web]. Roles de las tres líneas de defensa para la seguridad de la información y gobierno. 2019. Disponible en: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

Ramírez[12] seis de cada diez organizaciones han sufrido de ataques cibernéticos en el último año.
Con el tiempo han avanzado las técnicas y los atacantes son más sofisticados por lo que se presentan de manera continua en Latinoamérica las ciber amenazas con el objetivo de alterar, destruir o sustraer la información con el fin de interrumpir o dañar la reputación en las organizaciones cómo indica CCN-CERT[13] existe el ciber espionaje, ciberdelito, ciberactivismo, ciberterrorismo, ciberguerra los cuales han tenido un crecimiento continuo llegando a afectar la confidencialidad, integridad y disponibilidad de la información.

Debido a que se presenta a diario en diferentes países ciberataques tales como malware, phishing, ransomware, ataques de fuerza bruta, ddos, etc. Se debe evaluar las aplicaciones, bases de datos, sistemas, activos, la seguridad de una infraestructura por lo que es necesario tener en cuenta que la ciberseguridad cómo indica Molina[14], es un conjunto de herramientas, políticas, controles de seguridad y directrices que sirven para proteger los activos de una organización y de los usuarios, garantizando proteger la seguridad de la información cuando se presenta un ciberataque y de ese modo al proteger los datos, permitirá que una empresa no llegue a perder su reputación o que llegue este tipo de amenazas a afectarla económicamente.

Durante el año 2022 según indica Rey[15], se reportaron 54.121 denuncias por ciberataques, además 10 empresas sufrieron de ataques cibernéticos estas estadísticas fueron brindadas por el centro cibernético de la política nacional, de tal forma que Colombia está entre los primeros países que ha sufrido mayor número de ataques, cuándo una empresa cuenta con procesos y controles adecuados podrá actuar de manera eficiente ante un intento de ataque para mitigar el riesgo.

[12] RAMÍREZ, Maricela; CORPORATIVA, Responsabilidad Social. EL CONCEPTO DE CIBERSEGURIDAD EN EL ÁMBITO ORGANIZACIONAL. [en línea]. Universidad de granada, 2022. Disponible en Internet: https://xxencuentro.aeca.es/wp-content/uploads/2022/09/43estudiante.pdf
[13] ROMERO, J. C. Ciberseguridad: Evolución y tendencias. [en línea]. 2021.bie3: Boletín IEEE, (23), 460-494.pp 11-15
[14] MOLINA, J. OROZCO, L. Vulnerabilidades de los Sistemas de Información: una revisión. [en línea]. Disponible en Internet: https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1
[15] PORTAFOLIO. REY, G. Helena. [Sitio web]. Por qué ha crecido la importancia de la ciberseguridad. 2023. Disponible en Internet: https://www.portafolio.co/economia/finanzas/ciberseguridad-aumenta-a-la-par-de-los-ataques-ciberneticos-579612

4.2 MARCO CONCEPTUAL

Ciberseguridad: es un conjunto de prácticas, estrategias y herramientas para proteger la información que se encuentra almacenada en los diferentes sistemas de posibles amenazas digitales cómo: robos, daños y ataques.[16]

Malware: es un software malicioso que es usado para dañar un sistema, servicio o red, cuándo se explota este software se extraen datos con el fin de engañar al objetivo, robar datos o tener control de los dispositivos para lanzar ataques DDoS e infectar equipos existen diferentes tipos de malware como: gusanos, scareware, ransomware, spyware y troyanos[17].

Bots: son robots maliciosos que pueden hackear cuentas, enviar correos no deseados, realizar diferentes operaciones malignas, estos bots pueden combinarse con una botnet para afectar los dispositivos de manera masiva y realizar ataques de esa manera, existen diferentes tipos de bots para: spam, archivos, chat, stuffing, DoS o DDoS, analizadores de vulnerabilidades o fraudulentos y monitoreo de tráfico.[18]

Ataques de Phishing: es el envió de correos por medio de técnicas para engañar a las víctimas donde el remitente se hace pasar por una organización real y de esa forma gana la confianza del destinatario, dentro de este tipo de ataque se derivan otros ataques como smishing y vishing.[19]

Ransomware: Es un software malicioso que puede cifrar los archivos o bloquear dispositivos después pide un rescate a cambio para descifrar la información. Existen diferentes tipos de ransomware como: cifrador, bloqueador, scareware, RaaS.[20]

Amenazas persistentes avanzadas: son amenazas que usan técnicas de hackeo avanzadas para obtener acceso, infiltrarse e intensificar el acceso, mantenerse dentro del sistema para acceder a otros dispositivos, usando la información y manteniendo el proceso en funcionamiento en caso de acceso nuevamente al sistema por medio de una puerta trasera.[21]

Amenazas internas: estas amenazas surgen de los empleados o exempleados que

---

[16] AWS. [Sitio web]. ¿Qué es la ciberseguridad?. Disponible en Internet: https://aws.amazon.com/es/what-is/cybersecurity/

[17] MCAFEE. [Sitio web]. ¿Qué es malware?. Disponible en Internet: https://www.mcafee.com/es-co/antivirus/malware.html

[18] KASPERSKY. [Sitio web]. ¿Qué son los bots? Definición y explicación. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/what-are-bots

[19] PANDA. [Sitio web].¿Phishing. Disponible en Internet: https://www.pandasecurity.com/es/security-info/phishing/

[20] AVG. [blog]. ¿Qué es el ransomware?. Disponible en Internet: https://www.avg.com/es/signal/what-is-ransomware

[21] KASPERSKY. [Sitio web]. ¿Qué es una amenaza avanzada persistente (APT)?. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

tienen el conocimiento de información privilegiada donde abusan de los permisos que se les da de forma deliberada, entre estos existe la persona que compromete la cuenta de otro usuario, la persona que por desconocimiento provoca daños en los sistemas o la persona que se aprovecha de los permisos que tiene dentro del sistema para llevar a cabo acciones de manera maliciosa.[22]

Amenazas de seguridad ICloud: estas amenazas dependen de muchos factores cómo por mecanismos tradicionales que permiten que los hackers no sean detectados, fallas de configuración de permisos de las plataformas, plataformas de código abierto que puedan tener fallas de ciberseguridad o problemas de licenciamiento.[23]

Las organizaciones buscan obtener certificaciones de marcos de seguridad tales como: ISO,COBIT O NIST para cumplir con ciertos requerimientos que indica cada norma como definir procesos, procedimientos, alcances y evaluar la efectividad de esta, García[24] menciona que este procedimiento genera confusión y puede generar alto riesgo en el resultado y esto suele pasar con el personal porque es considerado el punto más débil e importante y porque una vez aprobada la certificación no se continua actualizando la documentación y en vez de mitigar los riesgos con los marcos de seguridad se queda en pausa sólo en la documentación hasta que nuevamente se vuelva a generar la revisión del ente certificador.

Las siguientes normativas y estándares en ciberseguridad son considerados los más importantes:

- **ISO/IEC 27001:** En esta normativa se establece los requisitos para un sistema de gestión de seguridad de la información SGSI, con esta normativa las organizaciones pueden implementar medidas de seguridad de la información con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información.[25]
- **PCI DSS:** Es un estándar aplicado a la seguridad de datos en organizaciones que manejan pagos con tarjeta de crédito y débito por eso está establecido los requisitos para proteger esta información y tiene controles definidos para la protección de datos sensibles como los datos del titular de la tarjeta en el

[22] IBM. [blog].¿Qué son las amenazas internas?. Disponible en Internet: https://www.ibm.com/co-es/topics/insider-threats

[23] DOCUSIGN. [blog]. Principales amenazas a la ciberseguridad en las empresas. [en línea]. 2022. Disponible en Internet: https://www.docusign.mx/blog/amenazas-la-ciberseguridad

[24] GARCÍA FORERO, Luis Felipe Guillermo, et al. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. [en línea]. 2020.Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/9545

[25] NORMAS ISO. [Sitio Web]. ISO 27001 seguridad de la información. Disponible en Internet: https://www.normas-iso.com/iso-27001/

proceso de autenticación, almacenamiento y transmisión.[26]

- **NIST SP 800-53:** Es un conjunto de controles de seguridad de la información y privacidad para sistemas de información desarrollado por la NIST permitiendo a las organizaciones la implementación de las medidas de seguridad de la información.[27]
- **Ley 1581 de 2012:** Ley de protección de datos personales que establece principios y requisitos para el correcto tratamiento de los datos personales.[28] Algunas prácticas de ciberseguridad que se pueden aplicar en las organizaciones son:
  - ✓ **Autenticación de dos factores:** Es un proceso para que exista una capa de seguridad proporcionando 2 factores para la autenticación de la persona y también tiene como beneficio que permite saber si alguien intenta acceder sin autorización.[29]
  - ✓ **Encriptación de datos:** con este proceso se protege la información de terceros y documentos importantes que se maneja en una organización para que esta sea manipulada y leída por la persona que lo pueda descifrar, por eso este proceso ofrece seguridad y confidencialidad.[30]
  - ✓ **Sistema de prevención de intrusiones:** es una herramienta importante para una organización ya que está permitiendo que se identifique el tráfico malicioso y poder bloquear el ingreso de ese tráfico, en caso de encontrar alguna amenaza se puede tomar medidas adecuadas.[31]
  - ✓ **Sistema de detección de vulnerabilidades:** Por medio de estas herramientas se identifica los fallos de seguridad que se presentan en un sistema, este proceso contiene diferentes fases para la recolección

[26] ACOSTA David. [Sitio web]. ¿Qué es PCI DSS?. 2022. Disponible en Internet: https://www.pcihispano.com/que-es-pci-dss/

[27] NIST. [Sitio Web]. Controles de seguridad y privacidad para sistemas de información y organizaciones. 2020. Disponible en Internet: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[28] MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. [Sitio Web]. Protección de Datos Personales. Disponible en Internet: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales

[29] KASPERSKY. [blog]. ¿Qué es la Autenticación de Dos Factores y Dónde Debo Utilizarla?. Disponible en Internet: https://latam.kaspersky.com/blog/que-es-la-autenticacion-de-dos-factores-y-donde-debo-utilizarla

[30] CTI SOLUCIONES. [blog]. Encriptación de datos para empresas ¿En qué consiste y cuáles son sus ventajas?. Disponible en Internet: https://www.ctisoluciones.com/blog/encriptacion-datos-para-empresas

[31] FORTINET. [Sitio web]. Definición de Sistema de prevención de intrusiones (IPS). Disponible en Internet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips

de información, detección de vulnerabilidades, explotación y borrado de huellas.[32]

4.3 MARCO HISTÓRICO

La Ciberseguridad comenzó a mediados de 1960 ya que en ese tiempo comenzaron a formarse redes y a conectarse los equipos, este concepto era aplicado al delito de forma manual, después de que se inventó el internet comenzó a tomar forma la ciberseguridad ya que años más tarde aparecería los software maliciosos cómo el malware, cómo indica Sánchez[33], en 1971 apareció el primer virus llamado creeper que se encargaba de replicarse en la red y de la misma manera se creó el primer software de ciberseguridad llamado Reaper como antimalware, con los años la tecnología y los ataques fueron avanzando cómo: ingeniería social, la implementación de cifrado y a desarrollarse otros tipos de virus y antivirus.

Uno de los ataques más recordados es Wannacry cómo indica Almonacid[34], afecto más de doscientos mil computadores en aproximadamente 150 países, este ataque fue denominado como ransomware por medio de este ataque el ciberdelincuente encripta la información, roba la información o realiza cambios de autenticación con el objetivo de pedir un cambio por la devolución de los datos encriptados y provoco pérdidas económicas demasiado costosas, en cuestión de días CCN-CERT publico una herramienta para evitar la ejecución del ransomware.

En definitiva desde los años 80 los malware han venido presentando mayor impacto e incrementación de la misma manera han mejorado los sistemas antimalware y han comenzado a generarse plataformas para detección y respuesta como EDR con el fin de proteger un sistema de los diferentes tipos de malware, como indica Infosecurity[35], desde los años 90 los ataques cibernéticos se volvió un tema primordial de forma internacional debido a la falta de conocimiento del ciberespacio, medidas de seguridad hasta el uso de la tecnología, hacia el 2001 apareció un comité de expertos de delios informáticos los cuales ya están en 56 países para protegerlos de la ciberdelincuencia.

---

[32] KEEPCODING. [blog]. Detección de vulnerabilidades informáticas. 2022. Disponible en Internet: https://keepcoding.io/blog/deteccion-de-vulnerabilidades/

[33] NORDVPN. SANCHEZ, O. Laura. [Blog]. La historia de la ciberseguridad. 2022. Disponible en Internet: https://nordvpn.com/es/blog/historia-ciberseguridad/

[34] ALMONACID DE CÁRDENAS, Álvaro. Auditoría técnica de seguridad: análisis y explotación de vulnerabilidades. pp.1-9.

[35] INFOSECURITY, MEXICO. [blog]. Ciberseguridad. Disponible en Internet: https://www.infosecuritymexico.com/es/ciberseguridad.html#historia

4.3.1 Evolución de las ciber amenazas

A través de los años se han venido presentando nuevas ciber amenazas cómo indica Romero[36], CCN.CERT quienes da una prioridad a las más presentadas, tales como:

1. Ciber espionaje: Es una práctica ilegal para obtener información confidencial y sensible con el fin de obtener una ventaja competitiva.
2. Ciberdelito: Es una actividad delictiva cometida a través de sistemas informáticos, se considera actividades delictivas como accesos no autorizados, robo de información, propagación de virus, estafa, extorsión etc.
3. Ciberactivismo: es considerado como activismo digital por lo cual utiliza las redes para promover cambios sociales, políticos, etc.
4. Ciberterrorismo: la tecnología es utilizada para llevar a cabo actos terroristas para causar daño en infraestructuras críticas.
5. Ciberguerra: Guerra que se lleva a cabo en el ciberespacio por medio de ataques cibernéticos puede ser entre estados con el fin de obtener información confidencial que los pueda afectar.

Figura 3. Importancia de las amenazas según CCN-CERT.

