PROPUESTA BASADA EN LA SEGURIDAD LÓGICA PERIMETRAL EN LAS PYMES, COMO ESTRATEGIA PARA LA PROTECCIÓN CONTRA CIBERATAQUES

ROSMEL ACOSTA ESCOBAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

PROPUESTA BASADA EN LA SEGURIDAD LÓGICA PERIMETRAL EN LAS PYME, COMO ESTRATEGIA PARA LA PROTECCIÓN CONTRA CIBERATAQUES

ROSMEL ACOSTA ESCOBAR

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

EDGAR ROBERTO DULCE
Director de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., Fecha sustentación

DEDICATORIA

Dedico este trabajo a mi familia, padres, esposa e hija, quien no pierde la esperanza de seguirme viendo triunfar y siempre cuento con su apoyo incondicional, como también a la universidad que me da la oportunidad de poder realizar mis estudios.

AGRADECIMIENTOS

Dios que nos permite vivir cada día, agradecerle a él de mantener la dicha y las ganas de estudiar, agradecer a la universidad y los diferentes medios que nos brinda para seguir luchando por un sueño hasta poder materializarlo, a la directora Yenny Núñez por sus aportes y análisis profundo al trabajo que me permite tener otro punto de vista para el desarrollo del trabajo.

CONTENIDO

GLOSARIO

- Correo: Es un servicio de red de comunicación asíncrona, que pertenece al grupo de plataforma como servicio (PAAS Platform as a Service).

- Firewall: Herramienta de seguridad, configurado con políticas que permite o deniega el tráfico.

- Hardening: Son las configuraciones de seguridad que se realizan en los sistemas para la protección del hardware como de la información contenida.

- Phishing: Es el engaño por medio de canales electrónicos que utilizan los delincuentes para extraer información.

- SIEM: Sistemas de seguridad informática que: detecta, responde y neutraliza amenazas informáticas.

- Spam: Características para describir a un correo basura, no solicitado

- WAF: Firewall encargado de la seguridad en los servers de aplicaciones

RESUMEN

En la siguiente monografía abarca sobre la importancia de la seguridad lógica perimetral, como estrategia para la protección contra ciberataques en las Pymes, se describen los principales riesgos a los que están expuestos las empresas si no se implementa y se mantiene en desarrollo un sistema de seguridad informática y de información como cualquier otro proceso de su sistema. También se aborda sobre las principales metodologías de ataque cibernéticos y cuál es el ataque que más se materializa. En el desarrollo de la actividad se identifican las primordiales herramientas de seguridad que las organizaciones deben contemplar para asegurar los datos y el sistema de red interno, así mismo sobre que marcos de referencias pueden orientarlo para la aplicación de controles de seguridad.

La seguridad lógica perimetral, cada día toma mayor importancia en las organizaciones, permite asegurar la infraestructura, la red, datos y el control de accesos no autorizados, articulando la seguridad de la información, seguridad informática y recursos humanos permite mantener y poder brindarle al usuario un sistema seguro de comunicación en la red; La construcción de la seguridad lógica perimetral puede apoyarse en metodologías ya conocidas, como la defensa en profundidad, los controles establecidos en el anexo A de norma ISO 27001 (sistema de gestión de seguridad de la información), los CIS controls entre otros, el costo de inversión para un sistema de gestión de seguridad de la información puede ser muy alto, por el cual las organizaciones deben de evaluar el alcance iniciando por los sistemas más críticos, y a medida que se valla desarrollando incluir otras áreas.

ABSTRACT

The following monograph covers the importance of perimeter logical security, as a strategy to protect against cyberattacks in SMEs, it explains the main risks that companies are exposed to if a security system is not implemented and is kept under development. computing and information as any other process on your system. It also addresses the main cyber attack methodologies and which is the attack that materializes the most. In the development of the activity, the main security tools that organizations must consider to secure the data and the internal network system are identified, as well as on which reference frameworks can guide it for the application of security controls.

Perimeter logical security, every day becomes more important in organizations, allows to secure the infrastructure, network, data and the control of unauthorized access, articulating information security, computer security and human resources allows to maintain and be able to provide the user a secure network communication system; The construction of the logical perimeter security can be supported by already known methodologies, such as defense in depth, the controls established in Annex A of the ISO 27001 standard (information security management system), the CIS controls among others, the cost Investment for an information security management system can be very high, for which organizations must evaluate the scope starting with the most critical systems, and as they go to include other areas.

LISTA DE IMÁGENES

LISTA DE TABLAS

INTRODUCCIÓN

El presente trabajo de monografía que lleva como título propuesta basada en la seguridad lógica perimetral en las PYMES, como estrategia para la protección contra ciberataques, tiene como importancia la seguridad en la protección de los datos, tema que ha tomado mucho auge en las organizaciones por el valor que la información representa; Se explicara como se encuentran las pequeñas y medianas empresas en materia de seguridad, cuáles son las herramientas de protección que utilizan; La seguridad es de todos, los ataques afectan la seguridad de una empresa sea PYME o una gran empresa, lo que varía es el método y lo sofisticado del ataque que cada día son más avanzados, alterando la integridad de la información y la disponibilidad de los servicios.

El término de seguridad a cambiado con el avance de la tecnología, la industria tecnológica comenzó asegurando la parte física y dejando a un lado la protección de la información, pero como los métodos de ataques también evolucionaron y no bastaba con una seguridad perimetral si no llevar los métodos de seguridad a la protección de la información, así la información y los servicios empezaron a tomar mayor importancia; Las empresas implementan un sistema de gestión de la seguridad de la información para proteger los activos informáticos y garantizar las características de la información (confidencialidad, integridad y disponibilidad) por medio de la seguridad lógica perimetral, la seguridad informática como método de control, busca la identificación de los activos de información, responsable, quine accede a ellos, como también busca que los usuarios que utilizan recursos de la red estén identificados como los permisos asignados; Para la aplicación de este control la norma ISO 27001 en su anexo A.9 permite una guía clara y de acceso libre y que puede ser consultado en el siguiente link HTTPS://normaiso27001.es/a9-control-de-acceso/

En el documento se identifican métodos de protección de seguridad informática de uso libre, y otros licenciados, de tipo hardware y software, y las ventajas que cada una de estas tiene, entre estas herramientas se encuentran los firewall, políticas de correos, WAF, SIEM y antivirus, cada una cumple una función y controlando el acceso de un objetivo específico, y le permite a la compañía la protección, monitoreo de los recursos y de la red contra diferentes tipos de amenazas, minimizando los principales riesgos asociados a la ciberseguridad con la utilización y parametrización de herramientas de seguridad lógica perimetral y la construcción de una política basada en la prevención de la infraestructura y de la información. Así mismo dar a conocer cuáles son los principales métodos de ataques cibernéticos y el costo que le representa a una empresa sufrir un ataque, así como los riesgos en las aplicaciones web según el proyecto abierto de seguridad de aplicaciones web (OWASP).

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Del informe ESET-security-report-LATAM2020, el 39% de las empresas no cuentan con políticas de seguridad, y apenas un 28% clasifica su información y solo el 48% de las empresas cuentan con las tres medidas básicas de protección (antivirus, backup y firewall)[1], se puede inferir que las pequeñas y medianas empresas están en proceso de creación o no cuentan con una política de seguridad, como tampoco una seguridad lógica perimetral, desconociendo el impacto que pueden sufrir si es materializado un ataque; La inversión en herramienta de protección y en el sistema de gestión de seguridad informática, muchas veces es visto como un gasto y se limita a implementar controles físicos y lógicos de seguridad creando una falsa sensación de protección[2]; Según documentación se tiene que el primer ciberataque de la historia ocurrió en el año 1834 y el primer hacker para el año 1903 realizando una interceptación de transmisión del telégrafo inalámbrico[3], para ese entonces el número de ataques informáticos como los métodos utilizados no eran tan relevantes como en la actualidad, eso quiere decir que los problemas de seguridad informática siempre han existido y con el pasar de los tiempos y el avance tecnológico se han incrementado y pasando a una transformación en la forma del ataque.

Los ataques de ciberseguridad a nivel mundial pueden costar en promedio 600 mil millones de dólares, para la región de AMÉRICA LATINA Y EL CARIBE en el mes de noviembre del 2020 se llegaron a presentar hasta 12.000 intentos de ataques diarios, con un crecimiento del 141% en comparación con el año 2019, en Colombia cerca del 87% de empresas son víctimas de ciberataques y muchos de esos casos no son denunciados, identificando que del 100% de esas empresas atacadas, el 60% incurrieron en costos de 1 millón, 20% hasta 15 millones, 15% hasta 235 millones y 5% hasta 4.000 millones de pesos; complementando con una encuesta realizada por Kaspersky en el año 2019 el 43% de las Pymes en América Latina fue afectada por violación de datos.[4]

---

[1] Welivesecurity. *ESET-security-report-LATAM2020.pdf. [sitio web]. [2020]. Disponible en: HTTPS://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf*

[2] Larepublica. Porcentaje de la población con acceso a internet. [sitio web]. Disponible en: HTTPS://www.larepublica.co/internet%20-economy/cuanto-gastan-las-empresas-para3%20LA%20REP%C3%9ABLICA.%20[sitio%20web].%20Bogot%C3%A1.%20%C2%BFCu%C3%A1nto%20gastan%20las%20empresas%20para%20recuperarse%20despu%C3%A9s%20de%20un%20ciberataque?.%20recuperarse-despues-de-un-ciberataque-2889536

[3] Esedsl. Primer ciberataque de la historia y los ciberataques que han perdurado en el tiempo. *[sitio web]. Disponible en:* HTTPS://www.esedsl.com/blog/primer-ciberataque-historia-y-ciberataques-que-han-perdurado-tiempo

[4] ACIS*. Ciberseguridad: la aliada de las PyMEs durante la realidad actual. [sitio web]. Bogotá. []junio, 2020]. Disponible en: HTTPS://www.acis.org.co/portal/content/noticiasdelsector/ciberseguridad-la-aliada-de-las-pymes-durante-la-realidad-actual*

El aumento de ataque a correos electrónicos por la técnica del phishing o cadenas de mensaje, utilizando la palabra “COVID-19” como señuelos[5], afectó a personas por no realizar verificación de correos y a empresas por no tener una correcta configuración de políticas en la zona del Sistema de Nombre de Dominios (DNS: Domain Name System) de correos, el abrir un correo que contenga estenografía o la ejecución de un malware, expone la infraestructura a cualquier ataque de ciberseguridad, como también a denegación de servicio, saturando los servidor de correos spam, impidiendo su funcionamiento, o colocando otro tipo de malware en los sistema para la captura de datos.

1.2 FORMULACIÓN DEL PROBLEMA

Con el desarrollo de la actividad se propone dar respuesta a, ¿Como la implementación de la seguridad lógica perimetral puede prevenir y minimizar riesgos de ciberseguridad en las Pymes?

[5] aepd. Campañas de phishing sobre el COVID-19. [sitio web]. [12, marzo, 2020]. Disponible en: HTTPS://www.aepd.es/es/prensa-y-comunicacion/blog/campanas-de-phishing-sobre-el-covid-19

2 JUSTIFICACIÓN

La seguridad lógica perimetral es un proceso de planificación y construcción, y no un tema para dejar desactualizado en ninguna empresa, la seguridad lógica perimetral va a caracterizar con buena reputación a la Pyme que gestione la protección de los datos y su infraestructura, con el uso de diferentes herramientas que la llevará a certificarse en ISO (19600 – 9001) y le permitirá la atracción de nuevos clientes, acelerará sus procesos y la mantendrá competitivamente en el mercado.

La seguridad lógica perimetral, la conforman medidas y actividades de seguridad que las empresas establecen para la prevención, detección y recuperación de los activos minimizando los tiempos de respuestas[6]; La tecnología ha ido evolucionando de forma muy rápida y en el mercado existen diferentes tipos de herramientas para la protección a diferentes métodos de ataques, entre las principales herramientas utilizadas para la seguridad lógica perimetral se encuentra, el firewall, políticas de correos, WAF, SIEM y antivirus, cada una cumple una función en controlar el acceso de un objetivo específico, y le permite a la compañía la protección, monitoreo de los recursos y de la red contra diferentes tipos de amenazas, minimizando los principales riesgos asociados a la ciberseguridad con la utilización y parametrización de herramientas de seguridad lógica perimetral y la construcción de una política basada en la prevención de la infraestructura y la información

La utilización de estas herramientas previene de posibles incidentes y sus diferentes vectores que podrían degradar o detener completamente las actividades y/o los servicios, sufriendo perdida o captura de información creando un impacto negativo en la reputación y posible quiebra de la empresa.