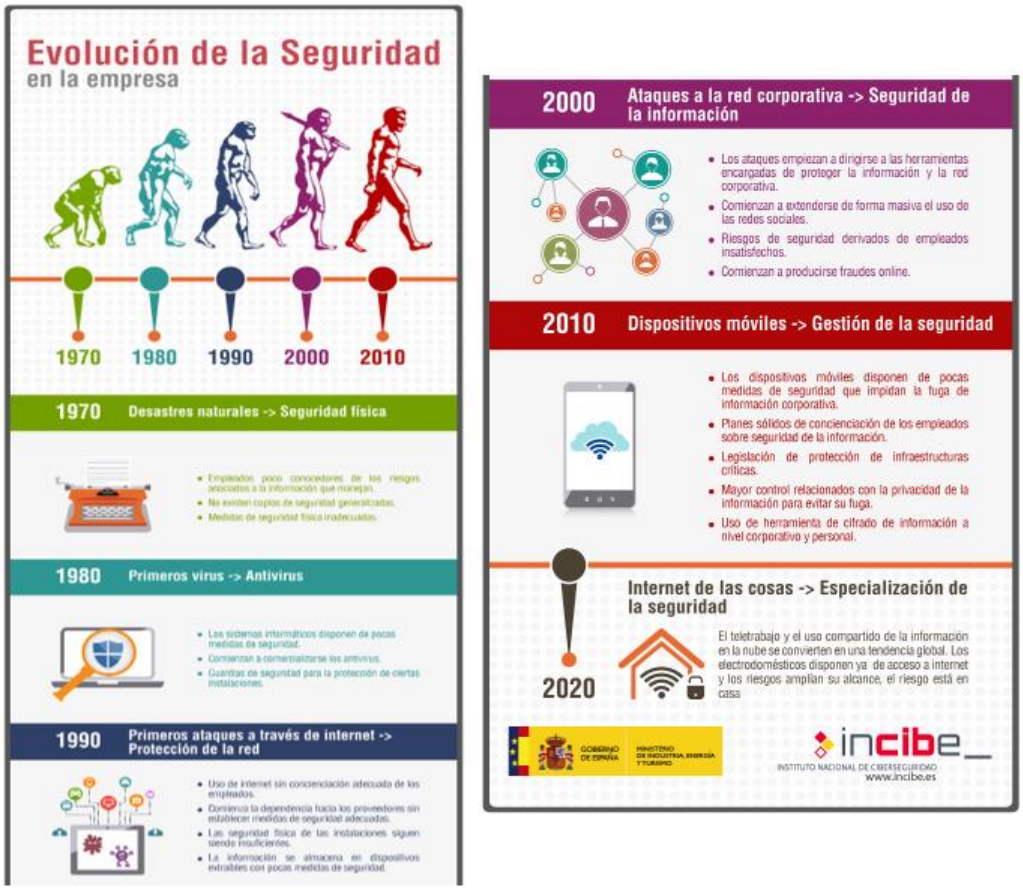
Fuente: ROMERO, Javier Candau. Ciberseguridad: Evolución y tendencias. (2021). https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

4.3.2 Ciberseguridad en las empresas

[36] ROMERO.Op.cit, p 12.

Las empresas buscan proteger y asegurar la información por lo que algunas ya cuentan con normas como ISO 27001 implementadas para garantizar la disponibilidad, confidencialidad e integridad de la información, las empresas ya conocen sus riesgos y como dar tratamiento a los mismos, pues bien existen ciertas prácticas de ciberseguridad que permite que todo sea mucho más claro, cómo indica CCIT[37], se debe contar con un análisis de escenarios para poder tener una vista sobre las amenazas y riesgos con el fin de accionar a los eventos presentados, contar con ciber inteligencia para monitoreo, pruebas de vulnerabilidades, defensa activa para poder tener un resultado claro y de tal manera poder anticipar, defender y proteger la información.

Figura 4. Evolución de la seguridad en la empresa.



Fuente: INCIBE. La seguridad vista desde sus inicios. (2015). https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

[37] CCIT. [Sitio web]. Mejores prácticas para el fortalecimiento de la ciberseguridad empresarial. Disponible en Internet: https://www.ccit.org.co/wp-content/uploads/mejores-practicas-para-la-ciberseguridad-en-las-empresas-vf.pdf

4.4 ANTECEDENTES O ESTADO ACTUAL

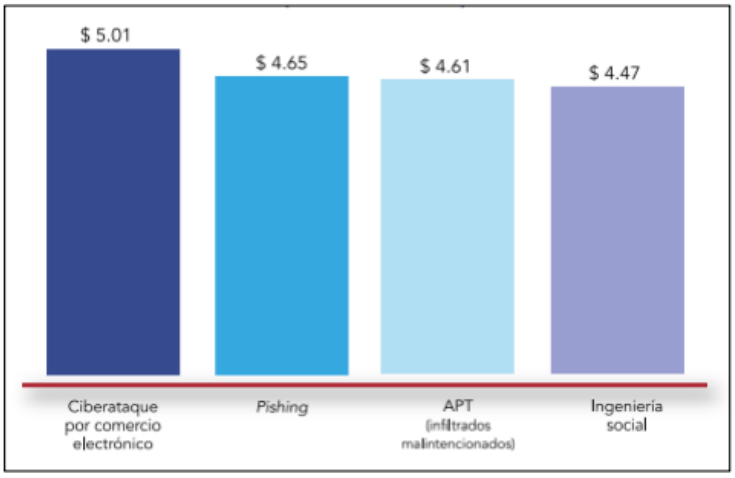
Bojórquez[38], indica que en 2022 se presenta gran porcentaje de usuarios que acceden a internet con la probabilidad de ser víctimas de un ciberataque como se puede observar en la tabla 2 y los costos que puede generar en perdidas cómo se puede ver en la figura 5.

Tabla 2. Población a nivel mundial de usuarios que tienen acceso a internet, 2022.

REGIÓN	POBLACIÓN ESTIMADA (Q1/2019)	PORCENTAJE POBLACIÓN MUNDIAL (%)	USUARIOS DE INTERNET (Q1/2019)	RATIO DE PENETRACIÓN (%)	PORCENTAJE INTERNET MUNDIAL (%)
África	1.340.598.447	55,1	2.366.213.308	55,1	11,3
Asia	4.294.516.659	55,1	2.366.213.308	55,1	50,9
Europa	834.995.197	10,7	727.848.547	87,2	15,7
Latinoamérica y Caribe	658.345.826	8,5	453.702.292	68,9	10,0
Medio Este	260.991.690	3,3	183.212.099	70,2	3,9
América del Norte	368.869.64	4,7	348.908.868	94,6	7,5
Oceanía y Australia	42.690.838	0,5	28.917.600	67,7	0,6
Total mundial	7.796.949.710	100	4.648.228.067	59,6	100

Fuente: BOJORQUEZ HUANCA, Jeymi Shirley. Ciberseguridad. (2022). https://repositorio.unam.edu.pe/handle/UNAM/420

Figura 5. Costo total promedio por ataque.



Fuente: BOJORQUEZ HUANCA, Jeymi Shirley. Ciberseguridad. (2022). https://repositorio.unam.edu.pe/handle/UNAM/420

[38] BOJORQUEZ HUANCA, Jeymi Shirley. Ciberseguridad. [en línea]. Informe profesional de ciberseguridad. Universidad Nacional de Moquegua, 2022. Disponible en Internet: https://repositorio.unam.edu.pe/handle/UNAM/420

En Colombia desde 2021 ha presentado crecimiento digital por lo que se puede observar en la figura 6, indica Alvino[39], que en Colombia creció 0.9% de población aproximando a 463 mil personas divididas entre 1.9% conectándose desde dispositivos móviles, 4.0% en usuarios de internet, y 11.4% de usuarios en redes sociales. El uso de internet ahora es más elevado desde cuarentena y aislamiento por COVID-19 debido a que se volvió una herramienta para trabajar, estudiar, entretener y cumplir con las responsabilidades.

Figura 6. crecimiento digital enero 2020 vs enero 2021.

Fuente: ALVINO, Clay. Estadísticas de la situación digital de Colombia en el 2020-2021. (2021). https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021

Incibe[40], indica que en el año 2022 se gestionaron 118.820 incidentes por filtración de datos, vulnerabilidades de sistemas tecnológicos, fraude a los ciudadanos, e incidentes en las empresas, reporta que 546 operadores críticos también presentaron vulnerabilidades en los que se encuentra el sector de energía, sistema

[39] ALVINO, Clay. [Sitio web]. Estadísticas de la situación digital de Colombia en el 2020-2021. 2021. Disponible en Internet: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021

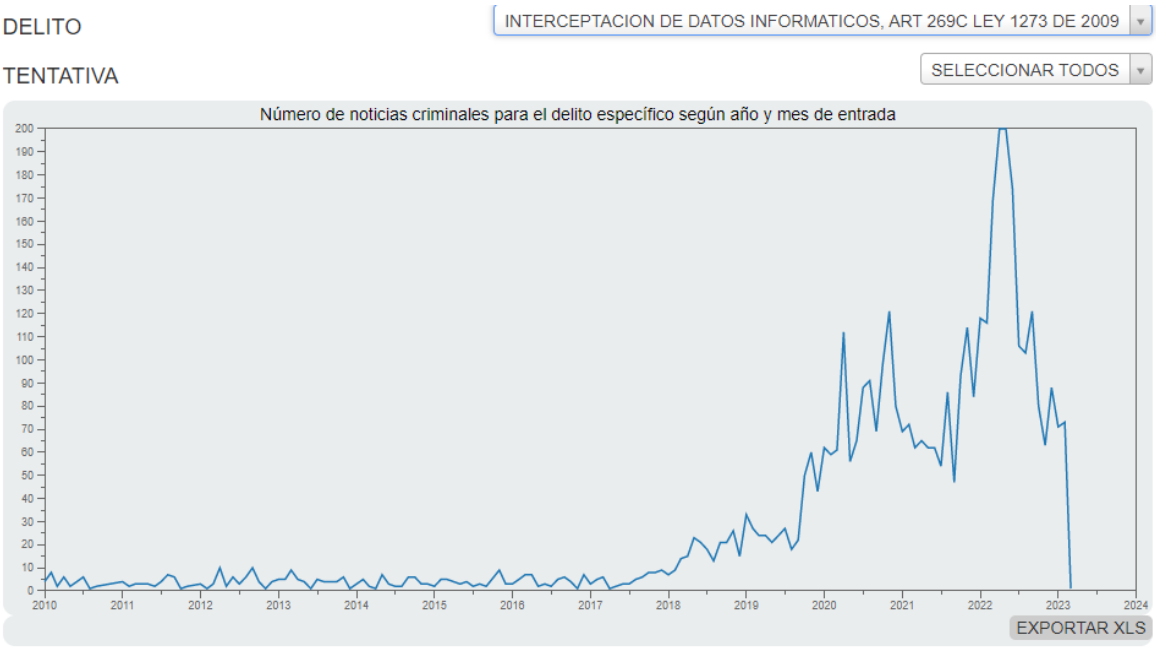
[40] INCIBE. [Sitio web]. Balance de Ciberseguridad 2022. 2022. Disponible en Internet: https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

financiero y tributario, sector de acueducto, transporte y académico, los incidentes más frecuentes son Phishing, Malware y Ransomware.

Desde el año 2022 al presente año muchas empresas en Colombia se han visto afectadas por los diferentes ciberataques que les han realizado, logrando así afectarla información, prestación del servicio y reputación de las mismas.
Al año 2023 en Colombia han realizado denuncias cómo se puede evidenciar en la figura 7 como ha variado la suplantación de sitios web para capturar datos personales relacionado con la ley 1273 de 2009 ART 269G.
Figura 7. Suplantación de sitios web para capturar datos personales

Fuente: FISCALIA. Estadísticas de denuncias por delitos. (2023). https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

Al año 2023 se puede evidenciar en la figura 8 como ha variado la interceptación de datos informáticos que han sido denunciados, relacionado con la ley 1273 de 2009 ART 269C.
Figura 8. Interceptación de datos informáticos.



Fuente: FISCALIA. Estadísticas de denuncias por delitos. (2023). https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

Al año 2023 se puede evidenciar en la figura 9 como ha variado la violación de datos personales denunciados relacionado con la ley 1273 de 2009 ART 269F.

Figura 9. Violación de datos personales

Fuente: FISCALIA. Estadísticas de denuncias por delitos. (2023). https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

4.5 MARCO LEGAL

Ley 1273 de 2009: Esta ley establece los atentados contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, donde se adiciona el código penal para la protección de la información, exponiendo las penas correspondientes y las medidas para prevención de delitos informáticos.[41]

Ley 1581 de 2012: Se establecen disposiciones para a protección de datos personales, describiendo los principios para el tratamiento de los datos, las categorías de datos, los derechos y condiciones para el tratamiento de los datos, la guía de los procedimientos y obligaciones que deben cumplir las empresas, los deberes de los responsables para dar el correcto manejo y tratamiento de los datos. [42]

Decreto 620 de 2020: Establece los lineamientos generales en el uso y operación de los servicios digitales, en este decreto se establece las medidas para asegurar el tratamiento de datos personales, seguridad y privacidad de la información.[43]

CONPES 3701 de 2011: Establece lineamientos para la Ciberseguridad y ciberdefensa en el país de Colombia en busca del desarrollo de estrategia para contrarrestar las amenazas por medio de planes, estrategias y políticas.[44]

Decreto 338 de 2022: Establece lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, en este decreto se define modelos para la gestión de incidentes estableciendo el alcance para los equipos de respuesta a incidentes de seguridad digital CSIRT[45].

[41] CONGRESO DE COLOMBIA. [Sitio web]. Ley 1273 delitos informáticos. 2009. Disponible en Internet: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
[42] CONGRESO DE COLOMBIA. [Sitio web]. Ley 1581 de 2012. 2012. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[43] FUNCION PUBLICA. Decreto 620 de 2020. [en línea]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337
[44] ALTA CONSEJERIA DISTRITAL. Conpes 3701 DE 2011. [en línea]. Disponible en Internet: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011
[45]FUNCION PUBLICA. Decreto 338 de 2022. [en línea]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

5. RIESGOS Y AMENAZAS EN LAS ORGANIZACIONES COLOMBIANAS Y SU IMPACTO EN LA CONTINUIDAD DEL NEGOCIO

5.1 Riesgos cibernéticos en las organizaciones.

Las organizaciones deben contar con la capacidad para la identificación de riesgos cibernéticos y poder afrontar los desafíos que pueden presentarse por los ciberataques, como indica Fernández[46], se debe tener en cuenta que el ciberespacio es un generador de amenazas, por lo cual conlleva a que la información este en riesgo cómo hurto de información o secuestro de datos en el ciberespacio.