[6] avansis. SEGURIDAD PERIMETRAL INFORMÁTICA. QUÉ ES, DEFINICIÓN Y MÉTODOS PARA PROTEGER TU NEGOCIO. [sitio web]. Disponible en: HTTPS://www.avansis.es/ciberseguridad/que-es-seguridad-perimetral/

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Proponer un plan estratégico para las Pymes, basado en la seguridad lógica perimetral como estrategia para la protección contra ciberataques a redes informáticas y de comunicación tomando como referencia el anexo A de la ISO/IEC 27001

3.2 OBJETIVOS ESPECÍFICOS

- Examinar el panorama actual de seguridad informática en las Pymes y los mecanismos que implementan para resguardar sus sistemas de información y de red.
- Establecer políticas, medidas, procedimientos y servicios de seguridad necesarios para implementación de una estrategia basada en la seguridad lógica perimetral para la detección, prevención y recuperación de la información.
- Diseñar un plan estratégico que sirva como guía empleando la seguridad lógica perimetral para la protección de redes informáticas y de comunicación en las Pymes.

4 MARCO REFERENCIAL

En el desarrollo de la temática se abarca el tema de la importancia de la seguridad lógica perimetral en las pymes, dando a conocer las posibles soluciones que se pueden implementar a los tipos de ataques y prevenir posibles incidentes.

Las Pymes como toda empresa debe de conocer a qué riesgos se pueden enfrentar en los diferentes tipos de ataques ciberataques entre algunos como ataque de correo electrónico y ataque al protocolo de escritorio remoto, sabiendo que ninguna red es cien por ciento segura, pero aplicando ciertas medidas de mitigación se tendrá un mayor control ante un posible evento.

Políticas y medidas de seguridad:

- Crear copias de seguridad periódicas incrementales.
- Realizar capacitación a usuarios finales en ciberseguridad.
- Contratación de una herramienta para protección de: software, datos, contraseñas, red, correo.
- Proyectar a servicios en la nube.
- Realizar una identificación de los riesgos asociados a la infraestructura.

Estas son posibles alternativas que las empresas pueden implementar de acuerdo al presupuesto, con un poco más de inversión se pueden hacer dos tipos de auditorías. La primera dirigida a los controles globales conformada por los sistemas de tecnología y de la información, que supervisa características fundamentalmente del funcionamiento para garantizar la seguridad y la continuidad de las plataformas; y otra, una auditoría de propósito específico, encaminada a la revisión de aspectos puntuales en los que se vean amenazas focalizadas para cada empresa.[7]

El software que tiene una mayor propagación y lidera el tema de ataques informáticos es el ransomware[8] (secuestro de datos), encripta los datos de las víctimas, con sus diferentes tipos, entre ellos los siguientes:

- Scareware simula un antivirus, identificando haber encontrado un posible problema en el computador, posteriormente solicita una suma de dinero para solucionarlo.

[7] larepublica. ¿Cuánto gastan las empresas para recuperarse después de un ciberataque? [sitio web]. Bogotá. D.C. La Republica [27, junio, 2019]. Disponible en: HTTPS://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536

[8] Latam. El ransomware: qué es, cómo se lo evita, cómo se elimina. [sitio web]. Disponible en: HTTPS://latam.kaspersky.com/resource-center/threats/ransomware

- Crypto malware con la capacidad de extenderse por las diferentes redes corporativas.
- Lockers bloqueando el sistema operativo por completo impidiendo acceder de ningún modo.
- Doxware aparte de exigir dinero por el rescate, amenaza con publicar la información robada si no recibe el pago.

Estos pagos deben efectuarse por medio de criptomonedas, con el fin de que los atacantes no sean rastreados[9]; el pago del soborno no garantiza que los datos robados sean devueltos en su totalidad, que vuelvan a realizar otro ataque o que esos datos sean vendidos a un tercero.

Una publicación realizada por welivesecurity indica que el ransomware fue la amenaza más activa y efectivas en el 2020, realizando ataques al protocolo de escritorio remoto (RDP) debido a que implanta un exploit en este protocolo, seguido del phishing de correo electrónico y la explotación de otras vulnerabilidades[10], entre ellas los programas de videoconferencias, todos estos ataques aumentaron en el inicio y transcurso de la pandemia debido a una mayor frecuencia en su utilización.

4.1 MARCO TEÓRICO

4.1.1 Índice Nacional De Ciberseguridad (NCSI, National Cyber Security Index)

El objetivo del NCSI es medir los compromisos que han asumido los países que pertenecen a la Unión Internacional de Telecomunicaciones (UIT) en materia de seguridad, y poder detectar deficiencia, servir como guía para la orientación estratégica, apoyar en la creación del marco jurídico, brindar capacitación en ciberseguridad, resaltar practicas idóneas, fortalecer las normas internacionales e incentivar una cultura de la ciberseguridad[11].

4.1.2 Modelo de Madurez de la Capacidad de Ciberseguridad

Busca medir el desarrollo de la capacidad cibernética que tiene un país, como también en materia de educación y formación, esta capacidad se divide en cinco dimensiones (Política y Estrategia de Ciberseguridad, Cultura Cibernética y Sociedad, Educación, Capacitación y Habilidades en Ciberseguridad, Marcos Legales y Regulatorios, Estándares, Organizaciones y Tecnologías) y cada una está conformada por un conjunto de factores, su objetivo es aumentar la dimensión y la

[9] Latam. El ransomware: qué es, cómo se lo evita, cómo se elimina. [sitio web]. Disponible en: HTTPS://latam.kaspersky.com/resource-center/threats/ransomware

[10] Iicybersecurity. Plan de seguridad informática – seguridad perimetral informática y seguridad lógica. [sitio web]. Disponible en: HTTPS://www.iicybersecurity.com/seguridad-logica-seguridad-perimetral.html

[11] itu. Los países refuerzan sus estrategias de ciberseguridad. [sitio web]. [29, junio, 2021]. Disponible en: HTTPS://www.itu.int/es/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx

efectividad en el crecimiento de la capacidad en ciberseguridad mediante conocimiento e investigación[12].

4.1.3 La seguridad informática

La seguridad informática es muy amplia y abarca muchos temas desde diferentes puntos contextuales, todas apuntando a un mismo objetivo sobre la protección de activos de información, activos informáticos, protección de las redes de datos, control perimetral entre otros de una compañía, garantizando lo más eficiente que se pueda la disponibilidad, integridad y confiabilidad, llevándola a una confianza y seguridad digital[13].

4.1.4 Seguridad perimetral

La seguridad perimetral es una herramienta de seguridad informática, contiene un concepto amplio sobre la protección de la información a nivel lógico y físico, la implementación de la seguridad perimetral permite la delimitación y la protección sobre la red, esta seguridad puede ser: física, en sistemas y aplicaciones, en la información, como aseguramiento, aplicando Hardening, gestión de acceso, seguridad en redes, conocer sobre la seguridad en general permitirá obtener una mayor visión de protección[14].

4.1.5 Ambiente seguro en los sistemas

Mantener un ambiente seguro es garantía de confianza, permite acceder a los sistemas con mayor tranquilidad, es por eso que las medidas que se tomen para garantizar los ambientes contenga recursos que permitan la prevención, detección y gestión sobre el control de acceso; La gestión de acceso se controla dentro y fuera de la red, con medidas de protección configuradas en los equipos del usuario y en las herramientas de seguridad; Configuración del archivo Hosts en los equipos de los usuarios, restringe el control acceso a contenido, direccionando el nombre de dominio a la IP pública del localhost, con este método se bloquea las páginas a la cual restringimos el acceso, como también asegurando los nombre de dominios a direcciones IP evitando caer en páginas falsas[15].

4.1.6 Herramientas para la protección

Existen diferentes herramientas para la protección y seguridad de la infraestructura y de datos, la utilización de control perimetral de ingreso a las instalaciones, autorización y habilitación de tarjetas de aproximación controlando el ingreso a determinadas zonas; La seguridad interna encargada del control y los permisos de

[12] Senado. Modelo de Madurez de Capacidades de Ciberseguridad para Naciones (CMM). [sitio web]. [31, 03, 2016]. Disponible en: HTTPS://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7840

[13] normaiso27001. NORMA ISO 27001. [sitio web]. Disponible en: HTTPS://normaiso27001.es/

[14] accensit. Seguridad perimetral informática: Información necesaria. [sitio web]. Disponible en: HTTPS://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/

[15] pmg-ssi. Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. [sitio web]. [1, febrero, 2018]. Disponible en: HTTPS://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

acceso a los usuarios a la red, este control es llevado por un directorio activo, el cual define los permisos de grupos y equipos de usuarios para acceder a los recursos de red, como también con la utilización de un servidor NAS, estos sistemas utilizan el protocolo de AAA[16].

4.1.7 Seguridad de empresa

La seguridad de una empresa empieza desde lo físico y locación, para ingresar a las instalaciones debe de ser autenticado y autorizado el ingreso, a esto se le llama gestión y control de acceso, aplicado también para dar permiso a los usuarios en las aplicaciones, redes y sistemas por medio de una autenticación de un login (usuario y contraseña), este usuario es creado mediante una política y se le otorgaran los accesos necesarios dependiendo al rol de su cargo asignándolo a un grupo en el directorio activo[17]

4.1.8 Gestión de acceso

La seguridad en la gestión de acceso e identidades, permite el control a los recursos y que garantice una trazabilidad, garantizando la integridad y/o disponibilidad de herramientas e información; Los software y herramientas no deben ser accedidos por fuera de la intranet, garantizando la política de seguridad de la red y evitar ataque de fuerza bruta, solamente es permitido por escritorio remoto utilizando VPN; Como la seguridad en la gestión de acceso es aplicada de forma horizontal tanto en la parte física como lógica, para las aplicaciones y sistemas permite controlar el horario de disponibilidad y dando un mayor de seguridad lógica perimetral, en aplicaciones es recomendable la utilización del doble factor de autenticación, garantizando con un mayor nivel el acceso indebido[18].

4.1.9 Responsabilidad del usuario

El usuario como uno de los principales recursos con que una empresa cuanta, encargado de velar por la disponibilidad de los servicios, y quien mantiene de pie a una organización, también se le añaden responsabilidades de seguridad que debe cumplir en el puesto de trabajo y cuando lo esté por fuera, esta seguridad va mucho más enfocada a la protección y NO divulgación de los datos, información confidencial y reservada que por su cargo y responsabilidad obtenga en el puesto de trabajo; por otra parte el buen uso de los equipos, no tratar de ingresar ni violentar los sistemas y cumplir con la política de seguridad que la empresa tenga vigente[19].

---

[16] Hacknoid. 5 herramientas de seguridad informática claves en empresas. [sitio web]. [23, abril]. Disponible en: HTTPS://www.hacknoid.com/hacknoid/5-herramientas-de-seguridad-informatica-claves-en-empresas/

[17] ealde . ¿Qué es la seguridad perimetral en el ámbito de los Riesgos Digitales? . [sitio web]. Disponible en: HTTPS://www.ealde.es/seguridad-perimetral-y-su-aplicacion/

[18] Helpsystems. Gestión de Identidades y Accesos [sitio web]. Disponible en: HTTPS://www.helpsystems.com/es/soluciones/seguridad-informatica/gestion-de-identificacion-y-accesos

[19] bib.uia. uso y responsabilidades de la red. [sitio web]. Disponible en: http://www.bib.uia.mx/tesis/pdf/014663/014663_02.pdf

4.1.10 Sistema Proxy

El sistema proxy también es una medida de protección, encargado de las conexiones que realiza el cliente a un destino tomándola a su nombre y ocultando la dirección IP del equipo, consultando primero la información en el historial del cache, sino es encontrada realizará la consulta a la WEB y devolverá la información, entre sus funciones: control del ancho de banda, protección contra ataques de red, registro de red, animando el tráfico, bloqueo de contenido[20].

4.1.11 Ventajas De Utilizar El Proxy

- Permite la navegación de forma anónima, al no utilizar la IP real.
- Permite utilizar servicios con restricción geográfica.
- Tiempos de carga de sitios WEB más rápido, guarda los datos de caché de páginas visitadas.
- Ayuda a bloquear sitios maliciosos.

4.1.12 Desventajas Del Uso Del Proxy

- La interacción con sitios WEB puede retrasar.
- En algunos casos la privacidad puede verse comprometida, al utilizar proxy gratuito.
- Limitación en el uso de puertos.
- Dificultad al acceder a servicios que estén ofrecidos en otro país.

4.1.13 Medidas Para Salvaguardar La Infraestructura

Las medidas de prevención, detección y gestión de acceso fortalecen la seguridad informática, controlan la autenticación y validación de los usuarios, el acceso seguro a la red por medio de la creación y asignación de usuarios tacas, denegando o permitiendo el acceso a sitios WEB con control de contenidos, comprobando la identidad del sitio por medio de certificados SSL; La interacción y aseguramiento de la red externa proporcionada con antivirus y políticas del firewall.

- Medida de prevención: Control de contenido, Infraestructura PKI, Certificado digitales, antivirus, antispam, sistema IPS, Hardening, firewall.
- Medidas de detección: HoneYpot, sistema IDS, stegextract, stegspy
- Gestión de acceso: Redes VPN, proxy, hosts

Asegurar el correo electrónico con protocolo SPF, DKIM, DMARC, previene el dominio de correos antispam y que sea utilizado para este tipo de ataque, verifica

[20] datos101. Que es un proxy y còmo afecta a mi seguridad. [sitio web]. Disponible en: HTTPS://www.datos101.com/blog/que-es-un-proxy-y-como-afecta-a-mi-seguridad/

la autenticidad del remitente del correo, que el contenido del cuerpo del mensaje no haya sido alterado; La utilización del correo electrónico en las empresas está alrededor de un 50% como herramienta principal de comunicación, debido a esto es la importancia de protegerlo, complementar la seguridad con métodos de stegextract, stegspy para garantizar que no se oculte información, y el certificado criptográfico que valida que solo el remitente al que fue enviado pueda abrir el mensaje.

Las medidas de detección utilizadas para la ciberseguridad cumplen un papel esencial para asegurar los datos y toda la infraestructura de las empresas, ayudan a identificar y conocer el comportamiento de los ataques, puede ser de tipo software o físico, supervisando las redes, equipos, detectando comportamiento de intrusión.

4.2 MARCO CONCEPTUAL

Seguridad Informática: Es el método de evitar e identificar el uso no autorizado de la información y los sistemas informáticos, y que a la vez nos permita garantizar la integridad, privacidad de la información contenida en los sistemas informáticos.[21]

Seguridad perimetral: Son las herramientas, hardware, software y métodos de protección informática, con el objetivo de establecer una línea de defensa, asegurando el entorno bajo el que se encuentra la infraestructura y la información de una empresa.[22]

Activo informático: Es la información o dato, dispositivo u otro cualquier componente que tenga valor para la organización y que apoya las actividades relacionadas con la información, generalmente son hardware, software e información crítica.[23]

Sistema De Detección De Intruso (IDS): Es un componente dentro del modelo de seguridad informática de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas, desde el exterior o interior de un dispositivo o una infraestructura de red.[24]

Sistema De Prevención De Intruso (IPS): Dispositivo de seguridad, básicamente para redes, que monitorea las actividades a nivel de la capa 3(red) y/o capa 7

[21] netec. ¿Qué es seguridad informática? [sitio web]. Disponible en: HTTPS://www.netec.com/que-es-seguridad-informatica

[22] Avansis. seguridad perimetral informática. qué es, definición y métodos para proteger tu negocio [sitio web]. Disponible en: HTTPS://www.avansis.es/ciberseguridad/que-es-seguridad-perimetral/

[23] Copro. Activo. [sitio web]. Disponible en: HTTPS://copro.com.ar/Activo_(seguridad_informatica).html

[24] Infotecs. IDS - Sistema de Detección de Intrusos. [sitio web]. [12, marzo, 2019]. Disponible en: HTTPS://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

(aplicaciones) del modelo OSI, identificando acciones indebidas o sospechosas y que de esta manera se consiga obtener defensa en tiempo real.[25]

Protocolo AAA: Corresponden a aquellos protocolos que ofrecen estos servicios (Autenticación, Autorización, Contabilización).

Servidor NAS: Herramienta que permite el almacenamiento conectado a la red. Permite hacer copias de seguridad de archivos dependiendo la configuración.[26]

Sistema UTM: Es un sistema unificado de amenazas, abreviado como (UTM), se refiere a una sola solución de seguridad que ofrece varias funciones de protección en un solo punto de red, ofreciendo servicios de:[27]

- Antivirus.
- Antispyware.
- Antispam.
- Firewall de red.
- Prevención y.
- Detección de intrusos.
- Filtrado de contenido.
- Prevención de fugas.

Política de seguridad: es la declaración de reglas que se deben respetar para acceder a la información y a los recursos, los documentos deben ser dinámicos, mejorarse continuamente según los cambios que se presenten.[28]

4.3 MARCO LEGAL

COBIT: Es un marco de trabajo para la ejecución de buenas prácticas y llevar un control en la tecnología de la información y los riesgos a que se exponen.

[25] Btob. ¿Qué es IPS o Sistema de Prevención de Intrusos (Intrusion Prevention System)?. [sitio web]. [6, enero, 2021]. Disponible en: HTTPS://btob.com.mx/ciberseguridad/que-es-ips-o-sistema-de-prevencion-de-intrusosintrusion-prevention-system/

[26] Xataka. Servidores NAS: qué son, cómo funcionan y qué puedes hacer con uno. [sitio web]. [9, octubre, 2020]. Disponible en: HTTPS://www.xataka.com/basics/servidores-nas-que-como-funcionan-que-puedes-hacer-uno

[27] latam.kaspersky. ¿Qué es la gestión unificada de amenazas (UTM)?. [sitio web]. Disponible en: HTTPS://latam.kaspersky.com/resource-center/definitions/utm

[28] Scielo. politicas de seguridad. [sitio web]. [septiembre, 2008]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

MAGERIT: Metodología De Análisis Y Gestión Del Riesgos De Los Sistemas De Información, explica sobre la valoración del riesgo en los sistemas de información identificando impacto y riesgo y las salvaguardas que se requieren

ISO 27001 Seguridad De La Información: Basada en el ciclo PHVA permite desarrollar un SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, con controles para minimizar todo tipo de riesgo.

ISO 27005: Gestión Del Riesgo De La Seguridad De La Información, abarca diferentes recomendaciones y directrices para la administración del riesgo en de la seguridad de la información.

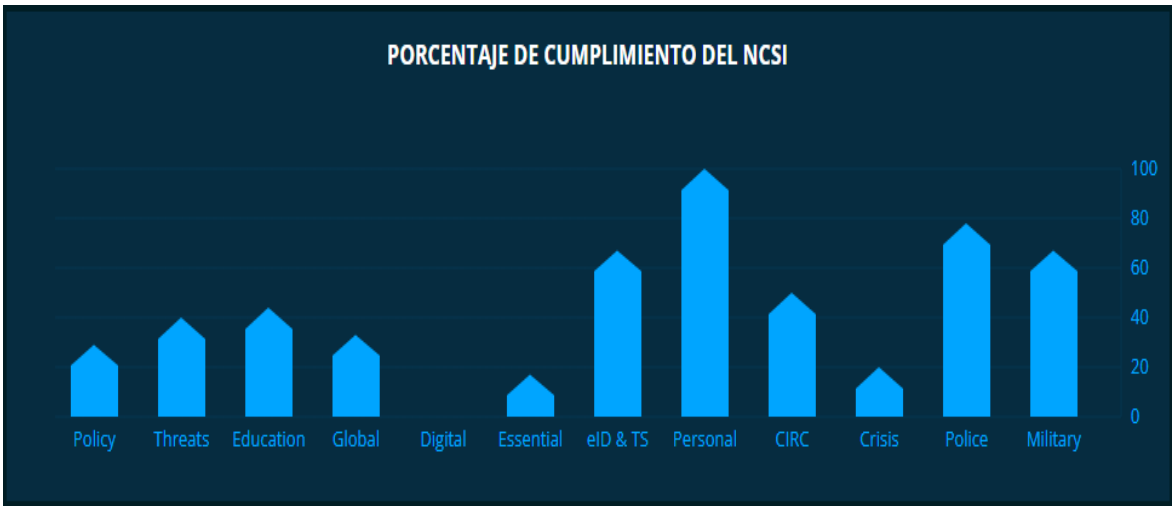
COMPES 3995: Política Nacional De Confianza Y Seguridad Digital, nos habla de fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado, para aumentar el nivel de desarrollo de las empresas en materia de seguridad digital.

COMPES 3854: Política Nacional De Seguridad Digital, plantea reforzar las competencias de ciberseguridad con una visión de gestión de riesgo, como la forma que mitigar el incremento en el tipo y número de amenazas

5 EXAMINAR EL PANORAMA ACTUAL DE SEGURIDAD INFORMÁTICA EN LAS PYMES Y LOS MECANISMOS QUE IMPLEMENTAN PARA RESGUARDAR LOS SISTEMAS DE INFORMACIÓN Y DE RED.

Para el informe publicado en el 13 de febrero de 2019 sobre el Índice Nacional De Ciberseguridad (NCSI, National Cyber Security Index) que es publicado cada 2 años, , este informe mide los siguientes ítems: Modelo; Grado y evolución del compromiso con la ciberseguridad en los diferentes países; Avance en el compromiso asumido en pro de la ciberseguridad de todos los países; Avance en el uso de herramientas que ayuden a mantener una ciberseguridad desde una perspectiva regional; Cuál es el porcentaje de participación de los países en las propuestas de ciberseguridad. Colombia está ubicada en el puesto número 71 y se resaltan cuatro indicadores por encima del 60%, Servicio de identificación electrónica y de confianza, Operaciones cibernéticas militares, cada una con un 67%; Lucha contra el ciberdelito con 78%; y protección de datos personales con un 100%[29]. El porcentaje de cumplimiento del NCSI revela que existen indicadores que se encuentran sin ningún o poco porcentaje de avance, entre ellos: protección de servicios digitales, protección de servicios esenciales y gestión de crisis cibernéticas (CRISIS), tema que debe ser liderado por el Gobierno y las entidades públicas y privadas.

Imagen 1: Porcentaje de cumplimiento del NCSI



Fuente: NCSI. Porcentaje de cumplimiento del NCSI. [sitio web]. Disponible en: HTTPS://ncsi.ega.ee/country/co/

[29] NCSI, Índice nacional de ciberseguridad [sitio web]. Disponible en: HTTPS://ncsi.ega.ee/country/co/

5.1 LOS PROBLEMAS Y RIESGOS ASOCIADOS A LA SEGURIDAD INFORMÁTICA

Para las pequeñas y medianas empresas, su objetivo y principal esfuerzo es aplicado al crecimiento del negocio, en algunas organizaciones la ausencia de Gobierno de TIC, desconocimiento de la protección de la información, la falta de presupuesto invertido a la seguridad informática, y considerar el problema de seguridad informática sólo para las grandes empresas, se exponen a riesgos de sufrir ataques informáticos, como a la pérdida de información. Los riesgos y problemas que las pequeñas empresas sufren en materia de ciberseguridad se encuentran al interior de la organización, no existe una categorización de la información, consideran la seguridad a un problema de virus, limitar la seguridad a las herramientas que poseen, gestión insuficiente de usuario[30].

Las empresas utilizan tres medidas básicas de protección para la seguridad informática, la utilización de un firewall, antivirus y como medida de protección ante pérdida de información respaldo por backup a los principales equipos[31]; estas medidas de seguridad son eficaces cuando la configuración es adecuada y las herramientas se encuentran actualizadas, de nada vale un firewall si se están permitiendo las conexiones a los servicios sin una VPN, cuando solo respaldan la información almacenada, quedando por fuera prácticas como toma de snapshot, estructura de los archivos, de bases de datos, y no contar con una política de backup, otro riesgo es que las pymes por medio de servicios y herramientas tecnológicas se conectan con proveedores y otras organizaciones más grandes, los ciberataques aprovechan las debilidades de seguridad de la Pymes para acceder a las grandes empresas[32].

El Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), por medio de un modelo de evaluación que mide el nivel de madurez de las capacidades de ciberseguridad de un país, describiendo el avance por el cumplimiento de etapas, ver imagen 1: Modelo de madurez de la capacidad de ciberseguridad, así mismo mide el nivel de madurez evaluando cinco dimensiones, compuestos por un conjunto de factores que explican cómo adquirir capacidad de seguridad cibernética y cómo mejorarlo, entre los factores se encuentran protección de la infraestructura, gestión de crisis, confianza y seguridad en internet, medios y

[30] *Destinonegocio. Principales vulnerabilidades cibernéticas que las Pymes deberían gestionar. [sitio web]. Disponible es: HTTPS://destinonegocio.com/mx/gestion-mx/recursos-materiales-mx-mx/vulnerabilidades-que-las-pymes-deberian-gestionar/*

31 Welivesecurity. ESET-security-report-LATAM2020.pdf. [sitio web]. [2020]. Disponible en: HTTPS://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

32 Elpais. La débil apuesta de las pymes por la seguridad informática. [sitio web]. [12, junio, 2017]. Disponible en: HTTPS://elpais.com/retina/2017/06/01/tendencias/1496307759_889133.html

redes sociales, sensibilización, marcos legales, calidad de software, controles criptográficos[33].

Imagen 2: Dimensiones del CMM

Fuente: digitalpolicylaw. América Latina se ubica en un nivel promedio básico de madurez para el desarrollo de ciberseguridad. [31, julio, 2020] Disponible: HTTPS://digitalpolicylaw.com/america-latina-se-ubica-en-un-nivel-promedio-basico-de-madurez-para-el-desarrollo-de-ciberseguridad/

Se realiza el análisis de la información del estado actual de las Pymes y al comparar con el Modelo de Madurez de la capacidad Cibernética, las pymes en su mayor porcentaje se encuentran en la etapa de Consolidada, la cual se describe como: Los indicadores están instalados y funcionando, sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y definida.[34].

Etapas de madurez de la capacidad de ciberseguridad:

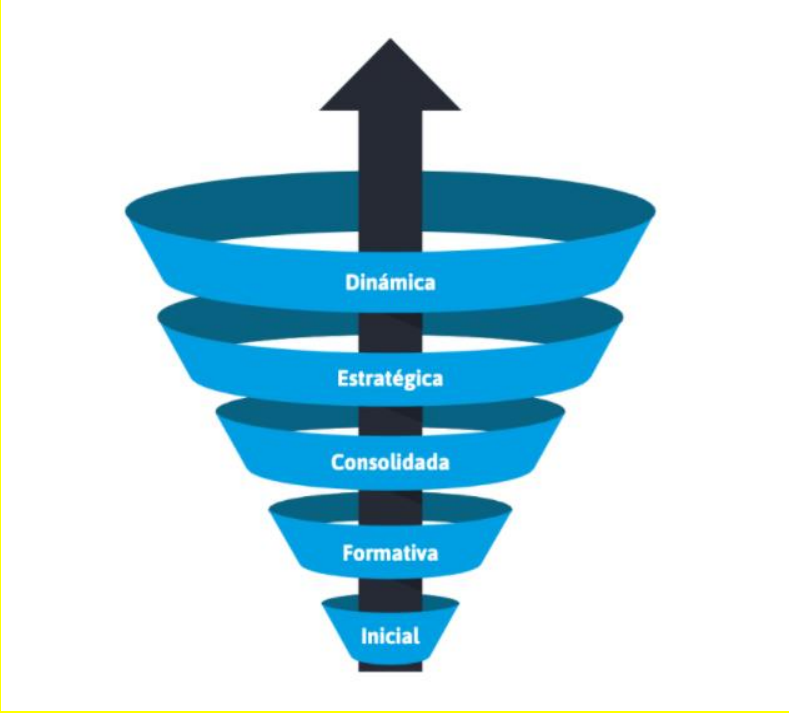
- Inicial: Proceso iniciales para el desarrollo de capacidad de ciberseguridad, pero sin ninguna medida observable.

[33] publications. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. [sitio web]. [julio, 2020]. Disponible en: HTTPS://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[34] publications. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe [sitio web]. [julio 2020]. Disponible en: HTTPS://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

- Formativa: Se evidencia procesos de formulación pero que deben ser corregidos.
- Consolidada: Indicadores instalados y en funcionamiento, pero falta la asignación de recursos, y socializar los beneficios.
- Estratégica: Identificación de los indicadores más relevantes.
- Dinámica: Existe tecnología dedicada a la contención de amenazas, como asignación de recursos

Imagen 3: Modelo de madurez de la capacidad de ciberseguridad



Fuente: digitalpolicylaw. América Latina se ubica en un nivel promedio básico de madurez para el desarrollo de ciberseguridad. [31, julio, 2020] Disponible: HTTPS://digitalpolicylaw.com/america-latina-se-ubica-en-un-nivel-promedio-basico-de-madurez-para-el-desarrollo-de-ciberseguridad/

Otro tema fundamental sobre el panorama de la seguridad en las Pymes es el manejo de la seguridad de la información y las medidas que toman para la protección de la seguridad informática; un estudio realizado por Red.es indica que alrededor de un 50% de las pymes trabajan sin seguridad, indicando que la información contenida no es relevante, pueden ser víctimas de delincuentes informáticos, desconociendo que no es una persona quien intenta el ataque, sino una máquina; A pesar de esto son cada vez más las empresas que implementan y se dan cuenta de la importancia de invertir en la seguridad de los sistemas y la información.

Con más del 80% las pymes conforman el sector productivo de Colombia, todas estas empresas del sector público y privado tienen la documentación y proyecto presentado a la alta dirección de un sistema de gestión de la seguridad de la información, en el cual está plasmado la importancia de los activos, amenazas y riesgos asociados, el problema que presentan es que no toman las medidas tecnologías (hardware y software) para contrarrestar y mitigar las vulnerabilidades, los principales problemas para no adquirir recursos de TIC, es que no se le presta la importancia necesaria y es visto como un gasto y no como la inversión, otro problema es la falta de presupuesto, al comprar un recurso de seguridad, también hay que agregar la contratación del ingeniero para la configuración y administración o en su defecto la contracción de un tercero para las medidas de seguridad

Para medida de protección y respaldo de información utilizan método de copias de seguridad en los discos y unidades extraíbles realizando copias semanales, ignorando los riesgos a que se exponen con la utilización de estos métodos.

5.2 PRINCIPALES ATAQUES INFORMÁTICOS, QUE ESTÁN EXPUESTAS LAS EMPRESAS, EN ESPECIAL LAS PYMES.

Los ataques informáticos, se tiene registro que vienen sucediendo desde el año 1836 mucho antes que existieran los computadores, se produjo en un sistema de comunicaciones del telégrafo óptico; El primer gusano informático dispersado en internet fue para el año 1988, conocido como el gusano morris[35].

Todas las empresas sufren amenazas y están expuestas por los diferentes tipos de ataques informáticos, entre los más comunes se encuentran el malware y sus distribuciones, virus, gusanos, troyanos, expiatorios: spyware, de publicidad: adware, de encriptación: ransomware, extorsión: doxing, engaño: phishing, DDOS, entre otros.

¿Porque las pymes tienen una mayor probabilidad de afectación?, las grandes empresas y multinacionales si cuentan con los sistemas de protección para cada terminal y servicio publicado, tiene un plan de contingencia y continuidad de negocio, cuentas con herramientas como Sitescope quien realiza una supervisión centralizada de la disponibilidad de la infraestructura, contando con personal dedicado a la administración de este sistema.

[35] Welivesecurity. Martes de retrospectiva: el gusano Morris. [sitio web]. [8, noviembre, 2016] Disponible en: HTTPS://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/

Por otro lado, las pymes, que con su corto personal y presupuesto no pueden garantizar cubrir las necesidades en materia de tecnología y es un blanco mucho más fácil para los atacantes por las debilidades que estas tienen.

todos los ataques afectan la seguridad de una empresa sea Pyme o una gran empresa, lo que varía es el método y la sofisticado del ataque que cada día son más avanzados, alterando la integridad de la información, disponibilidad de los servicios, la confidencialidad de los datos, secuestro de información, la reputación hasta el cierre; Según Alberto Fernández (experto en Cloud y Seguridad para empresa de Telefónica España), un 70% de las empresas que sufren una pérdida de datos cierran en menos de 1 año[36], en relación a estos efectos es la importancia de mantener los sistemas lo más seguros posible, y que las Pymes no se conviertan en una brecha de seguridad para las empresas aliadas.

Principales ataques:

- Troyanos: Se camufla como un software legítimo, utilizado para introducir malware, espiar, robo de datos, tomar control del equipo.
- Virus: Es necesario que el usuario ejecute una acción para que se active, es un tipo de malware y se propaga rápidamente por el sistema.
- Spyware: Su función es obtener información del usuario.
- Phishing: Utiliza la ingeniería social para que la víctima revele información confidencial, propagado por medio de correo electrónico.
- Adware: Utilizado para mostrar publicidad de manera invasiva, como también la para la instalación de otros malware.
- Ransomware: Encriptar la información recolectada.
- DDOS: Realizar peticiones a un servicio hasta lograr que este colapse y se bloquee.
- Inyección SQL: Aprovechan vulnerabilidades en las aplicaciones WEB para insertar un código y obtener información de las bases de datos.

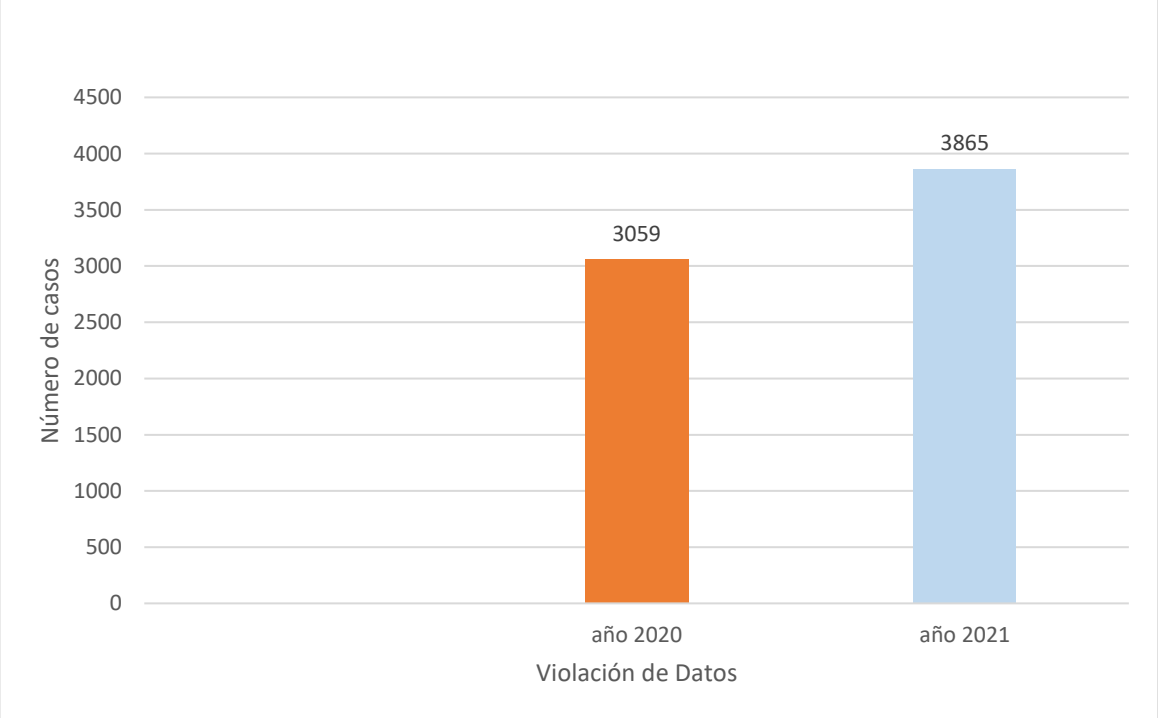
[36] Nephosit. El 70% de las empresas que sufre una pérdida de datos cierra en menos de un año. [sitio web]. [17, febrero, 2020]. Disponible en: HTTPS://www.nephosit.com/el-70-de-las-empresas-que-sufre-una-perdida-de-datos-cierra-en-menos-de-un-ano/

5.3 AUMENTO DE ATAQUES CIBERNÉTICOS EN COLOMBIA.

Una columna publicada por el portal WEB el Portafolio hace referencia al incremento del 30% de los delitos informáticos en comparación con el año anterior 2020, que, entre las principales ciudades como Bogotá con 8.355 caso denunciados, Medellín con 1.664 casos y Cali con 1.569 registro de denuncia, y a nivel nacional superan las 23.000 registraron de denuncias en materia de cibercrimen[37].