Los riesgos más comunes en una organización son:

Perdida de datos: estos pueden pasar por ataques maliciosos, fallos en el software o hardware, desastres naturales dejando un impacto negativo para la reputación de una organización.

Robo de datos: por medio de virus o por las vulnerabilidades que se puede presentar en un sistema, se puede robar todo tipo de datos que sean valiosos para el atacante y de los cuales pueda sacar una ganancia o beneficio propio.

Ransomware: con este malware se puede cifrar los datos que se encuentran de una organización, para después exigir un pago para desbloquearlos, pero nadie puede asegurar que en realidad al pagar el rescate puede tener su información.

Phishing: es una técnica muy utilizada en las organizaciones para engañar a los usuarios con el fin de que se proporcione información confidencial.

Malware: Es el ataque más utilizado porque permite que un sistema se pueda dañar y de esa manera poder robar información o tener el control de los dispositivos de una organización.

Servicios interrumpidos: Este es muy conocido debido al gran impacto que deja en una organización, dado que los sistemas son afectados por ataques DDoS, de tal manera que puede detener los procesos o el funcionamiento de una operación.

Es necesario tener en cuenta que estos riesgos se deben gestionar cómo se observa en la figura 10.

[46] FERNÁNDEZ, E. E. C., & Herrera, R. D. J. G. Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional. [en línea]. 2020. Disponible en Internet: https://www.redalyc.org/journal/5713/571361695004/571361695004.pdf

Figura 10. Gestión de los riesgos cibernéticos

Fuente: ATCAL. Gestión de los riesgos cibernéticos. https://www.implementandosgi.com/sistemas-de-gestion/gestionar-tus-riesgos-ciberneticos/

Por último, para las organizaciones es necesario comprender los riesgos cibernéticos, y como pueden emplear medidas para protegerse de forma adecuada, comenzando por auditorías internas de seguridad de la información, monitoreo, pruebas y capacitación al personal.

5.1.1 Vulnerabilidades cibernéticas más comunes.

Los ciber atacantes pueden aprovechar fallas en el hardware y software para obtener acceso, de esta manera tendrán la oportunidad de encontrar vulnerabilidades y explotar los sistemas si no cuentan con hardware y software actualizados.

Ahora bien, si los usuarios crean contraseñas débiles que pueden ser descifradas mediante ataques de fuerza bruta, es más probable que una vulnerabilidad se convierta en un riesgo cuándo no se implementan medidas de seguridad.

De acuerdo con Molina[47], algunas vulnerabilidades son más reconocidas son:

- Vulnerabilidades de sistemas de Información
- Vulnerabilidades día cero
- Vulnerabilidades de aplicación Web.
- Vulnerabilidades en las bases de datos.

Es importante que las organizaciones inviertan dinero para poder proteger sus activos de información e implementar controles que permitan que solo las personas autorizadas pueden acceder a la información, cualquier tipo de organización

[47] MOLINA, OPT.cit.,p 12

necesita contar con estrategias e implementación de sistemas que puedan detectar intrusiones o prevenirlas como los IDS/IPS.
Para finalizar se identifica que son necesarias las pruebas de penetración y pentesting, adicional que es importante poder tener identificadas las debilidades de los diferentes sistemas y establecer salvaguardas para mitigar cualquier tipo de ataque o pérdidas de información.

5.1.2 Análisis de riesgos y amenazas en las organizaciones.

Las amenazas cibernéticas representan intentos maliciosos para obtener acceso a información confidencial cómo puede ser información de clientes, proveedores, empleados o procesos internos que maneje la organización. Por lo tanto, las organizaciones están enfrentándose a una variedad de riesgos como lo son las ciber amenazas siendo promovidos por cibercriminales[48].
Algunos de los riesgos y amenazas más comunes que pueden afectar a una organización en el tema de ciberseguridad incluyen:

- **Malware:** son programas informáticos diseñados para dañar, alterar o robar información. Pueden propagarse a través de correos electrónicos, descargas de software, sitios web comprometidos, entre otros.
- **Phishing**: es un tipo de ataque que consiste en engañar a los usuarios para que revelen información confidencial, como contraseñas, números de tarjeta de crédito o datos de cuentas bancarias. Los atacantes suelen enviar correos electrónicos que parecen legítimos y que solicitan al usuario que haga clic en un enlace para iniciar sesión en una cuenta o proporcionar información.
- **Ataques de fuerza bruta:** consisten en intentar adivinar contraseñas mediante la utilización de programas que prueban diferentes combinaciones de caracteres hasta encontrar la correcta.
- **Ataques de denegación de servicio (DDoS):** se realizan para sobrecargar un servidor o red con tráfico malicioso, impidiendo que los usuarios legítimos puedan acceder a los servicios.
- **Ingeniería social:** consiste en manipular a los usuarios para que divulguen información confidencial o realicen acciones no deseadas. Los atacantes pueden utilizar tácticas como la intimidación, el engaño o la persuasión para obtener información.

[48] CANVIA. [blog]. Estas son las 10 amenazas cibernéticas más comunes en empresas.2023. Disponible en Internet: https://www.canvia.com/amenazas-ciberneticas/#:~:text=Las%20amenazas%20cibern%C3%A9ticas%20son%20aquellos,al%20funcionamiento%20de%20la%20organizaci%C3%B3n.

- **Vulnerabilidades de software:** son errores en el código de software que pueden ser explotados por los atacantes para tomar el control de los sistemas o acceder a información confidencial.
- **Ataques de ransomware:** consisten en cifrar la información de una organización y exigir un rescate a cambio de su liberación.
- **Ataques de suplantación de identidad (spoofing):** se realizan para engañar a los usuarios haciéndoles creer que están interactuando con una fuente confiable, como un sitio web o un correo electrónico.
- **Brechas de datos:** son violaciones de seguridad que permiten a los atacantes acceder a información confidencial, como nombres de usuarios, contraseñas, información de tarjetas de crédito o datos personales.
- **Robo de credenciales:** los atacantes pueden robar las credenciales de inicio de sesión de un usuario a través de ataques de phishing, malware o ingeniería social, lo que les permite acceder a los sistemas de la organización.

Existen más amenazas de ciberseguridad, pero cabe resaltar que la más presentada en el año 2023 para las organizaciones ha sido el ransomware[49] lo cual obliga a que el empresario deba pagar un rescate, bloqueando el acceso a los diferentes sistemas. De modo que para evitar esto es necesario utilizar antivirus, firewalls, VPN y copias de seguridad en lugares seguros. También es necesario mantener actualizados los diferentes sistemas y finalmente capacitar a los empleados.

5.1.3 Informes de seguridad y ataques cibernéticos presentados en Colombia.

La ciberseguridad se ha vuelto esencial en Colombia y en otros países, por lo cual se puede acceder a la información desde cualquier lugar donde se cuente con conexión a internet, De acuerdo a lo indicado por CCIT-TicTac[50] más de 23.000 noticias fueron reportadas a mediados de junio de 2021 por la fiscalía general de la nación, donde se evidencia que aumento 30% más que el año 2020.

El centro cibernético de la policía nacional confirmo sobre el aumento de reportes de ciberataques en Colombia en 2022 aumento a 54.121 denuncias[51].

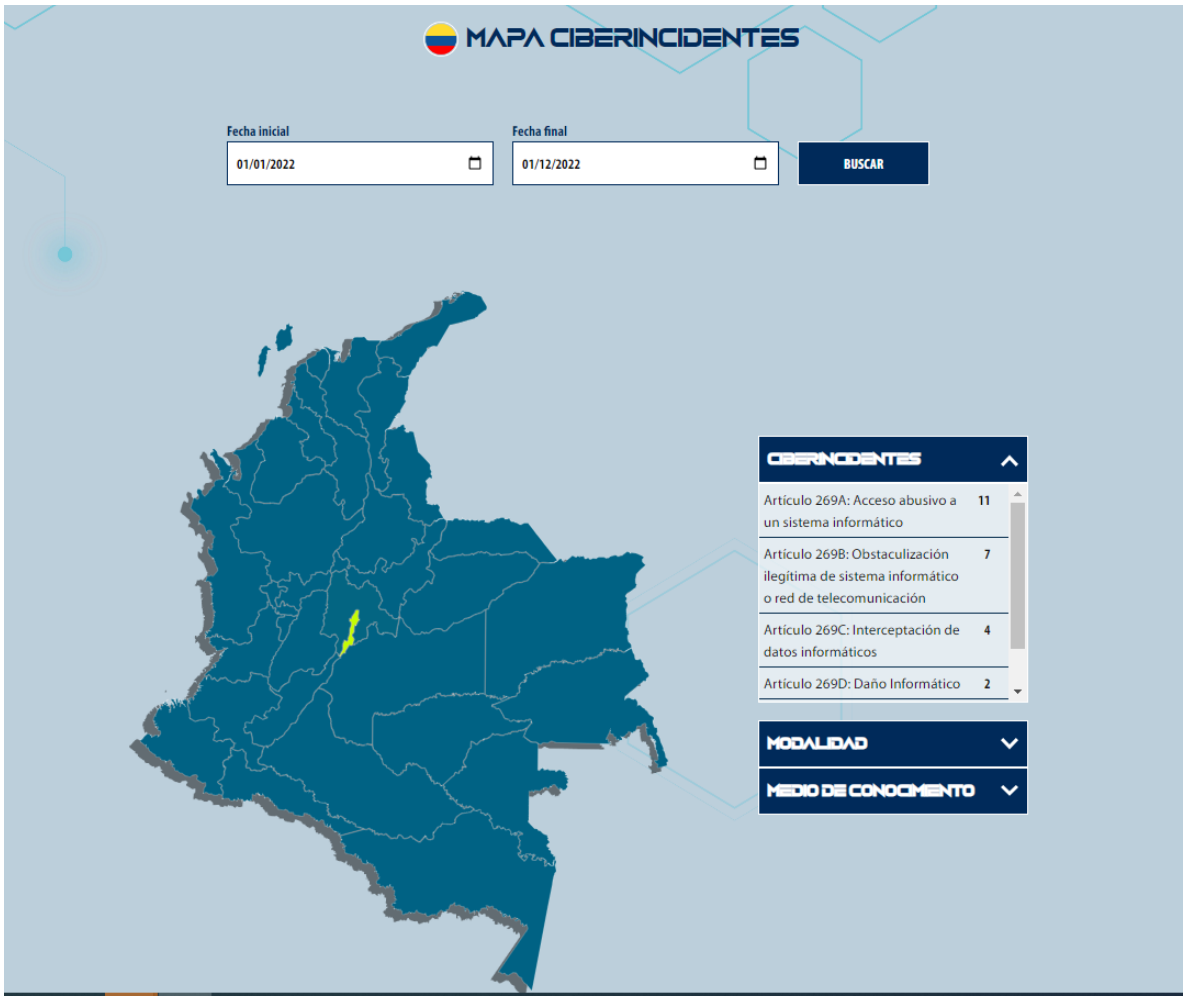
---

[49] Ibid.p.26

[50] CCIT – TicTac. [Sitio Web]. Informe: Evaluación, retos y amenazas a la ciberseguridad. 2021. Disponible en Internet: https://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/

[51] GUZMAN, Ana. [Blog]. La importancia de la Ciberseguridad en las empresas colombianas.2023. Disponible en Internet: https://welcome.atlasgov.com/es/blog/ciberseguridad/la-importancia-de-la-ciberseguridad-en-las-empresas-colombianas/

Figura 11.Ciber incidentes 2022.



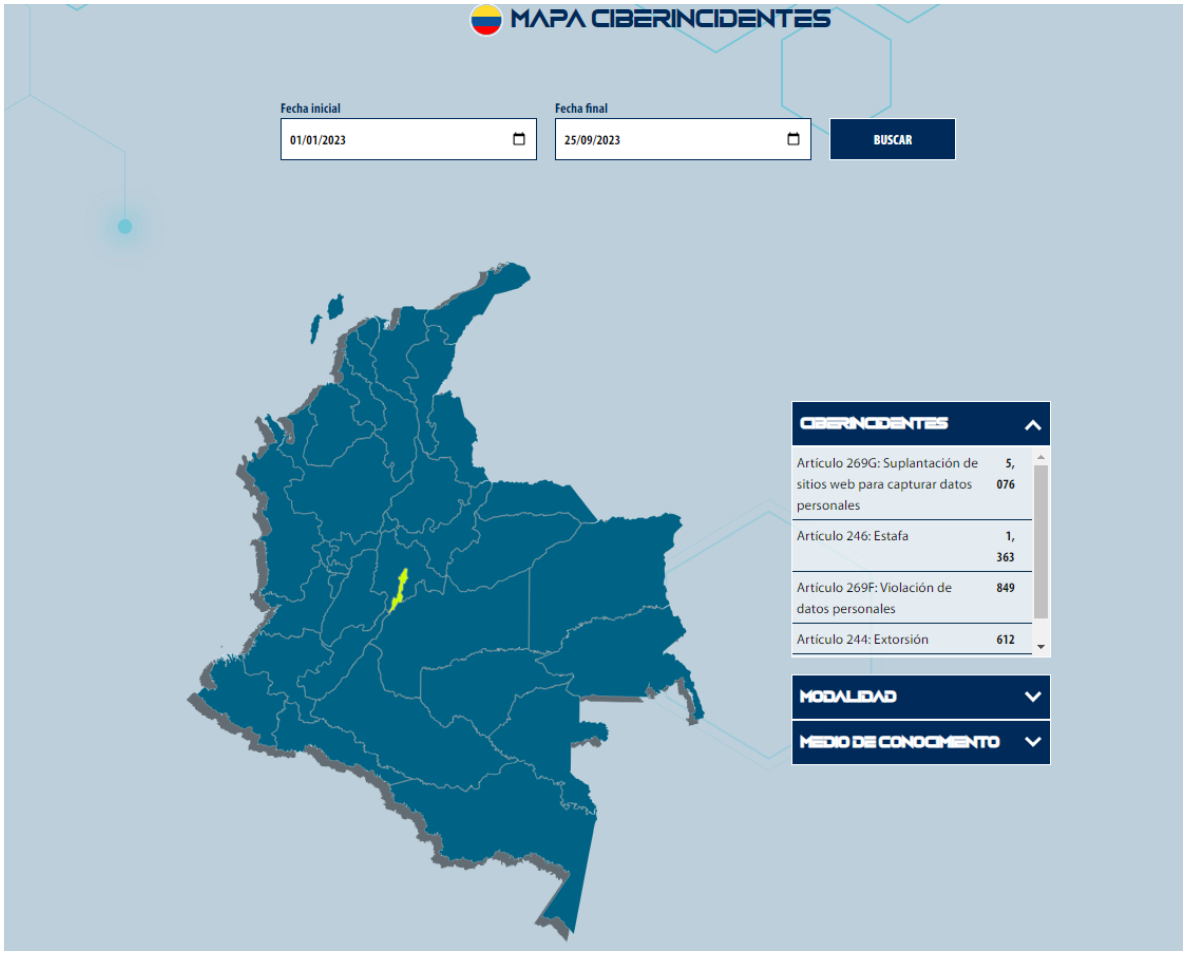
Fuente: Mapa ciber incidentes. https://caivirtual.policia.gov.co/ciberincidentes

En diciembre de 2022, COLCERT, el equipo de respuesta en ciberseguridad de Colombia, informó al Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic) sobre un total de 36 incidentes de seguridad cibernética. Estos incidentes se desglosaron en 19 casos de suplantación y 8 casos de suplantación de dominios. De los 36 ataques registrados, 18 de ellos estuvieron dirigidos a organizaciones del sector privado[52].

[52] MINTIC. [Sitio Web]. En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia. 2022. Disponible en Internet: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

Durante el año 2022 según demuestra la página de la policía se observa los tipos de incidentes y la modalidad de estos incidentes informáticos como Acceso remoto no autorizado, Botnets, Ataque DDoS, ataques DNS e Insider[53].

Figura 12. Ciber incidentes 2023.



Fuente: Mapa ciber incidentes. https://caivirtual.policia.gov.co/ciberincidentes

En 2023 se ha evidenciado por medio del mapa de ciber incidentes de la policía de Colombia[54] la modalidad que han usado los ciberdelincuentes como: Phishing, Estafa por compra y venta, suplantación de identidad, Vishing, amenazas por medio de las redes sociales.

Según el informe de SonicWall, el año 2023 experimentó un aumento en el malware, el cryptojacking y el ransomware. Por lo tanto, las organizaciones deben adquirir un

[53] CAI VIRTUAL. [Sitio Web]. Mapa ciber incidentes. 2022. Disponible en Internet: https://caivirtual.policia.gov.co/ciberincidentes

[54] CAI VIRTUAL. [Sitio Web]. Mapa ciber incidentes. 2023. Disponible en Internet: https://caivirtual.policia.gov.co/ciberincidentes

conocimiento profundo de las tácticas de los atacantes para proteger sus sistemas de posibles compromisos. El ransomware ha afectado significativamente diversas industrias, incluyendo finanzas, educación y atención médica[55].
Tanto las organizaciones como el gobierno deben continuar priorizando la seguridad digital y fortalecer las infraestructuras, dado que los ciberdelincuentes están mejorando constantemente sus estrategias y herramientas. A pesar de la preocupación generada por los diversos tipos de ataques mencionados anteriormente, es esencial esforzarse en reducir este tipo de amenazas.

5.1.4 Impacto de los incidentes en la continuidad del negocio.

Los incidentes pueden tener un impacto significativo en las organizaciones, afectando la confidencialidad de la información, la reputación, la continuidad del servicio y generando pérdidas económicas. Estos incidentes no se limitan a pequeñas empresas; incluso las grandes empresas con infraestructuras sólidas pueden ser vulnerables[56].

Algunos casos donde se ha presentado estos impactos son:

Nvidia: En 2022 sufrió ataque cibernético donde lograron filtrar la información personal de aproximadamente 71.000 empleados.
EPM: En 2022 fue víctima de ciberataque llegando a afectar la prestación de sus servicios.
Keralty sanitas: En 2022 un ataque cibernético alcanzo a afectar la información de 241589 usuarios.
SECOP II: A mediados de 2023 el ataque cibernético logro que estuviera esta plataforma fuera de línea.
IFX Networks S.A.S: En 2023 se ven afectados los servicios que prestan a entidades públicas por un ransomware de RansomHouse donde 760 compañías latinoamericanas fueron afectadas.[57]
Algunos impactos más comunes son:

[55] INTERNATIONALIIT. [Sitio Web]. SonicWall: Informe de amenazas cibernéticas. 2023. Disponible en Internet: https://www.internationalit.com/post/sonicwall-informe-de-amenazas-cibern%C3%A9ticas-2023?lang=es
[56] LINKEDIN. RENATA COLOMBIA. [Sitio Web]. Colombia segundo lugar en ciberataques en Latinoamérica, conozca los riesgos para evitar incidentes de ciberseguridad.2023. Disponible en Internet: https://www.linkedin.com/pulse/colombia-segundo-lugar-en-ciberataques/?originalSubdomain=es
[57] PIRANI.JIMENEZ, M. Maria. [Blog].¿Qué pudo causar el ataque cibernético a IFX Networks?.2023. Disponible en Internet: https://www.piranirisk.com/es/blog/posibles-causas-ataque-cibernetico-ifx-networks

Interrupción del servicio: los incidentes provocan la interrupción del servicio en una organización, generando pérdida de clientes, proveedores y dinero al interrumpir la operación normal[58].

Perdida de datos: Para una organización la perdida de datos o el acceso no autorizado puede generar graves consecuencias y aplica a incumplir leyes que son alineadas para la protección de datos.

Fugas de información: El factor humano es muy importante en una organización, por eso la fuga de información que se presente por errores humanos, falta de implementación de medidas de seguridad o problemas de hardware o software puede llegar a afectar a la organización por perdida de información sensible[59].

Mala Reputación: Cuando se presenta incidentes de seguridad y al ser divulgado que se presentó el incidente, es posible que dañe la reputación y la marca de la organización podría verse afectada a mediano o largo plazo.

Daños económicos: Las multas, demandas legales y costos de recuperación de datos representan un impacto significativo en la economía de la organización[60].

Es fundamental destacar que los incidentes pueden tener graves consecuencias, incluyendo daños a la reputación y pérdidas financieras significativas para las organizaciones. Por lo tanto, es esencial que las organizaciones implementen políticas y procedimientos para fortalecer la seguridad y realicen un monitoreo constante de su infraestructura.

Además, contar con planes de respuesta a incidentes es crucial, ya que no se debe subestimar el impacto que los incidentes de ciberseguridad pueden tener en la continuidad del negocio. La importancia de las medidas proactivas y la preparación para responder adecuadamente ante estos incidentes no puede ser pasada por alto. Las organizaciones deben tomar en serio la prevención y la respuesta como parte integral de su estrategia de seguridad cibernética.

---

[58] ISOTOOLS.Seguridad de la información. [Blog]. ¿Qué situaciones de SI pueden afectar la continuidad del negocio?. 2023. Disponible en Internet: https://www.pmg-ssi.com/2023/05/que-situaciones-de-si-pueden-afectar-la-continuidad-del-negocio/

[59] Ibid.

[60] CIBERSEGURIDAD. [Sitio Web]. Continuidad de negocio. Disponible en Internet: https://ciberseguridad.com/normativa/espana/medidas/continuidad-negocio/#Identificar_gastos_adicionales

6. ANÁLISIS DE POLÍTICAS Y NORMATIVAS EN COLOMBIA: EVALUACIÓN DE SU APLICACIÓN EN ORGANIZACIONES.

Las organizaciones en Colombia enfrentan la necesidad de comprender y adecuarse a las regulaciones gubernamentales por la adopción de nuevas tecnologías. Esto implica el desarrollo e implementación de estándares, normatividades y políticas que permitan abordar de manera eficiente los desafíos que se presenta por la transformación digital. Entre las normativas vigentes en Colombia que revisten importancia en este contexto, destacamos las siguientes:

Decreto 1008 de 2018: Establece lineamientos y estándares, para generar valor público en un entorno de confianza digital mediante el uso efectivo de las TIC.[61]

Ley 1273 de 2009: Esta ley establece medidas para la preservación integral de los sistemas que utilizan tecnologías de la información y las comunicaciones para la protección de los datos.[62]

Decreto 338 marzo 2022: Establece lineamientos para mejorar la gobernanza de la seguridad digital en Colombia se establecen mediante el Decreto 338 de 2022. Junto con la gestión de riesgos y la respuesta a incidentes relacionados con la seguridad digital, esto implica identificar la infraestructura cibernética crítica y los servicios esenciales.[63]

CONPES 3854: Este documento busca mejorar la eficiencia de la ciberseguridad y proporciona información y recursos sobre la ciberseguridad en Colombia[64].

Decreto 620 de 2020: Este documento proporciona medidas de seguridad de la información en el sector privado en Colombia y mencionan otras leyes que están enfocadas a la protección de datos personales y seguridad de la información.[65]

Ley 1581 de 2012: Conocida como la Ley de Protección de Datos Personales, reconoce y protege el derecho de todas las personas a conocer, actualizar y corregir la información que se recopila sobre ellas en bases de datos, tanto en entidades públicas como privadas.[66]

---

[61] FUNCION PUBLICA. [Sitio Web]. Decreto 1008 de 2018. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902 .

[62] CONGRESO DE COLOMBIA, OPT.cit.,p 23

[63] MINTIC. [Sitio Web]. Decreto de seguridad digital.2022. Disponible en internet: https://www.crossbordertech.com/wp-content/uploads/2022/03/Decreto-338-de-8-de-marzo-de-2022-3.pdf

[64] CONGRESO DE LA REPUBLICA DE COLOMBIA. CONPES 3854. [en linea]. Disponible en internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[65] NE, DIGITAL. [blog]. Guía esencial sobre la Ciberseguridad en Colombia. Disponible en internet: https://www.nedigital.com/es/blog/ciberseguridad-en-colombia

[66] MINAMBIENTE. [Sitio web]. Protección de Datos Personales. Disponible en internet: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

Resolución 500 de 2021: La Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece lineamientos y estándares para la estrategia de seguridad digital en Colombia. Su objetivo es implementar el Modelo de Seguridad y Privacidad de la Información (MSPI), guiar la gestión de riesgos de seguridad de la información y establecer procedimientos para la gestión de incidentes de seguridad digital[67].

Norma ISO 27001: La norma ISO 27001, creada en 2005 y actualizada en 2013, establece un marco para la implementación y gestión de sistemas de seguridad de la información. Se enfoca en procesos, análisis de riesgos y controles para proteger datos y mitigar riesgos. Esta norma ha sido utilizada por el Estado para su estrategia de Gobierno en Línea. La ISO 27001 aborda amenazas como la violación de datos, vandalismo y ciberataques.[68]

Norma ISO 31000: El propósito de esta norma es proporcionar directrices para la gestión de riesgos de forma estratégica y operativa, por lo que puede ser aplicada por cualquier entidad, ya sea pública o privada. Los principios fundamentales de la ISO 31000 incluyen la creación de valor, la integración en los procesos de la organización, la incorporación en la toma de decisiones entre otros.[69]

CONPES 3701 de 2011: En este documento se exponen los lineamientos de ciberdefensa y ciberseguridad que esta enfocados al desarrollo de una estrategia nacional para mitigar las amenazas informáticas que afectan al país, teniendo en cuenta la creciente importancia de la seguridad en el entorno digital y la necesidad de proteger los intereses nacionales de las ciber amenazas.[70]

Estas normativas aplican a empresas publicas y privadas con el fin de replantear las políticas para el correcto manejo de la información y fortalecer las herramientas de protección de datos. Se considera que estas normativas son iniciativas para sensibilizar y establecer controles de seguridad y cumplir requisitos necesarios para protección de los datos asegurando la integridad, confidencialidad y disponibilidad.
El marco legal en el ámbito de la economía de datos se basa en la ciberseguridad, la protección de secretos empresariales y la protección de datos personales. La

[67] MINTIC. [Sitio Web]. MINTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital.2021. Disponible en internet: https://gobiernodigital.mintic.gov.co/portal/Noticias/162625:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

[68] CAMARGO, Erney Alberto Ramírez; PINZON, RINCON, Miguel Alberto. La importancia de la seguridad de la información en el sector público en Colombia. [En línea]. Revista Ibérica de Sistemas e Tecnologías de Información. 2022. no 46, p. 87-99. Disponible en Internet: https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

[69] Ibid.

[70] CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL. CONPES 3701. [en línea]. Disponible en internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

entrada en vigor del Reglamento General de Protección de Datos (RPGD) de la Unión Europea en mayo de 2018 ha fortalecido la normatividad colombiana, al exigir un tratamiento leal, transparente y respetuoso de los datos. Esto presiona a las empresas para implementar controles necesarios en la protección de la información.[71]

En conclusión, las políticas y regulaciones de ciberseguridad en Colombia son importantes para proteger los activos digitales, la continuidad del negocio y la reputación de las organizaciones.

6.1 Organismos gubernamentales

En Colombia, además de las diversas regulaciones y normativas en el ámbito de la ciberseguridad, existen organismos gubernamentales que desempeñan un papel fundamental en la promoción y defensa de la ciberseguridad. Entre estos organismos destaca el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

El MinTIC tiene la responsabilidad de diseñar, adoptar y promover políticas, programas y proyectos relacionados con las tecnologías de la información y las comunicaciones (TIC) en el país. Además, su misión incluye la promoción del acceso a las TIC y la apropiación masiva de las mismas. Dentro de su amplio alcance de actuación, el Ministerio despliega esfuerzos significativos para apoyar la implementación de políticas de ciberseguridad y ciberdefensa en Colombia[72].