La publicación también da a conocer los tres delitos u ataques más utilizadas por los ciberdelincuentes:

Imagen 4: Violación de datos

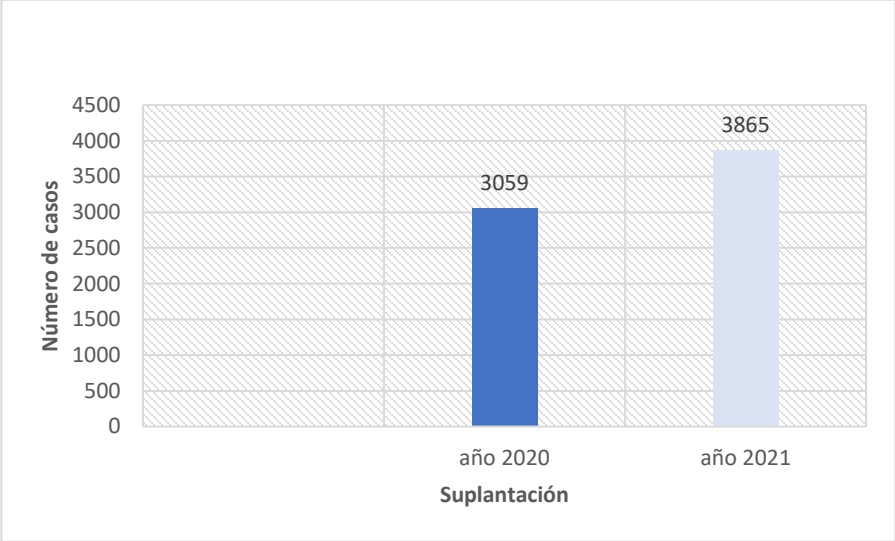


Fuente: autor

Violación de datos, con un aumento del 108% de casos, utilizando la técnica de del engaño “phishing”

[37] Portafolio. Aumentan en 30% los ataques cibernéticos en Colombia. [sitio web]. [8, junio, 2021]. Disponible en: HTTPS://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803

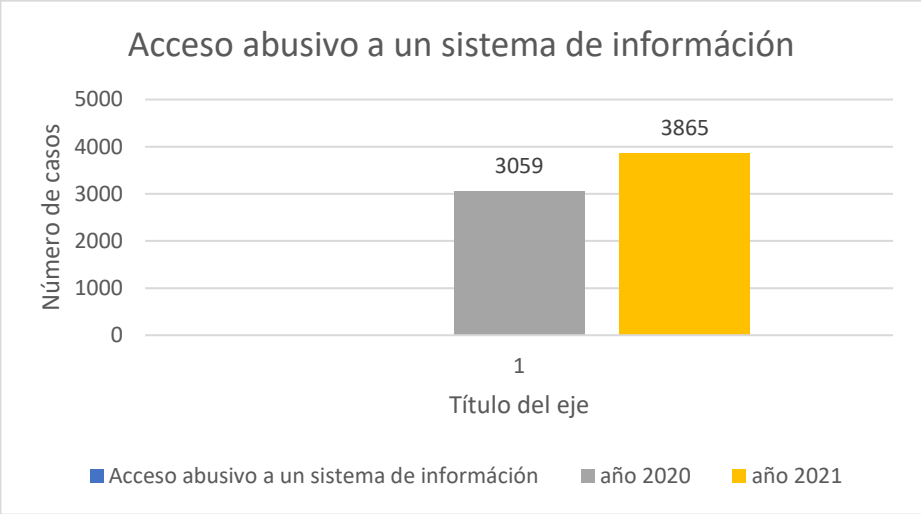
Imagen 5: Suplantación



Fuente: autor

Suplantación: Incremento de 368 en comparación con el año anterior aumentó un 29%, objetivo obtener la captura de datos personales, utilizando métodos como phishing, smishing y pharming

Imagen 6: Acceso abusivo



Fuente: autor

Acceso abusivo a un sistema informático: Con una diferencia de 806 casos comparándolo con el año anterior.

Se puede concluir que las tres técnicas están relacionadas y se asemejan en su forma de obtener la información, que cada día los ataques han ido en aumento. Se espera que el gobierno, sector público y privado aborden el tema de la ciberseguridad de forma proactiva y no solo con la implementación de políticas, sino con el acompañamiento de herramientas que permitan la verificación de usuarios legítimos una red y protegerla del exterior, utilizando doble factor de autenticación, configuración del WAF, políticas para correos seguros.

5.4 SEGURIDAD EN APLICACIONES WEB

Al hablar del panorama sobre la ciberseguridad, hay que incluir el tema tecnologías de las aplicaciones WEB, estas han tenido un crecimiento por los servicios que prestan y facilidad de acceder a ellas, contar con la información a la mano y acortando la distancia en las comunicaciones, pero ¿qué tan seguras son estas aplicaciones?, el portal latinpymes realizó una publicación en donde informa que más del 60% de las brechas de seguridad están relacionada a las aplicaciones WEB, las organizaciones que desarrollan estas herramientas utilizan metodologías de desarrollo ágil de software dejando a un lado al seguridad.[38]

Tabla 1: Estándares de seguridad en aplicaciones WEB

PCI	Security Standards Council
NIST SP 800-115	Metodología de pruebas de intrusión
OSSTMM	Open Source Security Testing Methodology Manual, proporciona pruebas de seguridad.
OWASP	WEB Security Testing Guide, guía para realizar pentesting en aplicaciones WEB
NIST	Marco de ciberseguridad

Fuente: latinpymes. MÁS DEL 60% DE LAS BRECHAS DE SEGURIDAD INVOLUCRAN APLICACIONES. [sitio web]. [19, junio, 2019].Disponible en: HTTPS://www.latinpymes.com/mas-del-60-de-las-brechas-de-seguridad-involucran-aplicaciones-web/

[38] latinpymes. más del 60% de las brechas de seguridad involucran aplicaciones web. [sitio web]. [19, junio, 2019]. Disponible en HTTPS://www.latinpymes.com/mas-del-60-de-las-brechas-de-seguridad-involucran-aplicaciones-web/

5.4 INFORME: EVALUACIÓN, RETOS Y AMENAZAS EN LA CIBERSEGURIDAD: CCIT

En el desarrollo del informe publicado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) en junio de 2021, intervinieron empresas reconocidas en el sector tecnológico y de seguridad informática, brindando estadísticas, crecimiento de los ciberataques, herramientas de protección entre otros, se extrae los temas considerados más relevantes.

La empresa Claro Colombia, amplió los alcances en sus servicios de ciberseguridad que ofrece, ratificando un aumento en el catálogo de servicios como: Aseguramiento de plataformas, aplicando líneas bases (Hardening), gestión de la seguridad y riesgos, aplicación de Red TEAM y Blue TEAM, de procedimientos en prevención de fuga de datos (DLP), monitorear el comportamiento inusual de los usuarios que están conectados a la red de la organización (UEBA), Respuesta en la detección proactiva de Incidentes de ciberseguridad con un sistema SIEM, evitando su propagación. Cabe aclarar que el 50% de las empresas que realizaron la contratación de los servicios actuaron de forma proactiva, bajo la premisa de estar preparados[39].

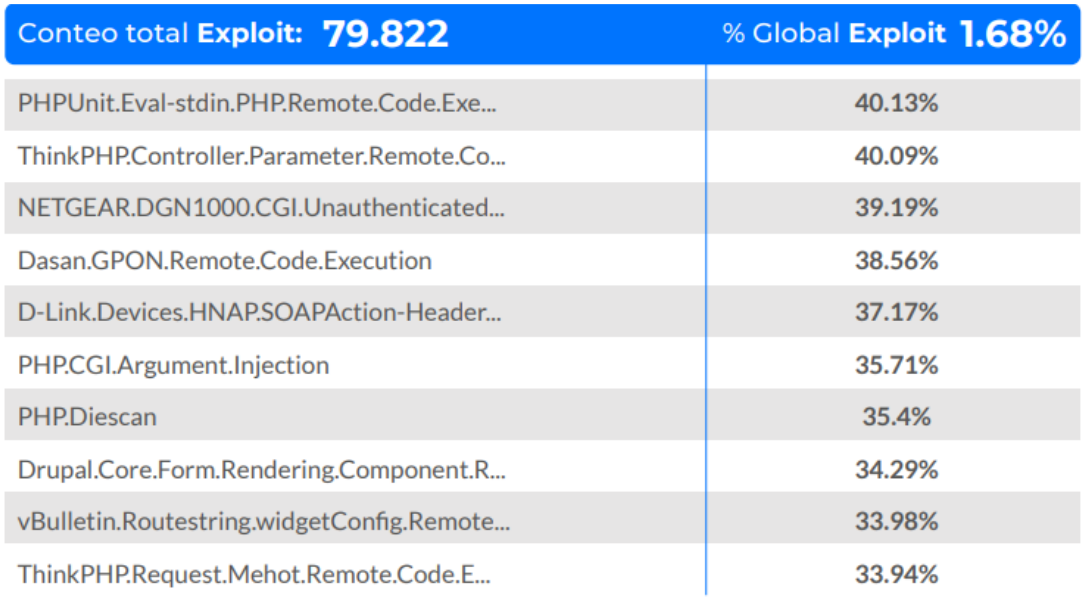
También indica las cifras de crecimiento en la cantidad de incidentes de seguridad con un aumento del 88%, que la suplantación de identidad aumentó un 42% para el año 2020 y que la fuga de información para comienzos del 2021 a tenido un incremento importante; Tiene un reporte superior a 3 millones de alertas mensuales.

Un dato muy importante que la empresa Fortinet revela sobre la estadística obtenida por su herramienta FortiGuard threat insider, que los 10 exploits por vulnerabilidades comunes reportados, 5 se encuentran relacionada con el lenguaje PHP, y este es uno de los más utilizados en Colombia, y que a nivel nacional el reporte de caso de exploit está el rededor de los 80.000[40]

[39] CCIT. Evaluación, retos y amenazas a la ciber-seguridad. [sitio web]. [junio, 2021]. Disponible en: HTTPS://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/

[40] CCIT. Evaluación, retos y amenazas a la ciber-seguridad. [sitio web]. [junio, 2021]. Disponible en: HTTPS://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/

Imagen 7: Top de exploit



Conteo total **Exploit:** 79.822	% Global **Exploit** 1.68%
PHPUnit.Eval-stdin.PHP.Remote.Code.Exe...	40.13%
ThinkPHP.Controller.Parameter.Remote.Co...	40.09%
NETGEAR.DGN1000.CGI.Unauthenticated...	39.19%
Dasan.GPON.Remote.Code.Execution	38.56%
D-Link.Devices.HNAP.SOAPAction-Header...	37.17%
PHP.CGI.Argument.Injection	35.71%
PHP.Diescan	35.4%
Drupal.Core.Form.Rendering.Component.R...	34.29%
vBulletin.Routestring.widgetConfig.Remote...	33.98%
ThinkPHP.Request.Mehot.Remote.Code.E...	33.94%

fuente: ccit. Informe: Evaluación, retos y amenazas a la ciberseguridad. [sitio web]. por CCIT – tacTac. [junio, 2021]. Disponible en: HTTPS://www.ccit.org.co/estudios/informe-evaluacion-retos-y-amenazas-a-la-ciberseguridad/

Como también indica la importancia de crear bases de conocimiento del TTP (Tactics, Technics and Procedures) tácticas, técnicas y procedimientos que utiliza el atacante para cumplir sus objetivos, por medio de la cacería de amenazas y estar un paso más delante de los atacantes, permitiendo mejorar la infraestructura.

6 ESTABLECER POLÍTICAS, MEDIDAS, PROCEDIMIENTOS Y SERVICIOS DE SEGURIDAD NECESARIOS PARA IMPLEMENTACIÓN DE UNA ESTRATEGIA BASADA EN LA SEGURIDAD LÓGICA PERIMETRAL PARA LA PREVENCIÓN, DETECCIÓN Y RECUPERACIÓN DE LA INFORMACIÓN

Establecer una política de seguridad perimetral de la información, que permita asegurar y garantizar el control de la compañía, realizar una gestión de los activos, que contemple: Identificación, clasificación, etiquetado, ciclo de vida de los activos informáticos; Control de acceso: para usuario y contraseña, gestión de contraseña, perímetros de seguridad y control de acceso a zonas; El control de los activos de información, permite conocer la información crítica y elaborar plan de restauración; Plan de capacitación a usuarios sobre la seguridad de la información.