Esto contribuye a la formación y sensibilización pública en materia de ciberseguridad, así como a la promoción de buenas prácticas y estándares de seguridad en el uso de las TIC. En resumen, el Ministerio de Tecnologías de la Información y las Comunicaciones cumple un papel importante en la creación de un entorno cibernético más seguro en Colombia, apoyando iniciativas relacionadas con la ciberseguridad y la ciberdefensa en el país.

Además, en Colombia existen 3 organismos especializados en ciberdefensa y ciberseguridad como:

Comando de Conjunto Cibernético de las Fuerzas Militares: Este comando se encarga de coordinar la respuesta a incidentes de seguridad que puedan impactar la seguridad nacional. La atención se centra en la protección de infraestructuras

[71] CASTILLO PARRA, Xenia Yaqueline. Normatividad de ciberseguridad en el sector financiero colombiano. [en línea]. 2018. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/8625

[72] VILLAMIL, Ximena Andrea Cujabante, et al. Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. [en línea]. 2020. Disponible en Internet: https://revistacientificaesmic.com/index.php/esmic/article/view/588

críticas y la ciberdefensa del país en situaciones que podrían comprometer la seguridad nacional.[73]

Centro Cibernético Policial: Este centro se dedica a investigaciones criminales relacionadas con información y datos en el dominio digital.[74]

Grupo de Respuesta COLCERT: Este equipo es responsable de coordinar la ciberseguridad y la ciberdefensa a nivel nacional. Su objetivo es prevenir, detectar y responder a amenazas y ciberataques que puedan afectar a Colombia.[75]

Estos organismos trabajan en conjunto con el gobierno y otras entidades para fortalecer la ciberseguridad y la ciberdefensa en el país. Su trabajo abarca desde responder a incidentes cibernéticos hasta prevenir e investigar delitos cibernéticos, contribuyendo significativamente a la seguridad digital de Colombia

6.1.1 Seguridad Digital en Colombia: Evaluación de la Efectividad de las Políticas y Normativas Vigentes.

En Colombia, a pesar de la creación de legislaciones durante varios años para sancionar los delitos cibernéticos, se sigue observando un aumento en los cibercrímenes, ya que a menudo es difícil identificar a los responsables de los ciberataques. A pesar de los esfuerzos legislativos y normativos para abordar este problema, las amenazas cibernéticas continúan siendo frecuentes debido al aumento de la participación en procesos digitales. El Conpes 3701 de 2011 marcó el inicio de los lineamientos de ciberseguridad y ciberdefensa, y junto con el Conpes 3854, ayuda a fortalecer las capacidades para identificar, gestionar y mitigar los riesgos de seguridad digital en un entorno digital, promoviendo la colaboración entre las partes interesadas[76].

Cómo indica Mintic[77], la seguridad digital de Colombia es el resultado de un proceso participativo que involucra al sector privado, el gobierno, la industria de tecnologías de la información y la academia. Basado en recomendaciones de organismos internacionales como la OCDE y la OEA, así como en grupos de trabajo colaborativos entre el Departamento de Planificación Nacional, el Ministerio de Tecnología de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y otras entidades relacionadas con la seguridad digital.

---

[73] SÁNCHEZ PINEDA, Julie Andrea. Estrategias nacionales de ciberseguridad en perspectiva comparada: lecciones y aprendizajes para el caso colombiano. [en línea]. 2022. Disponible en Internet: https://bdigital.uexternado.edu.co/entities/publication/387c0817-be23-4e1e-9be3-3f1584dfeb7e

[74] Ibid.

[75] Ibid.

[76] BUENO MUNAR, Laura Daniela, et al. Ciberseguridad en Colombia, avances y retos.pp.7-10.

[77] MINTIC. [Sitio Web]. Política de Seguridad Digital. Disponible en internet: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital

La información y datos son fundamentales en el entorno digital, y varias regulaciones buscan protegerlos, como las leyes de privacidad y los derechos humanos en el ciberespacio. En Colombia, la normativa de protección de datos ha progresado, especialmente en la lucha contra el crimen cibernético, con algunos sectores implementando regulaciones más estrictas en ciberseguridad[78].

Para que las políticas y normativas en materia de ciberseguridad sean verdaderamente efectivas, es crucial que las organizaciones se familiaricen con las leyes aplicables en Colombia. De esta manera, podrán establecer las medidas necesarias para garantizar la protección de la información y de los sistemas. Es importante tener en cuenta que el incumplimiento de ciertas normativas puede dar lugar a sanciones administrativas y, en algunos casos, a consecuencias legales de carácter penal, dependiendo de la ley infringida. Por lo tanto, el conocimiento y el cumplimiento de estas regulaciones son esenciales para mantener la integridad y la seguridad de la información en un entorno digital cada vez más complejo y vulnerable[79].

En resumen, las leyes y normativas de ciberseguridad pueden ser efectivas, pero su eficacia depende en gran medida de que las organizaciones las implementen adecuadamente. Si no se acompañan de medidas de ciberseguridad, estas regulaciones pueden resultar insuficientes y no brindar la protección necesaria para la información. Es esencial que las organizaciones realicen evaluaciones periódicas de su seguridad digital para identificar posibles incumplimientos normativos y anticiparse a posibles sanciones.

[78] CANO MARTÍNEZ, Jeimmy José. Prospectiva de ciberseguridad nacional para Colombia a 2030. [en línea]. 2022. Disponible en http://www.scielo.org.co/scielo.php?pid=S1900-65862022000400814&script=sci_arttext

[79] JUSTICIA DIGITAL. [Blog]. Ciberseguridad en Colombia: ¿Cómo son protegidos los datos desde el Sistema Judicial?.2022. Disponible en Internet: https://lajusticiadigital.com/blog/ciberseguridad-en-colombia

7. MÉTODOS Y ESTRATEGIAS DE LA CIBERSEGURIDAD

La ciberseguridad se ha convertido en una preocupación cada vez mayor para las organizaciones, tanto grandes como pequeñas, en todo el mundo. Los avances tecnológicos y la creciente dependencia de las empresas en los sistemas y aplicaciones digitales han aumentado significativamente los riesgos y las amenazas cibernéticas. Por lo tanto, se han desarrollado varios métodos y estrategias de ciberseguridad para proteger los sistemas y la información de las organizaciones.

Uno de los métodos de ciberseguridad más eficaces es la implementación de medidas técnicas de seguridad. Esto puede incluir el uso de firewalls, sistemas de detección y prevención de intrusiones, soluciones de encriptación y herramientas de análisis de seguridad. Los firewalls son una barrera de protección esencial que ayuda a filtrar el tráfico de red no autorizado y protege la red de intrusiones externas. Los sistemas de detección y prevención de intrusiones identifican y bloquean los intentos de ataque, mientras que la encriptación ayuda a proteger los datos confidenciales[80].

Otra estrategia importante de ciberseguridad es el desarrollo de políticas y procedimientos de seguridad claros. Las políticas y procedimientos pueden abordar el acceso a los datos, la gestión de contraseñas, la autenticación, la gestión de incidentes y otros temas relacionados con la ciberseguridad. Las políticas y procedimientos efectivos son esenciales para garantizar que todas las partes interesadas entiendan los riesgos y las responsabilidades de la ciberseguridad.

Las pruebas de penetración y las evaluaciones de vulnerabilidades también son métodos críticos de ciberseguridad. Las pruebas de penetración implican la simulación de un ataque cibernético para identificar las debilidades en los sistemas y aplicaciones y corregirlas antes de que sean explotadas por los atacantes. Las evaluaciones de vulnerabilidades ayudan a las organizaciones a identificar las debilidades de seguridad en sus sistemas y aplicaciones, para que puedan tomar medidas para corregirlas antes de que sean explotadas por los atacantes.

La formación y concienciación del personal es otro método importante de ciberseguridad. Las organizaciones deben formar y concienciar a sus empleados sobre las amenazas cibernéticas y cómo prevenirlas. Esto puede incluir sesiones

[80] GARCIA, Vanesa. [Sitio web]. Así debe realizarse una correcta estrategia de ciberseguridad. 2022. Disponible en Internet: https://revistabyte.es/ciberseguridad/ciberseguridad-estrategia/

de formación, campañas de concienciación y simulaciones de ataques de phishing. Al formar a los empleados, se les empodera para tomar medidas proactivas para proteger sus sistemas y datos.
La gestión de parches y actualizaciones también es crucial para la ciberseguridad. Las organizaciones deben asegurarse de que sus sistemas y aplicaciones estén actualizados con los últimos parches de seguridad y actualizaciones para minimizar las vulnerabilidades de seguridad. Las actualizaciones y los parches pueden proporcionar protección adicional contra amenazas emergentes.

Los planes de contingencia y recuperación de desastres son otra estrategia importante de ciberseguridad. Los planes de contingencia ayudan a minimizar el tiempo de inactividad y recuperarse rápidamente de los ataques cibernéticos y otros desastres. Las organizaciones deben tener planes detallados que aborden la recuperación de datos, la restauración de sistemas y la continuidad del negocio.

7.1 Marcos de trabajo de ciberseguridad.

Los marcos de ciberseguridad son esencialmente un sistema de estándares, directrices y mejores prácticas para gestionar los riesgos emergentes en el mundo digital. Por lo general, esto se alinea con los objetivos de seguridad de una organización, como evitar el acceso no autorizado a sistemas con controles. A continuación, se identifican algunos de los marcos de ciberseguridad más destacados:
NIST: El marco de ciberseguridad del NIST (Instituto Nacional de Estándares y Tecnología) fue diseñado principalmente para proteger la infraestructura crítica, pero sus principios y enfoque se pueden aplicar a una amplia gama de organizaciones que buscan fortalecer su seguridad. Este marco proporciona un conjunto integral de mecanismos centrados en identificar, proteger, detectar, responder y recuperarse de las amenazas cibernéticas.[81]
ISO27000: La familia ISO/IEC es un conjunto de normas de seguridad que abarca diversas áreas, incluyendo ISO 27001 para la gestión de seguridad de la información, ISO 27005 para la gestión de riesgos, ISO 27031 para la continuidad del negocio, y ISO 27035 que ofrece buenas prácticas para la gestión de seguridad de la información. Estos marcos de referencia son fundamentales para implementar procesos efectivos en una organización y garantizar un enfoque completo hacia la seguridad de la información.[82]

[81] GUTIERREZ, Norman. [Blog]. Marcos de Ciberseguridad: La Guía Definitiva.2020. Disponible en Internet: https://preyproject.com/es/blog/marcos-de-ciberseguridad-la-guia-definitiva
[82] TBSEK. [Blog]. Normas, estándares y marcos de trabajo de seguridad de la información. 2023. Disponible en https://www.tbsek.mx/blog/2023/marzo/38.normasestandaresymarcos.html

COBIT: Es un marco de trabajo que brinda una estructura sólida para la gestión de la seguridad de la información, abarcando procesos, recursos humanos, tecnologías y la organización en su conjunto. Este marco está diseñado para ayudar a las organizaciones a establecer y mantener controles efectivos en materia de seguridad de la información, garantizando así la integridad, confidencialidad y disponibilidad de los activos digitales.[83]

ITIL: Es una guía de buenas prácticas diseñada para la gestión de servicios de tecnologías de la información (TI). Esta guía ITIL ha sido creada para abordar de manera integral la infraestructura, el desarrollo y las operaciones de TI, con el objetivo de dirigirlas hacia la mejora de la calidad del servicio, de modo que las organizaciones pueden garantizar la eficiencia y calidad de los servicios de TI.[84]

CIS: Constituyen un conjunto de mejores prácticas diseñadas para proporcionar a las organizaciones una guía concreta y precisa para lograr sus metas y objetivos. Estos controles se han creado con la intención de cumplir con los requisitos establecidos en diversos marcos legales, regulaciones y normativas.[85]

MITRE ATTQ&CK: Se basa en ofrecer una serie de matrices en las que se detallan las tácticas de ataque más habituales, junto con recomendaciones sobre cómo afrontarlas. Su flexibilidad le permite centrarse en cualquier punto de la cadena de ciberataque o explorar objetivos y tipos de ataques específicos para adaptar un marco de defensa personalizado.[86]

Los diversos marcos de ciberseguridad proporcionan un conjunto de mejores prácticas que desempeñan un papel fundamental en el fortalecimiento de la seguridad de los activos digitales y la información de una organización. Estas mejores prácticas contribuyen a prevenir la violación de datos y a mantener la integridad y confidencialidad de la información sensible. Además, permiten una evaluación constante de la efectividad de los controles de seguridad establecidos por el marco, lo que posibilita una mejora continua en la postura de seguridad cibernética de la organización.

7.1.1 Métodos efectivos para implementar la ciberseguridad en las organizaciones

Existen varios métodos efectivos para proteger la información de las organizaciones, algunos de los cuales se describen a continuación:

---

[83] Ibid.

[84] GLOBALSUITE. [Blog]. ¿Qué es ITIL y para qué sirve?.2023. Disponible en Internet: https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/

[85] AWS. [Sitio web]. ¿En qué consisten los puntos de referencia del CIS?. Disponible en Internet: https://aws.amazon.com/es/what-is/cis-benchmarks/

[86] CONNECTIS. [Blog]. Los cinco principales marcos de ciberseguridad. Disponible en internet: https://www.connectis.tech/es/the-top-five-cyber-security-frameworks/

1. Implementar medidas técnicas de seguridad: esto incluye el uso de firewalls, sistemas de detección y prevención de intrusiones, soluciones de encriptación y herramientas de análisis de seguridad. Los firewalls actúan como una barrera de protección esencial que ayuda a filtrar el tráfico de red no autorizado y protege la red de intrusiones externas. Los sistemas de detección y prevención de intrusiones identifican y bloquean los intentos de ataque, mientras que la encriptación ayuda a proteger los datos confidenciales.
2. Desarrollar políticas y procedimientos de seguridad claros: las políticas y procedimientos pueden abordar el acceso a los datos, la gestión de contraseñas, la autenticación, la gestión de incidentes y otros temas relacionados con la ciberseguridad. Las políticas y procedimientos efectivos son esenciales para garantizar que todas las partes interesadas entiendan los riesgos y las responsabilidades de la ciberseguridad.
3. Realizar pruebas de penetración y evaluaciones de vulnerabilidades: las pruebas de penetración implican la simulación de un ataque cibernético para identificar las debilidades en los sistemas y aplicaciones y corregirlas antes de que sean explotadas por los atacantes. Las evaluaciones de vulnerabilidades ayudan a las organizaciones a identificar las debilidades de seguridad en sus sistemas y aplicaciones, para que puedan tomar medidas para corregirlas antes de que sean explotadas por los atacantes.
4. Capacitar y concienciar al personal: las organizaciones deben formar y concienciar a sus empleados sobre las amenazas cibernéticas y cómo prevenirlas. Esto puede incluir sesiones de formación, campañas de concienciación y simulaciones de ataques de phishing. Al formar a los empleados, se les empodera para tomar medidas proactivas para proteger sus sistemas y datos.
5. Gestionar parches y actualizaciones: las organizaciones deben asegurarse de que sus sistemas y aplicaciones estén actualizados con los últimos parches de seguridad y actualizaciones para minimizar las vulnerabilidades de seguridad. Las actualizaciones y los parches pueden proporcionar protección adicional contra amenazas emergentes.
6. Implementar planes de contingencia y recuperación de desastres: los planes de contingencia ayudan a minimizar el tiempo de inactividad y recuperarse rápidamente de los ataques cibernéticos y otros desastres. Las organizaciones deben tener planes detallados que aborden la recuperación de datos, la restauración de sistemas y la continuidad del negocio en caso de una interrupción.