Tener un sistema de gestión integral, que permita el almacenamiento de Procedimientos, formatos y guías plenamente aprobados por un comité, los procedimientos pueden ser para entrega y retiro de equipos, formato para el ingreso de personal, para la creación, modificación y eliminación de usuarios, baja de equipos, entre otros.

Como servicios para la implementación de la seguridad de la información y seguridad perimetral y que garantice la disponibilidad, integridad y confidencialidad de la información, se debe iniciar con las tres medidas más utilizadas por las organizaciones, la utilización de firewall que permitirá un control perimetral desde y hacia fuera de la empresa, como segunda media la utilización de un antivirus que permitirá la protección contra virus informático, como última medida la utilización de backup, respaldando información, datos, bases de datos, Filesystem y sistema operativo.

Un software para el monitoreo de los servicios como páginas web, bases de datos, perfomance del server, llenado de disco, que emitan una alarma sobre eventos de caída, pérdida de conexión, lentitud o cualquier otro tipo de incidente sobre la disponibilidad de servicios, reduciendo los tiempos de respuesta al identificar la causa, para este tipo de monitoreo se pueden utilizar las herramientas de Nagios, PRTG Network Monitor, Pandora FMS.

Identificar los recursos que puedan ser consumidos tanto interno como externos, y separarlos por direccionamiento, aplicar donde sea posible la utilización del doble factor de autenticación para ingresos a recursos.

Crear una política sobre la zona de correo, con registros tipo DKIM, DMAR, SPF, que aparte de proteger el dominio de ataques, permita evitar que el dominio sea utilizado para el envío de correo spam.

6.1 ELEMENTOS REQUERIDOS PARA PROTECCIÓN FÍSICA Y LÓGICA PERIMETRAL.

Las medidas de prevención para resguardar la información se garantizan con control a las instalaciones y zonas restringidas a ciertos empleados, se debe garantizar que el personal cuente con tarjeta de proximidad y permisos a zonas específicas de su labor, si necesita acceder a zonas restringidas debe de ser con autorización y acompañamiento dependiendo a donde requiera acceder; Otras medidas de protección es la vigilancia con circuito cerrado de televisión, puertas de seguridad con mecanismos de ingreso biométricos; los mecanismo de escaneo de rayos “x”, muy utilizado para el ingreso a los bunkers, con el fin de detectar elementos no permitido … entre otras.

Para asegurar la infraestructura y la información de una organización, las herramientas informáticas proporcionan estas medidas, complementando con seguridad lógica, este conjunto de mecanismos permite resguardar ante posibles ataques, como también identificarlos y realizar filtrado de tráfico, se nombran unos elementos básicos y fundamentales que requieren tener dependiendo a las necesidades de cada compañía.

Firewall o Cortafuegos: son sistemas por el cual es transmitido el tráfico cumpliendo la función de aceptar o denegar las peticiones sobre las políticas y reglas configuradas, existen a:

- Nivel de red: Encargado del control del tráfico por medio de direcciones IP (origen y destino), y se encuentran las siguientes herramientas, el FortiGate 30E, con la ventaja que permite la creación de dominios virtuales (VDOM), de fácil utilización, administración por la nube, vigilancia de aplicaciones, defensa contra amenazas, sistema IPS, filtrado web, conexión VPN.

- Nivel de aplicaciones: conocidos como WAF, controla el tráfico de contenido mediante protocolos en las capas superiores como telnet, DNS, DHCP, TCP, UDT.

- Cisco Meraki MXW: Monitorea y prioriza el tráfico, no afecta el ancho de banda, filtra el contenido, protección contra malware, seguridad WIFI, gestión en la nube.

- SonicWall T400: Basado en la nube, monitoreo de red sin reducción de velocidad, sirve como antivirus.

- WatGuard Firefox T15: permite la detección de intrusos, ransomware, antivirus, prevención en pérdidas de datos, conexión VPN.

- Firewalla: Difícil de instalar y configurar; permite seguridad cibernética, protección de red, control parental, antivirus, malware, bloqueo de anuncios, servidor VPN.

- Palo alto: Brinda las siguientes características principales, detector de aplicaciones, análisis de malware en: aplicaciones puerto y protocolo, contiene protección de antivirus, antispyware, IPS, filtrado web, denegación de servicios; Compuesto por dos secciones de hardware, protección en aplicaciones SaaS[41]

- PFSense: Firewall de red con kernel personalizado, disponible en hardware, virtual, y binario; alguna de sus principales funciones: cortafuego, balanceo de carga, traducciones de red, red privada virtual, monitoreo en tiempo real, DNS dinámicos.

- IPFire: Permite la personalización, utilizado como cortafuego, servidor proxy, conexión VPN; posee características IDS (sistema de detección de intrusos).

- OPNSense: Las funciones que se pueden utilizar, como firewall, VPN, 2FA (doble factor de autenticación), IDPS (sistema de prevención y detección de intrusos), Proxy, Webfiler entre otras, su sistema Gui viene disponible en varios idiomas.

6.1.1 Ventaja de la utilización del firewall

- Controla el acceso a la red privada.

- Administra los segmentos de la red, permitiendo acceso a máquinas autorizadas.

- Define niveles de acceso a la información necesaria por grupos de usuarios.
- Identifica los componentes que forman la red para que la comunicación sea más directa optimizando el acceso.

- Ayuda a la seguridad, monitoreando el tráfico entrante y saliente.

[41] Cerounosoftware. ¿Qué es Palo Alto Networks?. [sitio web]. Disponible en: HTTPS://cerounosoftware.com.mx/2018/05/07/qu%C3%A9-es-palo-alto-networks/.

6.2 MEDIDAS UTILIZADAS EN SEGURIDAD LÓGICA PERIMETRAL PARA LA PREVENCIÓN, DETECCIÓN Y RECUPERACIÓN DE LA INFORMACIÓN.

Sistemas De Detección Y Prevención De Intrusos (IDS/IPS): Elemento de seguridad informática, que puede ser software o hardware, encargado de vigilar las redes y los equipos, permite detectar si un intruso ha ingresado a la infraestructura y contrarrestar automáticamente cualquier ataque, supervisan el tráfico, red, puertos, paquetes de datos, buscando patrones sospechosos.

6.2.1 Sistemas IDS/IPS:

Cisco NGIPS: Las reglas de políticas y las firmas de amenazas son actualizadas en periodo de dos horas puede funcionar en ambientes físicos o instancia VMware.

Corelight y Zeek: Análisis general y detallado del tráfico de la red, funciona en dispositivos físicos como virtuales y de interfaz gráfica fácil de usar.

Zentayl: Interfaz gráfica sencilla de configurar, viene con reglas preconfiguradas

Fidelis Network: Permite el análisis de tráfico por medio de puertos, utiliza diferentes protocolos para detectar anomalías, genera metadatos de la información recolectada, trabaja en la red y en la nube, escaneo de la topografía de la red.

Antivirus y antispam: inspeccionan la red, filtran y bloquean el contenido malicioso, impiden la infección por malware, aunque muchos vienen con paquetes adicionales, dependiendo la necesidad de la compañía; entre los principales antivirus están: Bitdefender, Norton, Avira, Kaspersky.

6.2.3 Honeypots y honeynets

Los honeypots son herramientas que permiten la simulación de servicios y aplicaciones vulnerable en ambientes controlados con el fin de atraer atacantes y con la información recolectada mejorar la seguridad de la organización, este escenario debe de estar separado de la interfaz de producción; Los honeynets son redes en las cuales se implementan los honeypot que permite la alta interacción, en la cual se utilizan equipos, sistema operativo y aplicaciones reales.

6.2.3.1 Sistemas honeypots:

Honeypots de tipo SSH

- Kippo: Construido para identificar y registrar ataques de fuerza bruta.

- Cowrite: Brinda un sistema de registro/archivo falso.

6.2.3.2 Honeypots de tipo HTTP

- Glastopf: Descubre ataques de aplicaciones web, inyección SQL.
- Nodepot: de aplicaciones web, puede ejecutarse con recursos limitados de hardware.
- Google hack honeypot: emulador de aplicaciones WEB, oculto a peticiones directas.

6.2.3.3 Honeypots de tipo base de datos

- ElasticHoney: Permite detectar solicitudes maliciosas que intentan explotar las vulnerabilidades RCE (ejecución remota de código)[42]
- Honey MySQL: la función es proteger ISS.

6.2.3.4 Honeypot de correo electrónico

- Honeymail: Identifica y previene ataques a los servidores SMTP.
- Spamhat: Evita que los correos spam infecten los buzones del correo electrónico.

6.2.3.5 Honeypot de internet de las cosas (IOT)

- Kako: Ejecutan simulaciones de servidores de tipo telnet, Http/s.
- HoneyThing: Actúan como un módem que tiene un servidor web.

6.2.4 Sistemas Anti-DDOS

Para conocer los sistemas que impiden ataques de DDos, hay que conocer qué es el ataque de denegación de servicios o DDos, es la solicitud de muchas peticiones a un servicio para que este trabaje más lento hasta llevarlo a la caída del servicio.

Los servidores pueden mitigar estos ataques aplicando filtros que restringen paquetes mal formados, modificados, con IP falsas, permitiendo que solo lleguen peticiones legítimas; Hay soluciones basadas en la nube para la detección y protección DDOS:

[42] Atico34. Honeypots o sistemas trampa. Definición y funciones. [sitio web]. [23, septiembre, 2020]. Disponible en: HTTPS://protecciondatos-lopd.com/empresas/honeypots-sistemas-trampa/

Kona DDOS Defender: garantiza el funcionamiento del sitio web aun cuando ha sido atacado, desviando las peticiones SYN o UDP y absorbe las peticiones HTTP Get y Post de la red evitando que lleguen a las aplicaciones centrales.

Sucuri: Utiliza el aprendizaje automático para mitigar ataques, también proporciona la eliminación de malware, monitoreo de listas negras, limpieza de pirateo, firewall.

AppTrana: Permite la protección de la infraestructura a nivel de red, transporte y aplicaciones, como también contra DDOS con la actualización de reglas.

Incapsula: Previene ataque de DDOS, en la capa 3 (red), capa 4 (transporte) y capa 7 (aplicación), como también ataque de fuerza bruta, ping de la muerte, nxdomain, entre otros.

Alibaba: puede prevenir ataques de alto volumen y admite protocolos TCP, UDP, Http/s, también brinda una solución para ayudar a identificar el origen del ataque.

CheckPoint: Realiza la identificación por el nombre de usuario y no por la dirección IP, permite la creación, gestión y control de políticas a grupos de usuarios, bloqueo de amenazas.

6.2.5 Medida De Monitoreo De La Infraestructura

SIEM: permite el análisis de amenazas internas, externas como en la nueve, permite la supervisión centralizada, la automatización de tareas, disminución en la detención de ataques, alertas sobre cualquier evento sospechoso.

Nagios: Supervisión de las redes y sistemas, reportes detallados, informe de alarmas, historial de eventos.

Zabbix: interfaz web, configuración fácil, reportes minuciosos de los sistemas, bajos costos de operación.

6.3 PROPUESTA DE POLÍTICAS PARA LA IMPLEMENTACIÓN DE UNA ESTRATEGIA BASADA EN LA SEGURIDAD LÓGICA PARA LA PROTECCIÓN DE LA INFORMACIÓN.

La política de seguridad de la información es el conjunto de medidas preventivas, reactivas y sistemas tecnológicos que permiten resguardar y proteger la información

buscando mantener la confidencialidad, la disponibilidad, integridad y autenticidad.[43]

Las acciones que ponen riesgo los sistemas y la información que se deben evitar:

Trabajar en computadores sin protección de antivirus, como también acceder a sistemas de la compañía en equipos desconocidos.

No tener un plan de copias de seguridad, o que las copias queden mal hechas, asumir el riesgo de perder información importante como bases de datos, proveedores, proyectos.

Para correos sospechosos, evitar abrir este tipo de correos, como la descarga de archivos, de dar clic a enlaces, pueden contener malware.