En resumen, la protección de la información de las organizaciones es una tarea crítica y continua que requiere una combinación de medidas técnicas, políticas y procedimientos efectivos, pruebas regulares, capacitación y concienciación del personal y planes de contingencia. La implementación de estos métodos y estrategias de ciberseguridad puede ayudar a reducir significativamente los riesgos y las amenazas cibernéticas y proteger la información valiosa de la organización[87].

7.1.2 Estrategias efectivas para implementar la ciberseguridad en las organizaciones

Además de los métodos mencionados anteriormente, existen algunas estrategias efectivas que las organizaciones pueden implementar para proteger su información[88]:

1. Adoptar un enfoque de seguridad en capas: Las organizaciones deben implementar múltiples capas de seguridad en su infraestructura de TI para protegerse contra las amenazas cibernéticas. Esto incluye la implementación de cortafuegos, antivirus, detección de intrusiones, autenticación multifactorial, cifrado y monitoreo de seguridad continuo. La combinación de estas tecnologías crea una defensa en profundidad, lo que hace más difícil para los atacantes penetrar en el sistema.
2. Implementar políticas de gestión de acceso: Las organizaciones deben limitar el acceso a la información sensible solo a aquellos empleados que lo necesiten para realizar sus funciones. La implementación de políticas de gestión de acceso ayuda a reducir la posibilidad de que la información confidencial sea accedida por personas no autorizadas.
3. Establecer una cultura de seguridad: Las organizaciones deben establecer una cultura de seguridad donde la seguridad cibernética sea una prioridad en todos los niveles de la organización. Esto incluye la educación y concienciación de los empleados sobre las amenazas cibernéticas y la implementación de prácticas de seguridad sólidas, como la creación de contraseñas fuertes y el uso de autenticación multifactorial.

[87] CORPONET. [blog]. CASTRO, Julio. Ciberseguridad: concepto, tipos, amenazas y estrategias. 2022. Disponible en Internet: https://blog.corponet.com/ciberseguridad-concepto-tipos-amenazas-estrategias

[88] EUNCET BUSINESS SCHOOL Y PWC ESPAÑA. [blog]. Estrategia de ciberseguridad: panorama actual e implementación en la empresa. Disponible en Internet: https://blog.euncet.com/beneficios-plan-estrategico-ciberseguridad/

4. Realizar pruebas de simulación de ataques: Las organizaciones deben realizar pruebas de simulación de ataques para evaluar la efectividad de sus medidas de seguridad y para identificar debilidades en su infraestructura. Estas pruebas pueden ayudar a las organizaciones a mejorar sus medidas de seguridad antes de que un atacante real pueda explotar las vulnerabilidades.
5. Proteger los dispositivos móviles: Los dispositivos móviles son un vector de ataque común utilizado por los atacantes. Las organizaciones deben implementar políticas de seguridad para dispositivos móviles que incluyan la autenticación multifactorial y la encriptación de datos para proteger la información confidencial que se almacena o se accede desde dispositivos móviles.
6. Colaborar con expertos en ciberseguridad: Las organizaciones pueden colaborar con expertos en ciberseguridad externos para identificar amenazas emergentes y tomar medidas proactivas para proteger su infraestructura. Los expertos en ciberseguridad pueden proporcionar asesoramiento y orientación en la implementación de políticas y procedimientos de seguridad, pruebas de seguridad y la gestión de incidentes de seguridad.

En resumen, la implementación de estas estrategias efectivas puede ayudar a las organizaciones a proteger su información y reducir el riesgo de un ataque cibernético exitoso. La ciberseguridad debe ser una prioridad en todas las organizaciones, y la implementación de políticas y medidas de seguridad efectivas puede ayudar a proteger a la organización contra las amenazas cibernéticas en constante evolución.

8. MECANISMOS Y BUENAS PRACTICAS PARA LA GESTIÓN DE RIESGOS

La Gestión de Riesgos de la Información (IRM) es un proceso fundamental que implica la identificación, evaluación, mitigación y control de los riesgos relacionados con la información y la seguridad dentro de una organización. El objetivo es mantener un nivel aceptable de riesgo y proteger los activos de información.

Es importante reconocer la diversidad de categorías de riesgos a los que las organizaciones pueden enfrentarse. A continuación, se definen algunas de estas categorías[89]:

Daños Físicos: Estos riesgos se materializan a través de eventos como inundaciones, cortes de energía, desastres naturales e incendios. Pueden dañar la infraestructura física y afectar gravemente la disponibilidad de los recursos y datos críticos de la organización.

Acciones Humanas: Los riesgos asociados con las acciones humanas son especialmente relevantes, ya que pueden ser tanto accidentales como deliberados. Los errores humanos, causados a menudo por falta de capacitación o conocimiento, pueden exponer a la organización a amenazas inesperadas.

Fallo de Sistemas: Estos riesgos se manifiestan cuando los sistemas y dispositivos informáticos experimentan fallas técnicas o mal funcionamiento. Estas interrupciones pueden poner en riesgo la integridad de los datos y la continuidad de las operaciones de la organización.

Ataques Externos e Internos: Los ataques cibernéticos pueden ser de origen externo, como los perpetrados por piratas informáticos y malware, o internos, involucrando a empleados deshonestos o personas con acceso privilegiado. Estos ataques suelen ser intencionados y pueden comprometer la seguridad de la organización.

Uso Indebido de la Información: La divulgación no autorizada de información sensible o confidencial representa un riesgo significativo. Compartir datos cruciales fuera de la organización puede exponerla a amenazas, como el robo de datos y la pérdida de ventajas competitivas.

Pérdida de Información: La pérdida de datos, ya sea de manera intencionada o accidental, puede tener graves repercusiones en la continuidad de las operaciones y la toma de decisiones de la organización.

Errores de Aplicaciones: Los errores en aplicaciones y software, como el ingreso de datos erróneo y vulnerabilidades de seguridad, pueden dar lugar a problemas operativos y amenazas a la seguridad de la información.

---

[89] VILLAMIL BELTRAN, Wilmar Fabian. Gestión de riesgos en entidades del gobierno en Colombia. [en línea]. 2019. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/6351

En un entorno económico globalizado, las organizaciones enfrentan mayores amenazas debido a la falta de políticas para identificar, analizar, valorar y abordar riesgos y vulnerabilidades cibernéticas. La ausencia de medidas de control adecuadas puede llevar a ataques cibernéticos, fraudes financieros y la pérdida de información crítica para la toma de decisiones. Para abordar estas amenazas, se han desarrollado métricas como el Sistema de Puntuación de Vulnerabilidad Común (CVSS, 2014), que utiliza tres categorías de métricas (base, temporal y de entorno), cada una con submétricas para evaluar y calificar los riesgos y vulnerabilidades cibernéticas[90].

Es importante que las organizaciones reconozcan la importancia de comprender y gestionar los riesgos que enfrentan. Un mecanismo eficaz de gestión de riesgos implica una serie de pasos importantes, comenzando con la identificación de riesgos.

Como mencionó Mintic[91], el proceso de gestión de riesgos generalmente sigue los siguientes pasos:

Identificación de riesgos: Es necesario identificar las causas que puedan afectar los procesos de seguridad, identificar activos críticos y mantener un inventario de activos de información confidencial. Esto implica identificar activos críticos, amenazas que podrían afectarlos y vulnerabilidades existentes en una organización.

Análisis de riesgos: implica la evaluación detallada de activos, amenazas y riesgos para comprender su probabilidad y su impacto. Esto permite priorizar los riesgos y determinar cuáles necesitan atención inmediata.

Evaluación de riesgos: Es esencial para valorar la eficacia de los controles existentes y determinar qué controles adicionales son necesarios para mitigar los riesgos. Esta evaluación implica el análisis de la probabilidad de ocurrencia y el impacto en caso de que un riesgo se materialice. La valoración de riesgos se realiza de manera cualitativa para comprender la efectividad de los controles y la severidad de los riesgos.

Tratamiento de riesgos: Durante esta etapa, se desarrollan estrategias para abordar los riesgos, que pueden incluir la implementación de controles adicionales, la transferencia de riesgos o la aceptación de riesgos dentro de niveles tolerables. Se inicia evaluando los controles existentes en la organización, considerando su descripción, formalidad y efectividad, comparándolos con los criterios previamente definidos en las etapas de identificación y análisis de riesgos. El objetivo es seleccionar los controles más efectivos para reducir la exposición al riesgo.

[90] FERNÁNDEZ, OPT.cit.,p 24

[91] MINTIC. [Sitio Web]. Guía de gestión de riesgos. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Posteriormente, se realiza un nuevo cálculo comparativo con los criterios establecidos para lograr un nivel de riesgo aceptable en cada proceso relacionado con la seguridad.

Implementación de un plan de administración del riesgo: Una vez identificados y seleccionados los controles más adecuados para lograr un nivel de riesgo aceptable en los procesos dentro del alcance del MSPI, se procede a la elaboración de un plan de tratamiento de riesgos, que incluye aspectos relacionados con la seguridad de la información. Este plan detalla cómo se abordarán los riesgos, las acciones específicas que se llevarán a cabo y quiénes serán responsables de su implementación. El plan proporciona un desglose detallado de cada acción, sus etapas y procedimientos, lo que facilita la supervisión y el seguimiento durante la ejecución. El objetivo del plan es establecer medidas concretas para gestionar y mitigar los riesgos de manera efectiva.

En resumen, la gestión efectiva de riesgos requiere la implementación de mecanismos y buenas prácticas. Algunas de estas buenas prácticas[92] clave incluyen:

Monitoreo: Implementar sistemas de seguimiento y monitoreo en la red para detectar posibles amenazas y vulnerabilidades.

Participación de la alta dirección: Obtener la aprobación y atención de la alta dirección es esencial para llevar a cabo una estrategia efectiva de gestión de riesgos.

Capacitación: Proporcionar capacitación a las partes interesadas para evitar comprometer la seguridad de la información y contar con programas de formación en seguridad de la información y gestión de riesgos.

Enfoque de gobernanza TI: Establecer un marco de seguridad que se alinee con las estrategias y sistemas de gestión de riesgos existentes, lo que permite identificar brechas de seguridad y responder eficazmente a incidentes.

Documentación: Mantener documentadas las políticas, procedimientos, procesos y protocolos de seguridad para garantizar una comunicación directa y sin alteraciones a todas las partes interesadas de la organización. Estas prácticas son esenciales para gestionar los riesgos de manera efectiva.

8.1 Prevención y defensa de seguridad digital en las organizaciones.

[92] ESCUELA EUROPEA DE EXCELENCIA. [blog]. 10 mejores prácticas de ciberseguridad para las organizaciones.2020. Disponible en Internet: https://www.escuelaeuropeaexcelencia.com/2020/11/10-mejores-practicas-de-ciberseguridad-para-las-organizaciones/

Las vulnerabilidades de seguridad digital en las empresas pueden causar problemas financieros y disruptivas interrupciones en los procesos. Por lo tanto, la ciberseguridad es crucial para garantizar la continuidad del negocio. Los atacantes suelen explotar un conjunto limitado de vulnerabilidades, lo que resalta la importancia de abordar medidas fundamentales de ciberseguridad, como la actualización oportuna de parches, que podría haber prevenido la mayoría de las vulnerabilidades internas[93].

En consecuencia, la implementación de políticas de seguridad digital es esencial en las organizaciones para prevenir incidentes de seguridad y ataques. En este sentido, la Subsecretaría de Defensa ha establecido un conjunto de 4 políticas fundamentales[94]:

Política de Uso Aceptable de Equipos Electrónicos: Esta política define las directrices para el uso adecuado de los recursos electrónicos institucionales, incluyendo computadoras de escritorio, laptops y teléfonos fijos o móviles. Su objetivo es establecer normas que salvaguarden la información y brindar instrucciones sobre el manejo correcto de estos equipos para prevenir riesgos como ataques informáticos, filtración de información y virus.

Uso Aceptable de Correo Electrónico e Internet: Proporciona directrices para un uso adecuado del correo electrónico institucional, redes sociales a través de redes institucionales y la red de la organización, incluyendo el ancho de banda. También se recomienda la implementación de escaneo automático para detectar virus, malware, spam y otras amenazas en el correo electrónico.

Uso de Contraseñas: Esta política se centra en establecer reglas para la creación y uso adecuado de contraseñas al acceder a recursos institucionales a través de computadoras o redes de la organización. Subraya la importancia de seleccionar contraseñas fuertes que sean fáciles de recordar para el empleado, difíciles de adivinar para otros y resistentes a métodos automáticos de descifrado. Se destaca que contraseñas débiles pueden poner en riesgo la seguridad, permitiendo a personas no autorizadas acceder a recursos a los que no deberían tener acceso.

[93] NUVA. [blog]. Seguridad digital: Principales riesgos y cómo prevenirlos en tu empresa. 2022. Disponible en Internet: https://www.nuva.co/seguridad-digital-principales-riesgos-y-como-prevenirlos-en-tu-empresa/

[94] SUBSECRETARIA DE DEFENSA. Manual de Seguridad Digital Políticas de Seguridad Digital y Guías de Ayuda. [en línea]. Disponible en Internet: https://www.ssdefensa.cl/media/2018/02/manseg.pdf

Política de Respuesta a Incidentes de Seguridad Digital: detalla los procedimientos para prevenir incidentes de seguridad y, en caso de que ocurran, describe cómo identificar y mitigar los incidentes. Enfatiza que cualquier persona dentro de una organización puede ser víctima de un incidente de seguridad digital. Aunque la mayoría de las políticas se centran en la prevención, es crucial que, en caso de un incidente, quienes lo detecten sean capaces de reconocerlo y reportarlo para poder abordar las consecuencias del incidente.

La defensa de seguridad digital y el análisis de riesgos son interdependientes y esenciales para las organizaciones. El análisis de riesgos permite identificar amenazas y vulnerabilidades, fortaleciendo la seguridad y la comunicación. Dado que los riesgos evolucionan con el tiempo y el contexto, los análisis periódicos son cruciales. Este proceso evalúa el riesgo como amenaza por vulnerabilidad dividido por capacidad. Para organizaciones en contextos complejos o en acciones de alto riesgo, como demandas legales, los análisis de riesgos son fundamentales. Mejorar las capacidades en defensa digital requiere compromiso y práctica constante. Ante ataques, buscar apoyo y formar un equipo de confianza es crucial[95].

La defensa de seguridad digital requiere buenas prácticas, tecnologías y políticas para proteger los sistemas de información contra amenazas cibernéticas. Esto incluye medidas como la protección contra malware, la actualización de sistemas, el uso de cifrado, el respaldo de datos y la implementación de planes de seguridad digital específicos para cada organización.

Conforme a IBM[96], la implementación de controles de seguridad abarca la seguridad física, digital, ciberseguridad y seguridad en la nube. Esto se hace para establecer barreras contra intrusiones, prevenir accesos no autorizados, mitigar ataques DDoS y garantizar la protección de datos y cargas de trabajo. En resumen, es vital reconocer que, al igual que existen mecanismos para gestionar riesgos, también hay enfoques para prevenir y defender la seguridad digital en las organizaciones, evitando incidentes perjudiciales.

[95] PAEZ, Córdova Anais, IBAÑEZ, Edison, FINLAY, Jonathan. [Sitio Web]. Defensa digital para organizaciones sociales. 2021. Disponible en Internet: https://www.coeescv.net/attachments/article/4341/Guia%20de%20proteccion%20digital.pdf

[96] IBM. [blog]. ¿Qué son los controles de seguridad?. Disponible en Internet: https://www.ibm.com/mx-es/topics/security-controls

CONCLUSIONES

- Se examinó a través de informes de seguridad los riesgos y amenazas más comunes que afectaron a las organizaciones en Colombia y se llevó a cabo una evaluación de su impacto a través del uso del mapa de ciber incidentes proporcionado por la policía, en el cual se identificó las tendencias en las modalidades de ciber incidentes. Estos informes suministraron información valiosa sobre las vulnerabilidades y peligros recurrentes.
- En el presente trabajo, se identificaron las amenazas y riesgos más recurrentes en las organizaciones. Entre estas amenazas se destacan el phishing, el ransomware, las estafas a través de redes sociales, los ataques de fuerza bruta, los ataques DDoS y las vulnerabilidades en los sistemas, siendo las principales preocupaciones en el ámbito de la seguridad cibernética.
- Se determinó la efectividad de las políticas, normativas y lineamientos generados por el gobierno nacional de Colombia para garantizar la seguridad digital en las organizaciones. Se concluye que estas regulaciones ofrecen respaldo al proporcionar directrices para la protección de datos y la mejora de la eficiencia en el campo de la ciberseguridad en el país.
- Se identificó que, además de las regulaciones, existen organismos gubernamentales que desempeñan un papel fundamental en el fortalecimiento de la ciberseguridad. Estos organismos colaboran en la prevención, detección y respuesta a amenazas, investigando actividades criminales en el ámbito digital y proporcionando respuestas efectivas ante incidentes.
- Se identifico los métodos y estrategias de ciberseguridad que pueden fortalecer y complementar las políticas de seguridad digital en Colombia. Esto se logra a través de la implementación de herramientas de seguridad perimetral, el desarrollo de políticas de seguridad, la capacitación del personal en temas cibernéticos, la creación de conciencia y el establecimiento de planes de contingencia.
- Se identificó que existen marcos de trabajo que fortalecen la gestión de riesgos de seguridad en una organización, como el marco NIST, ISO 27000, COBIT e ITIL. Estos marcos proporcionan directrices valiosas para mejorar los procesos de seguridad.
- Se llevó a cabo la evaluación de los mecanismos y buenas prácticas para la gestión de riesgos, la prevención y la defensa de la seguridad digital en organizaciones. Durante este proceso, se identificaron las categorías de

riesgos y se exploraron los mecanismos que pueden implementarse siguiendo la guía de gestión de riesgos.

- Se identifico la importancia de las políticas en el ámbito de la seguridad digital, y se estableció la relación entre la seguridad digital y el análisis de riesgos.

RECOMENDACIONES

- Identificar riesgos, vulnerabilidades y amenazas, realizar pruebas de penetración y mantener sistemas actualizados para proteger la operación de la organización.
- Priorizar la seguridad digital y adquirir conocimientos sobre las tácticas de los atacantes para fortalecer las infraestructuras, ya sea infraestructuras on-premise o en la nube.
- Analizar y comprender cómo las regulaciones pueden respaldar la implementación y utilización de tecnologías para asegurar la seguridad de los datos, activos y la continuidad del negocio.
- Implementar medidas que aseguren la protección de los datos en el entorno digital y llevar a cabo evaluaciones periódicas para verificar el cumplimiento de las regulaciones.
- Implementar un marco de trabajo para fortalecer la gestión de servicios y riesgos, y evaluar la existencia de políticas y sistemas efectivos para la protección de la información.
- Aplicar medidas técnicas, pruebas periódicas y concienciación del personal debido al riesgo de ataques cibernéticos.
- Establecer prácticas regulares y hábitos para mantenerse actualizado en materia de seguridad digital.
- Establecer barreras efectivas contra intrusiones, prevenir accesos no autorizados, mitigar ataques DDoS y proteger datos y cargas de trabajo.

BIBLIOGRAFÍA

ACOSTA David. [Sitio web]. ¿Qué es PCI DSS?. 2022.Consultado el 19 de marzo de 2023. Disponible en Internet: https://www.pcihispano.com/que-es-pci-dss/

ALMONACID DE CÁRDENAS, Álvaro. Auditoría técnica de seguridad: análisis y explotación de vulnerabilidades. [en línea]. Trabajo de grado. Universidad politécnica de Madrid, 2019. Consultado el 30 de marzo de 2023. Disponible en Internet: https://oa.upm.es/id/eprint/56124

ALTA CONSEJERIA DISTRITAL. Conpes 3701 DE 2011. [en línea]. 2011.Disponible en Internet: https://tic.bogota.gov.co/transparencia/marco-legal/normatividad/conpes-3701-2011

ALVINO, Clay. [Sitio web]. Estadísticas de la situación digital de Colombia en el 2020-2021. 2021. Consultado el 5 de abril de 2023. Disponible en Internet: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2020-2021

APONTE, D. M. la república. Obtenido de Ciberseguridad: Empresas Bajo Ataque. [en línea]. 2023.Consultado el 2 de marzo de 2023. Disponible en Internet: https://www.larepublica.co/analisis/diego-molano-aponte-3548807/ciberseguridad-empresas-bajo-ataque

AVG. [blog]. ¿Qué es el ransomware?. Consultado el 12 de marzo de 2023.Disponible en Internet: https://www.avg.com/es/signal/what-is-ransomware

AWS. [Sitio web]. Controlar el tráfico hacia las subredes utilizando las ACL de red. Consultado el 10 abril de 2023. Disponible en Internet: https://docs.aws.amazon.com/es_es/vpc/latest/userguide/vpc-network-acls.html

AWS. [Sitio web]. ¿Qué es la ciberseguridad?. Consultado el 7 abril de 2023. Disponible en Internet: https://aws.amazon.com/es/what-is/cybersecurity/

AWS. [Sitio web]. ¿En qué consisten los puntos de referencia del CIS?. Consultado el 22 octubre de 2023. Disponible en Internet: https://aws.amazon.com/es/what-is/cis-benchmarks/

BOJORQUEZ HUANCA, Jeymi Shirley. Ciberseguridad. [en línea]. Informe profesional de ciberseguridad. Universidad Nacional de Moquegua, 2022. Consultado el 5 abril de 2023. Disponible en Internet: https://repositorio.unam.edu.pe/handle/UNAM/420

BUENO MUNAR, Laura Daniela, et al. Ciberseguridad en Colombia, avances y retos. [en línea]. Ensayo Académico. Universidad Militar Nueva Granada, 2022.Consultado el 21 octubre de 2023. Disponible en Internet: https://repository.unimilitar.edu.co/handle/10654/41303

CAI VIRTUAL. [Sitio Web]. Mapa ciber incidentes. 2022. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://caivirtual.policia.gov.co/ciberincidentes

CAI VIRTUAL. [Sitio Web]. Mapa ciber incidentes. 2023. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://caivirtual.policia.gov.co/ciberincidentes

CAMARGO, Erney Alberto Ramírez; PINZON, RINCON, Miguel Alberto. La importancia de la seguridad de la información en el sector público en Colombia. [En línea]. Revista Ibérica de Sistemas e Tecnologías de Información. 2022. no 46, p. 87-99. Consultado el 20 de octubre de 2023. Disponible en Internet:

https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

CANVIA. [blog]. Estas son las 10 amenazas cibernéticas más comunes en empresas.2023. Consultado el 23 de septiembre de 2023. Disponible en Internet: https://www.canvia.com/amenazas-ciberneticas/#:~:text=Las%20amenazas%20cibern%C3%A9ticas%20son%20aquellos,al%20funcionamiento%20de%20la%20organizaci%C3%B3n.

CANO MARTÍNEZ, Jeimmy José. Prospectiva de ciberseguridad nacional para Colombia a 2030. [en línea]. 2022. Consultado el 21 de octubre de 2023. Disponible en http://www.scielo.org.co/scielo.php?pid=S1900-65862022000400814&script=sci_arttext

CASTILLO PARRA, Xenia Yaqueline. Normatividad de ciberseguridad en el sector financiero colombiano. [en línea]. 2018. Consultado el 20 de octubre de 2023. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/8625

CCIT. [Sitio web]. Mejores prácticas para el fortalecimiento de la ciberseguridad empresarial. Consultado el 5 abril de 2023. Disponible en Internet: https://www.ccit.org.co/wp-content/uploads/mejores-practicas-para-la-ciberseguridad-en-las-empresas-vf.pdf

CCIT – TicTac. [Sitio web]. Informe: Evaluación, retos y amenazas a la ciberseguridad. 2021. Consultado el 23 de septiembre de 2023. Disponible en Internet: https://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/

CIBERSEGURIDAD. [Sitio web]. Continuidad de negocio. Consultado el 24 de septiembre de 2023. Disponible en Internet:

https://ciberseguridad.com/normativa/espana/medidas/continuidad-negocio/#Identificar_gastos_adicionales

CTI SOLUCIONES. [blog]. Encriptación de datos para empresas ¿En qué consiste y cuáles son sus ventajas?. Consultado el 19 de marzo de 2023.Disponible en Internet: https://www.ctisoluciones.com/blog/encriptacion-datos-para-empresas

CONGRESO DE COLOMBIA. [Sitio web]. Ley 1273 delitos informáticos. 2009. Consultado el 7 de abril de 2023. Disponible en Internet: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

CONGRESO DE COLOMBIA. [Sitio web]. Ley 1581 de 2012. 2012. Consultado el 7 de abril de 2023. 2012. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

CONGRESO DE LA REPUBLICA DE COLOMBIA. CONPES 3854. [en linea]. Consultado el 25 de septiembre de 2023. Disponible en internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL. CONPES 3701. [en línea]. Consultado el 20 de octubre de 2023. Disponible en internet: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

CONNECTIS. [Blog]. Los cinco principales marcos de ciberseguridad. Consultado el 22 de octubre de 2023. Disponible en internet: https://www.connectis.tech/es/the-top-five-cyber-security-frameworks/

CORPONET. [blog]. CASTRO, Julio. Ciberseguridad: concepto, tipos, amenazas

y estrategias. 2022. Consultado el 12 mayo de 2023. Disponible en Internet: https://blog.corponet.com/ciberseguridad-concepto-tipos-amenazas-estrategias

DOCUSIGN. [blog]. Principales amenazas a la ciberseguridad en las empresas. [en línea]. 2022.Consultado el 15 de marzo de 2023. Disponible en Internet: https://www.docusign.mx/blog/amenazas-la-ciberseguridad

EUNCET BUSINESS SCHOOL Y PWC ESPAÑA. [blog]. Estrategia de ciberseguridad: panorama actual e implementación en la empresa. Consultado el 11 de mayo de 2023. Disponible en Internet: https://blog.euncet.com/beneficios-plan-estrategico-ciberseguridad/

ESCUELA EUROPEA DE EXCELENCIA. [blog]. 10 mejores prácticas de ciberseguridad para las organizaciones.2020. Consultado el 23 de octubre de 2023. Disponible en Internet: https://www.escuelaeuropeaexcelencia.com/2020/11/10-mejores-practicas-de-ciberseguridad-para-las-organizaciones/

FORTINET. [Sitio web]. Definición de Sistema de prevención de intrusiones (IPS). Consultado el 26 de marzo de 2023. Disponible en Internet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips

FERNÁNDEZ, Luis Jonalber, et al. Incidencia del factor humano en la seguridad de la información de las organizaciones públicas de categoría 6. [en línea]. Trabajo de grado. Universidad Nacional Abierta y Distancia UNAD, 2020. Consultado el 5 de mayo de 2023. Disponible en Internet: https://repository.unad.edu.co/handle/10596/38893