Evitar dejar la sesión de las aplicaciones y de nuestro equipo abierta, para evitar el robo y pérdida de información, como también dejar visibles las contraseñas (debajo del teclado, en el escritorio)

Mensajes sospechosos de las redes sociales, al abrir estos mensajes existe la posibilidad de ser víctimas de estafas, ingeniería social, infección.

Evitar la utilización de dispositivos USB en los computadores de la compañía, las memorias USB pueden venir con virus que se auto ejecutan para el robo de información; son de gran facilidad, pero es unos de las principales formas de contagios.

Las medidas que ayudan a garantizar el control de la seguridad de información son las políticas como medidas de protección,

La política de contraseña tendrá una longitud de 12 caracteres alfanumérico, debe contener mayúscula, minúscula y un carácter, tiempo de expiración de 90 días, no se tendrá habilitado recordar contraseña, pero si se llevará un historial de contraseñas, se restringe en uso de números y letras consecutivas.

Para inicio de sesión a los equipos tendrán habilitado la secuencia de teclas (control + alt +suprimir), para evitar que las aplicaciones se ejecuten la inicio, se bloquearán después de tres intentos fallidos, la sesión se terminará una vez se llegue a los 15

[43] pagosimple. Seguridad de la información. [sitio web]. Obtenido de: HTTPS://www.pagosimple.com/seguridad-de-la-informacion/#:~:text=La%20Seguridad%20de%20la%20Informaci%C3%B3n%20es%20el%20conjunto%20de%20medidas,e%20integridad%20de%20la%20misma.

minutos de inactividad; para sistemas de alto riesgo se utilizará la autenticación de doble factor.

Opciones para tener en cuenta:

- Los puntos de acceso deben estar protegidos con contraseñas.

- Implementar el sistema de copias de seguridad de la información, completa, diferencial e incremental; garantizando que la información esté respaldada, realizar pruebas totales como granulares para verificar el correcto funcionamiento de las restauraciones.

- Mantener los sistemas operativos actualizados con los últimos parches de seguridad, protegiendo la información de amenazas informáticas.

- Cifrado de la información y las comunicaciones, evitando que la información sea legible para usuarios no autorizados; Realizar el cifrado de datos financieros, contactos; aparte de asegurar la información también las comunicaciones son importantes que se cifren de manera simétrica o asimétrica.

- Cifrado simétrico: utiliza la misma clave para el cifrado y descifrado, ejemplo: tipo AES (Advanced Encryption Standard), con longitud de clave hasta 256 bits; Cifrado asimétrico: utiliza dos claves (pública y privada) para el cifrado y descifrado, ejemplo: tipo RSA y DSA.

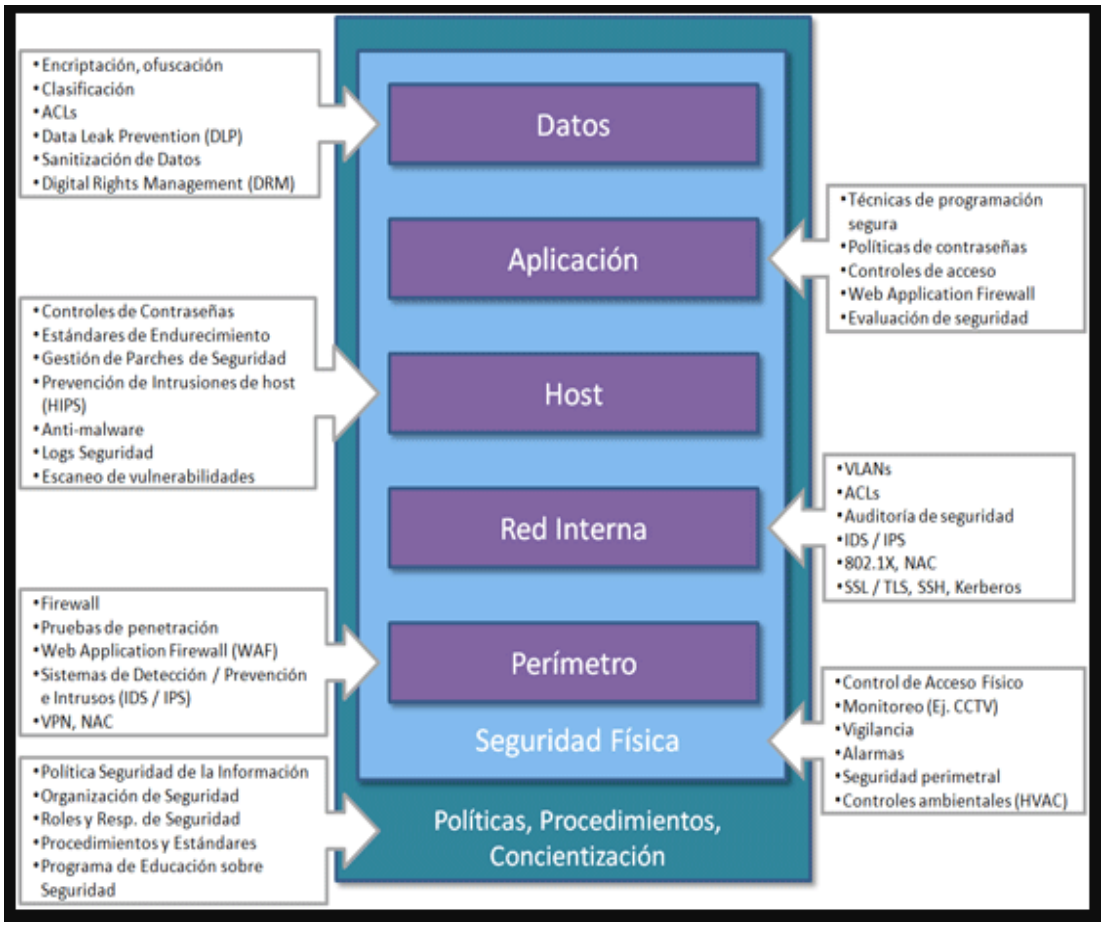
6.4 MODELO DEFENSA EN PROFUNDIDAD COMO UN MECANISMO DE PROTECCIÓN EN LA SEGURIDAD DE LA INFORMACIÓN.

La defensa en profundidad (o Defense in Depth por su siglas en inglés), también conocida como defensa elástica y permite la protección de la información sensible de accesos no autorizados y contempla 7 capas de seguridad (Políticas, seguridad física, perímetro, red interna, host, aplicaciones y datos), para la CIS (Center of Internet Security), mediante este enfoque se intenta desarrollar mecanismos y controles tecnológicos diferentes de forma selectiva para asegurar los principios de la información (confidencialidad, integridad y disponibilidad), si como de la red y los datos que se almacenan. Si bien las medidas de controles individuales de seguridad tecnológicas no poseen la capacidad para contener las diferentes amenazas cibernéticas, juntas brindan una mayor protección de mitigación y reducción de

riesgo informático, al tiempo que incorporan diversidad y redundancia en caso de que algún mecanismo o control particular fallará[44].

Como es de saber que entre más protección se implementa para asegurar los datos, será mucho más difícil que personal no autorizado puede acceder a ellos, este modelo de seguridad nos permite garantizar que todas las capas de la infraestructura tengan una protección que requiera una autenticación y autorización para poder acceder a los datos, este modelo proviene del mundo militar como una estrategia que permite relentizar y que pierda fuerza un ataque, como poder identificarlo en zonas menos críticas y tomar las medidas necesarias para controlarlo

Imagen 8: Defensa en profundidad



fuente: seguinfo. Defensa en Profundidad. [sitio web]. [5, noviembre, 2021]. Disponible en: HTTPS://seguinfo.wordpress.com/2010/11/05/defensa-en-profundidad/

[44] Cisecurity. Foco de seguridad electoral - Defensa en profundidad (DiD). [sitio web]. Disponible en: HTTPS://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/

Se describen cada una de las capas del modelo de defensa en profundidad.

- Políticas: La política de seguridad de la información debe de ser conocida por cada uno del personal interno y externo de la compañía.

- Seguridad física: Controlar el acceso físico a la infraestructura.

- Defensa perimetral: Controlar el acceso de conexiones remotas y a la red con políticas de seguridad.

- Red interna: Es la protección, control y monitoreo de la red interna.

- Host: La seguridad en server, como en equipos clientes se gestiona con: mantener actualizado el equipo con parches de seguridad, protección de un antivirus, restricción de instalación.

- Aplicación: La seguridad se aplica mediante la autenticación y autorización para el acceso a las aplicaciones.

- Datos: Los datos como principal activo de una organización deben de ser protegidos con técnicas de encriptación, políticas de backup.

6.5 DEFENSA EN PROFUNDIDAD POR FUNCIÓN

La defensa en profundidad garantiza una estructura sólida de seguridad moderna, con una estrategia de combinación de herramientas que permitirán la detección y bloqueo de amenazas, debilitando la fuerza del ataque cada vez que se enfrente con una capa de seguridad, se considera redundante debido a que las capas de seguridad están preparadas para prevenir el ataque. Hay que garantizar que los controles de seguridad y ciberseguridad funcionen correctamente, la siguiente tabla describe la defensa en profundidad por función.

Tabla 2: Defensa en profundidad por función

Prevención	Autentificación
	Autorización
	Encriptación
	Cortafuegos
	Etiquetado/Manejo/Retención de datos

	Gerencia de Ciberseguridad
	Seguridad Física
	Prevención de intrusos
	Escaneo de malware
	Seguridad del personal
	Concientización y capacitación
	Pruebas de ciberseguridad
	Escaneo automático persistente
Contención	Autorización
	Privacidad de los datos
	Cortafuegos
	Dominios de seguridad
	Segmentación de redes
	Seguridad física
Detección	Monitoreo
	Notificación
	Mediciones/métricas
	Auditoría/registros en bitácoras
	Honeypots
	Detección de intrusos
	Detección de virus
Reacción	Respuesta a incidentes
	Cambio en políticas y procedimientos
	Mecanismos de seguridad adicionales
	Nuevos / mejores controles

	Respuesta a incidentes
Medidas de recopilación evidencia/monitoreo de incidentes	Auditoría/registro en bitácoras
	Gerencia/monitoreo
	No repudio
	Informática forense
	Recuperación / restablecimiento
	Conexión de apoyo (failover) sitios remotos
	Planes de continuidad del negocio
	Recuperación de desastres

Fuente: blogdelciso. CiberDefensa en profundidad por función. [sitio web]. [23, agosto. 2018]. Disponible en .HTTPS://blogdelciso.com/2018/08/23/ciberdefensa-en-profundidad-por-funcion/+&cd=4&hl=es&ct=clnk&gl=co

6.5.1 Arquitectura de defensa en profundidad

Los modelos de protección de ciberseguridad deben de ir cambiando, nos protegen de las amenazas y de la red externa, pero cuando el atacante logra ingresar el sistema lo puede considerar como confiable, la arquitectura de ciberseguridad permite aislar los componentes críticos de cualquier amenaza o daño, estos controles se dividen en:

- controles físicos: Encargado de proteger los sistemas de TI de daños físicos.
- controles técnicos: Métodos de protección de la red, a nivel de hardware, software y red.
- Controles administrativos: Conformada por la seguridad de la información

Otro tema importante del que se debe hablar es sobre los especificados en la IEC 62443, la norma está dirigida al sector industrial se refiere a unos temas muy puntuales a considerar en la defensa en profundidad.

- Control de acceso: Protección de los activos e información ante accesos no autorizados.
- Control de uso: Evitar manipulación y operación no autorizadas.

- Integridad de la información.

- Confidencialidad.

- Restringir el flujo de datos: Protección de los canales de comunicación y garantizar que la información solo llegue a los destinos autorizados.

- Respuesta ante incidentes: Mantener un control sobre monitorización, reportes, eventos, alertas, acciones correctas y de mejora.

- Disponibilidad de recursos: garantizar la disponibilidad de los sistemas.

complementando en lo posible garantizar el cifrado de datos, y controlar el riesgo que sean borrados, extraídos, copiados, alterados, el cifrado se debe de garantizar en tránsito como en reposo.

Cifrado en tránsito (EIT): Protección de la información que se está transmitiendo por cualquier canal o aplicación.

Cifrado en reposo (EAR): Asegurar los datos almacenados, utilizando métodos como el PIN, contraseña.