FERNÁNDEZ, Enier Enrique Caamaño; HERRERA, Richard de Jesús Gil. Prevención de riesgos por ciberseguridad desde la auditoría forense:

Conjugando el talento humano organizacional. [en línea]. 2020. Consultado el 23 de octubre de 2023. Disponible en Internet: https://www.redalyc.org/journal/5713/571361695004/571361695004.pdf

FUNCION PUBLICA. Decreto 620 de 2020. [en línea]. Consultado el 5 de abril de 2023.Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337

FUNCION PUBLICA. Decreto 338 de 2022. [en línea]. Consultado el 5 de abril de 2023. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

FUNCION PUBLICA. [Sitio Web]. Decreto 1008 de 2018. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902

GAMBOA SUAREZ, José Luis. Importancia de la seguridad informática y ciberseguridad en el mundo actual. [en línea]. 2020. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/8668

GARCÍA FORERO, Luis Felipe Guillermo, et al. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. [en línea]. 2020.Consultado el 8 de marzo de 2023.Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/9545

GARCIA, Vanesa. [Sitio web]. Así debe realizarse una correcta estrategia de ciberseguridad. 2022. Consultado el 10 de mayo de 2023. Disponible en Internet: https://revistabyte.es/ciberseguridad/ciberseguridad-estrategia/

GLOBALSUITE. [Blog]. ¿Qué es ITIL y para qué sirve?.2023. Consultado el 22

de octubre de 2023. Disponible en Internet: https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/

GUTIERREZ, Norman. [Blog]. Marcos de Ciberseguridad: La Guía Definitiva.2020. Consultado el 22 de octubre de 2023. Disponible en Internet: https://preyproject.com/es/blog/marcos-de-ciberseguridad-la-guia-definitiva

GUZMAN, Ana. [Blog]. La importancia de la Ciberseguridad en las empresas colombianas.2023. Consultado el 23 de septiembre de 2023. Disponible en Internet: https://welcome.atlasgov.com/es/blog/ciberseguridad/la-importancia-de-la-ciberseguridad-en-las-empresas-colombianas/

HERNÁNDEZ GONZÁLEZ, Holber Steven. Importancia de Estructurar un Gobierno de Seguridad y Ciberseguridad en las Organizaciones. [en línea]. 2022. Consultado el 25 de marzo de 2023. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/12278

IBM. [blog]. ¿Qué son los controles de seguridad?. Consultado el 24 de octubre de 2023. Disponible en Internet: https://www.ibm.com/mx-es/topics/security-controls

IBM. [blog].¿Qué son las amenazas internas?. Consultado el 15 de marzo de 2023. Disponible en Internet: https://www.ibm.com/co-es/topics/insider-threats

INCIBE. [Sitio Web].¿Qué son y para qué sirven los SIEM, IDS e IPS?. 2020 Disponible en https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

INCIBE. [Sitio web]. Balance de Ciberseguridad 2022. 2022. Consultado el 10 de abril de 2023. Disponible en Internet:

https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf

INCIBE. [Sitio Web]. La seguridad vista desde sus inicios. 2015. Consultado el 2 de abril de 2023. Disponible en Internet: https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

INCIBE. [Sitio web]. INCIBE gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020. 2021. Consultado el 2 de marzo de 2023. Disponible en Internet: https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-130000-incidentes-ciberseguridad-durante-el-ano-2020

INFOSECURITY, MEXICO. [blog]. Ciberseguridad. Consultado el 5 de abril de 2023. Disponible en Internet: https://www.infosecuritymexico.com/es/ciberseguridad.html#historia

INTERNATIONALIIT. [Sitio web]. SonicWall: Informe de amenazas cibernéticas. 2023. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://www.internationalit.com/post/sonicwall-informe-de-amenazas-cibern%C3%A9ticas-2023?lang=es

ISACA. [Sitio web]. Roles de las tres líneas de defensa para la seguridad de la información y gobierno. 2019.Consultado el 2 de abril de 2023.Disponible en: https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

ISOTOOLS.Seguridad de la información. [Blog]. ¿Qué situaciones de SI pueden afectar la continuidad del negocio?. 2023. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://www.pmg-ssi.com/2023/05/que-situaciones-de-si-pueden-afectar-la-continuidad-del-negocio/

JUSTICIA DIGITAL. [Blog]. Ciberseguridad en Colombia: ¿Cómo son protegidos los datos desde el Sistema Judicial?.2022. Consultado el 21 de octubre de 2023. Disponible en Internet: https://lajusticiadigital.com/blog/ciberseguridad-en-colombia

KASPERSKY. [Sitio web]. ¿Qué son los bots? Definición y explicación. Consultado el 9 de marzo de 2023. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/what-are-bots

KASPERSKY. [Sitio web]. ¿Qué es una amenaza avanzada persistente (APT)?. Consultado el 12 de marzo de 2023. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

KASPERSKY. [blog]. ¿Qué es la Autenticación de Dos Factores y Dónde Debo Utilizarla?. Consultado el 19 de marzo de 2023.Disponible en Internet: https://latam.kaspersky.com/blog/que-es-la-autenticacion-de-dos-factores-y-donde-debo-utilizarla

KEEPCODING. [blog]. Detección de vulnerabilidades informáticas. 2022.Consultado el 19 de marzo de 2023.Disponible en Internet: https://keepcoding.io/blog/deteccion-de-vulnerabilidades/

LINKEDIN. RENATA COLOMBIA. [Sitio Web]. Colombia segundo lugar en ciberataques en Latinoamérica, conozca los riesgos para evitar incidentes de ciberseguridad.2023. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://www.linkedin.com/pulse/colombia-segundo-lugar-en-ciberataques/?originalSubdomain=es

MCAFEE. [blog]. Qué es un proxy. [en línea].2021. Consultado el 11 de abril de 2023.Disponible en Internet: https://www.mcafee.com/blogs/es-es/privacy-identity-protection/que-es-un-proxy/

MCAFEE. [Sitio web].¿Qué es malware?. Consultado el 9 de marzo de 2023. Disponible en Internet: https://www.mcafee.com/es-co/antivirus/malware.html

MANRIQUE Reyna, V. H. Modelo de ciberseguridad para mejorar la gestión de tecnología de la información en un instituto superior tecnológico público. [en línea]. Tesis de grado. Universidad Cesar Vallejo, 2022. Consultado el 5 de marzo de 2023. Disponible en Internet: https://repositorio.ucv.edu.pe/handle/20.500.12692/84954

MINAMBIENTE. [Sitio web]. Protección de Datos Personales. Consultado el 25 de septiembre de 2023. Disponible en internet: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

MINTIC. [Sitio Web]. En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia. 2022. Consultado el 23 de septiembre de 2023. Disponible en Internet: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

MINTIC. [Sitio Web]. Decreto de seguridad digital.2022. Consultado el 25 de septiembre de 2023. Disponible en internet: https://www.crossbordertech.com/wp-content/uploads/2022/03/Decreto-338-de-8-de-marzo-de-2022-3.pdf

MINTIC. [Sitio Web]. MINTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital.2021. Consultado el 25 de

septiembre de 2023. Disponible en internet: https://gobiernodigital.mintic.gov.co/portal/Noticias/162625:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

MINTIC. [Sitio Web]. Política de Seguridad Digital. Consultado el 21 de octubre de 2023. Disponible en internet: https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/15430:Politica-de-Seguridad-Digital

MINTIC. [Sitio Web]. Guía de gestión de riesgos. Consultado el 23 de octubre de 2023. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. [Sitio Web]. Protección de Datos Personales. Consultado el 19 de marzo de 2023.Disponible en Internet: https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales

MOLINA, J. Orozco, L. Vulnerabilidades de los Sistemas de Información: una revisión. [en línea]. Consultado el 19 de marzo de 2023.Disponible en Internet: https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1

MONTOYA, Yan Cornejo; VERDEZOTO, Victor Hugo; RAMÍREZ, Andrea Villacis. Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad. [en línea]. 2019. Consultado el 6 de mayo de 2023 Disponible en Internet: http://www.imjst.org/wp-content/uploads/2019/02/IMJSTP29120135.pdf

NE, DIGITAL. [blog]. Guía esencial sobre la Ciberseguridad en Colombia.

Consultado el 25 de septiembre de 2023. Disponible en internet https://www.nedigital.com/es/blog/ciberseguridad-en-colombia

NIST. [Sitio Web]. Controles de seguridad y privacidad para sistemas de información y organizaciones.2020. Consultado el 19 de marzo de 2023.Disponible en Internet: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

NORMAS ISO. [Sitio Web]. ISO 27001 seguridad de la información. Consultado el 18 de marzo de 2023. Disponible en Internet: https://www.normas-iso.com/iso-27001/

NUVA. [blog]. Seguridad digital: Principales riesgos y cómo prevenirlos en tu empresa. 2022.Consultado el 24 de octubre de 2023. Disponible en Internet: https://www.nuva.co/seguridad-digital-principales-riesgos-y-como-prevenirlos-en-tu-empresa/

OLAYA OLIVEROS, Alexander. Ataques cibernéticos. [en línea]. Trabajo de grado. Universidad Militar Nueva Granada, 2021. Pp.15-36. Consultado el 2 de mayo de 2023. Disponible en Internet: https://repository.unimilitar.edu.co/handle/10654/39021

OSPINA DÍAZ, M. R., & SANABRIA RANGEL, P. E. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista criminalidad. [en línea]. 2020. Consultado el 1 de mayo de 2023. Disponible en: https://biblat.unam.mx/hevila/Revistacriminalidad/2020/vol62/no2/5.pdf

PANDA. [Sitio web].¿Phishing. Consultado el 10 de marzo de 2023.Disponible en Internet: https://www.pandasecurity.com/es/security-info/phishing/

PAEZ, Córdova Anais, IBAÑEZ, Edison, FINLAY, Jonathan. [Sitio Web]. Defensa digital para organizaciones sociales. 2021. Consultado el 24 de octubre de 2023. Disponible en Internet: https://www.coeescv.net/attachments/article/4341/Guia%20de%20proteccion%20digital.pdf

PIRANI. [Blog]. JIMENEZ, M. Maria.¿Qué pudo causar el ataque cibernético a IFX Networks?.2023. Consultado el 24 de septiembre de 2023. Disponible en Internet: https://www.piranirisk.com/es/blog/posibles-causas-ataque-cibernetico-ifx-networks

PORTAFOLIO. REY, G. Helena. [Sitio web]. Por qué ha crecido la importancia de la ciberseguridad. 2023. Consultado el 3 de abril de 2023. Disponible en Internet: https://www.portafolio.co/economia/finanzas/ciberseguridad-aumenta-a-la-par-de-los-ataques-ciberneticos-579612

RAMÍREZ, Maricela; CORPORATIVA, Responsabilidad Social. EL CONCEPTO DE CIBERSEGURIDAD EN EL ÁMBITO ORGANIZACIONAL. [en línea]. Universidad de granada, 2022. Consultado el 6 de marzo de 2023. Disponible en Internet: https://xxencuentro.aeca.es/wp-content/uploads/2022/09/43estudiante.pdf

REALPE, M.; CANO, J. Amenazas cibernéticas a la seguridad y defensa nacional. Reflexiones y perspectivas en Colombia. [en línea]. 2020. Consultado el 5 de mayo de 2023. Disponible en Internet: https://www.researchgate.net/profile/Jeimy-Cano-M/publication/340465740_Amenazas_Ciberneticas_a_la_Seguridad_y_Defensa_Nacional_Reflexiones_y_perspectivas_en_Colombia/links/5e8fb6dc92851c2f52910dce/Amenazas-Ciberneticas-a-la-Seguridad-y-Defensa-Nacional-Reflexiones-y-perspectivas-en-Colombia.pdf

ROMERO, J. C.Ciberseguridad: Evolución y tendencias. bie3: Boletín IEEE, (23), 460-494. [en línea]. 2021. Consultado el 2 de marzo de 2023. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

NORDVPN. SANCHEZ, O. Laura. [Blog]. La historia de la ciberseguridad. 2022. Consultado el 29 de marzo de 2023. Disponible en Internet: https://nordvpn.com/es/blog/historia-ciberseguridad/

SÁNCHEZ PINEDA, Julie Andrea. Estrategias nacionales de ciberseguridad en perspectiva comparada: lecciones y aprendizajes para el caso colombiano. [en línea]. 2022. Consultado el 20 de octubre de 2023. Disponible en Internet: https://bdigital.uexternado.edu.co/entities/publication/387c0817-be23-4e1e-9be3-3f1584dfeb7e

SOLANO, Brigadier General Ricardo Charry. El riesgo de los ciberataques para Colombia. [en línea]. 2022. Consultado el 5 de mayo de 2023. Disponible en Internet: https://esici.edu.co/wp-content/uploads/2023/02/Boletin_05_V4.pdf

SUBSECRETARIA DE DEFENSA. Manual de Seguridad Digital Políticas de Seguridad Digital y Guías de Ayuda. [en línea]. Consultado el 24 de octubre de 2023. Disponible en Internet: https://www.ssdefensa.cl/media/2018/02/manseg.pdf

TBSEK. [Blog]. Normas, estándares y marcos de trabajo de seguridad de la información. 2023. Consultado el 22 de octubre de 2023. Disponible en https://www.tbsek.mx/blog/2023/marzo/38.normasestandaresymarcos.html

ULLOA MORA, Jimmy. Automatización, ciberseguridad y ciencia de datos: la nueva estrategia empresarial. [en línea]. Trabajo de grado. Instituto Tecnológico De Costa Rica, 2021. Consultado el 8 de mayo de 2023. Disponible en Internet:

https://repositoriotec.tec.ac.cr/handle/2238/13722

VILLAMIL, Ximena Andrea Cujabante, et al. Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. [en línea]. 2020. Consultado el 20 de octubre de 2023. Disponible en Internet: https://revistacientificaesmic.com/index.php/esmic/article/view/588

VILLAMIL BELTRAN, Wilmar Fabian. Gestión de riesgos en entidades del gobierno en Colombia. [en línea]. 2019. Consultado el 23 de octubre de 2023. Disponible en Internet: http://repository.unipiloto.edu.co/handle/20.500.12277/6351