6.6 ENDURECIMIENTO DE LOS SISTEMAS, UNA MEDIDA PARA ASEGURAR LA INFRAESTRUCTURA E INFORMACIÓN.

Los sistemas vienen con configuraciones predeterminadas desde fabrica para que sea de fácil uso, su implementación y manejo, y no están dirigidas a la seguridad, algunos servicios vienen abiertos exponiendo los sistemas a vulnerabilidades, para realizar configuración de seguridad en los sistemas se requiere analizar la función que va a cumplir en la red.

El hardening que traducido al español significa endurecimiento, es una técnica de seguridad que se aplica a la infraestructura y sistemas, para evitar posibles ataques corrigiendo vulnerabilidades, y logrando un equilibrio en un entorno sin riesgo de seguridad, este método es basado que en: un sistema que presta un único servicio es más seguro que uno que desempeña varias funciones, alguna de las recomendaciones es:

- Cambiar claves por defecto.

- Desinstalar software innecesario o no autorizado.

- Tener contraseñas robustas /aplicadas a una política.
- Eliminar usuarios predeterminados.
- Deshabilitar servicios sin uso.
- Protección de antivirus.
- Cerrar puertos.
- Usar encriptación de datos.
- Configuración de permisos de acceso.
- Ejecución de backup.
- Actualización con parches de seguridad.

6.7 TÉCNICAS DE HARDENING

Se listan algunas herramientas utilizadas para la seguridad y endurecimiento de los sistemas.

- Los Sistema de Detección de Intrusos conocidos por siglas IDS, nos previene de acceso no autorizados al computador o la red.
- Sistemas de detección de intrusos en host HIDS, revisa anomalías potenciales de riesgos, actividades y ejecutar medidas protectoras.
- NIDS, herramienta centralizada que permite la detección de usuarios intrusos dentro de una Red, verificación de comportamientos anómalos, permite analizar el tráfico de entrada y salida.
- Snort, detector de intruso basado en red, las acciones de respuestas deben de ser preconfiguradas.
- Antivirus, Cumple la función de detectar y eliminar los virus informáticos.
- Firewall, cortafuego de hardware o software para controlar el tráfico y acceso de servicios por medio de políticas.
- DMZ, su función es proteger la intranet, los equipos que se encuentren en la DMZ no tengan conexión con la red interna.

- GPG, permite el cifrado en las comunicaciones y la firma digital.

La metodología de aplicación de hardening en los sistemas se realiza aplicando listas de chequeo (checklist)

Restrinja el acceso de inicio de sesión local a los administradores, puede comprometer el dispositivo, pudiendo iniciar sesión desde la consola.

Configure el número de inicios de sesión anteriores en la memoria caché, se recomienda disminuir el número de sesiones almacenadas como los tiempos de almacenamiento, por si un atacante logra acceder a la carpeta se exponen menos credenciales y disminuir ataques de fuerza bruta.

Deshabilitar carpetas compartidas, evita que gusanos se puedan propagar.

Deshabilite ejecuciones automáticas de dispositivos USB, evitará que malware se reproduzcan en el equipo.

Habilitar ver archivos ocultos, los códigos maliciosos se esconden con este atributo.

Habilitar extensiones de archivos, permite identificar la extensión verdadera de los archivos

7 DISEÑAR UN PLAN ESTRATÉGICO QUE SIRVA COMO GUÍA EMPLEANDO LA SEGURIDAD LÓGICA PERIMETRAL PARA LA PROTECCIÓN DE REDES INFORMÁTICAS Y DE COMUNICACIÓN EN LAS PYMES.

Las redes informáticas y de telecomunicaciones, son sistemas informáticos que se conmutan por elementos guiados y no guiados entre sí, mediante una serie de dispositivos inalámbricos o alámbricos, gracias a los cuales pueden compartir información[45], para que estos datos se encuentren seguros las organizaciones deben de garantizar la protección del tráfico (Entrante, saliente y el tráfico dentro de la red), cumplir con regulaciones para la protección de las redes, garantizar que las herramientas se encuentren actualizadas para la protección de los nuevos desafíos de la seguridad en las redes o se requiere nuevas herramientas de tipo hardware o software.

Los sistemas no son cien por ciento seguros, debido que no se puede eliminar todos los riesgos a los que están expuestos los sistemas y la información, pero es posible tener un plan efectivo para la seguridad lógica perimetral de las redes informáticas, y debe empezar con la creación de una política de seguridad informática que abarque recursos y la información.

Para el desarrollo de este objetivo se investiga la referencia de las guías publicadas por el ministerio de las TIC (MINTIC) en el Modelos De Seguridad enfocado a las buenas prácticas de seguridad, citando apartes del modelo de seguridad publicado por MINTIC, la implementación del Modelo De Seguridad Y Privacidad De La Información – MSPI, estará determinado por requisitos de seguridad, procesos, el tamaño de la organización, todo esto para preservar la confidencialidad, integridad, disponibilidad de los activos de la información, garantizando su buen uso y la privacidad de los datos[46].

Una forma de robustecer la seguridad de las redes informáticas y de las comunicaciones como los datos que viajan sobre ellas, no solo implica asegurar el hardware, software, las plataformas, herramientas de seguridad y monitoreo, sino que también es necesario incluir al recurso humano en las actividades de aseguramiento de la información por medio de: capacitaciones, vallas informativas, información del Sistema Integrado de Gestión (SIG), en materias de seguridad de la información, que así como los sistemas son corregidos con parches de seguridad, el factor humano es actualizado en estas capacitaciones sobre los nuevos y diferentes modelos de ataques y como poder protegerse.

[45] Concepto.de. redes informáticas. [sitio web]. Disponible en: HTTPS://concepto.de/redes-informaticas/

[46] Mintic. Modelos de seguridad. [sitio web]. Disponible en: HTTPS://mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Citando la norma, el control A7.2.2 concientización, educación y formación en seguridad de la información: Todos los empleados de la organización y, cuando sea pertinente, contratista, deberían recibir concientización, entrenamiento y formación adecuada y capacitaciones periódicas en política y procedimientos organizacionales, relevantes para su formación laboral[47].

7.1 PLAN ESTRATÉGICO DESARROLLADO MEDIANTE EL CICLO PHVA, PARA LA PROTECCIÓN DE INFORMACIÓN.

7.1.1 Planear

Elaborar un plan estratégico que contenga el inventario de activos de información (equipos personales, servidores, directorio activo, herramientas y software de protección lógica perimetral, bases de datos, aplicaciones, router, switch, entre otros), así mismo crear políticas de seguridad sobre los servicios, procedimiento para: La gestión de procesos, de activos, de riesgo y gestión de usuarios, asegurar los datos almacenados y en tránsito con procesos de encriptación, como también política de backup (Diferencial, Incremental y full), canales de comunicación seguros por medio de enrutamiento estático, configuración de usuarios para la conexión de acceso remoto y validación de los privilegios a usuarios de la red.

Documentar y publicar qué información, aplicaciones, servicios, hardware y software son necesarios para la continuidad del negocio de la organización y para que siga prestando los servicios, como también de que personal dependen estos servicios o sistemas, en caso de presentarse eventos, incidentes de seguridad o desastres; Para saber cómo enfrentar los incidentes de seguridad y contenerlos en un menor tiempo es necesario elaborar una matriz de escalamiento y de comunicación.

El plan estratégico está orientado sobre los controles de la ISO 27002, control A8.1.1 inventario de activos, A8.2.1 clasificación de la información, A8.2.2 etiquetado de la información; Control A9 Control de acceso; Control A12 Seguridad de las operaciones; Control A13 Seguridad de las comunicaciones; Control A16 Gestión de incidentes de la seguridad de la seguridad de la información.

7.1.2 Hacer

En esta etapa se desarrollarán todas las actividades para verificar el estado en que se encuentra la organización a nivel de seguridad, se fijarán las estrategias y planes de acción para alcanzar los objetivos y el nivel de seguridad deseado de la

[47] Normaiso27001. A7 seguridad relativa a los recursos. [sitio web]. Disponible en: HTTPS://normaiso27001.es/a7-seguridad-relativa-a-los-recursos/

información y estos deben ir alineados con los objetivos organizacionales, definir roles y responsabilidades para la gestión y administración de la seguridad de la información, realizar la matriz de escalamiento y contar con el personal adecuado para realizar las funciones de monitoreo, detección, contención y mitigación de incidentes de seguridad y entre ellos un documentador para ir creando la base de conocimiento.

Para este punto se realiza la configuración de las herramientas para la seguridad lógica perimetral (Firewall, VPN, DDOS, Rapib7, IDS/IPS, WAF,) para la protección de la red, estas herramientas deben de pasar por el proceso de implementación y hardening antes de entrar a producción, implementar la seguridad para la protección de correo electrónico con protocolos de autenticación (DKIM, SPF, DMARC). Organizar los activos de información realizando un inventario, llevar el control, poder clasificarlo y garantizar el nivel de protección que requiere según la criticidad de cada activo y la valoración de los riesgos, así mismo identificar el responsable del activo como el uso adecuado.

Tabla 3: Inventario de activo

<table>
<tr><td colspan="2">Tipo de Activo</td><td colspan="2">Código de Servicio / Placa de Inventario</td><td colspan="2">Ubicación Física/Virtual</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3" rowspan="2">Valor del Activo</td><td rowspan="2">Riesgo</td><td rowspan="2">Nivel del Riesgo</td></tr>
<tr><td>Confidencialidad</td><td>Disponibilidad</td><td>Integridad</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Descripción del Activo</td><td>Responsable del Activo</td><td>Control de Parchado</td><td colspan="2">Licencia / Certificado</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2">Red /Comunicación</td><td></td><td colspan="2"></td></tr>
<tr><td>IP</td><td>VLAN</td><td colspan="4">Notas</td></tr>
<tr><td>Si es servidor indicar IP (producción, gestión y administración)</td><td></td><td colspan="4"></td></tr>
</table>

Organizar las actividades en procedimientos, y que estos se encuentren publicados y conocidas por todo el personal, deben de mantenerse actualizados y aprobados por un comité de cambio y calidad, los procedimientos pueden ser para solución de problemas como también para estandarizar el flujo de un proceso.

Tabla 4: Lista de procedimientos

Nombre del procedimiento	Versión actual
Gestión de usuarios (creación, modificación y eliminación)	
Gestión de activos (Asignación, rotación, devolución y baja)	
Control de parchado y certificados	
Hardening	
Control de cambio	
Gestión de incidentes	

7.1.2.1 Control de acceso

Esta política dirigida al control, privilegios, autorización y permisos que un usuario tiene para acceder a los recursos de red, debe de iniciar por un flujo de creación y registro de usuario, asignación de privilegios hasta la cancelación y retiro del usuario de la red.

Todo usuario que acceda a la red debe tener los privilegios mínimos para realizar las actividades, y pertenecer a un rol para el acceso a las aplicaciones. La seguridad para el control de acceso y permiso que un usuario pueda tener se garantizan con la aplicación de políticas sobre herramientas de seguridad, entre ellas se encuentra el Directorio activo, LDAP, Radius, consola EPO, Detección y respuesta en Punto Final (EDR), como también es importante asegurar el punto final para la protección de la integridad de la información utilizando Prevención de Pérdida de Datos (DLP), antivirus, Monitoreo de Integridad de Archivos (FIM).

7.1.2.2 Implementar la seguridad en las operaciones

Para este paso garantizar que los procesos y procedimientos se encuentren actualizados, esto garantiza resolver en un menor tiempo los incidentes y eventos de seguridad; Identificación de la información crítica, es la que permite el funcionamiento, y cumplir la misión de la organización; Gestión de riesgo, permite identificar la criticidad y reducir el impacto en la integridad y disponibilidad de la información; Vulnerabilidades y riesgos cibernéticos, mantenerse actualizado de las nuevas vulnerabilidades y riesgos que afectan la seguridad, en páginas del proveedor de la infraestructura y software; Copias de seguridad, es el respaldo ante posibles eventos, asegurando la disponibilidad e integridad de la información mediante políticas (incrementales, diferenciales y total) de copias de seguridad, recordar que se deben realizar pruebas de restauración periódicas para verificar la disponibilidad.

7.1.2.3 Monitoreo y análisis de la infraestructura

Garantizar que la infraestructura se encuentre operando en óptimas condiciones, así mismo como los servicios de red y aplicaciones, que garantice la disponibilidad de la información, para ello se debe de contar con herramientas de monitoreo (Nagios, Zabbix, CloudWatch, Libre NMS), mantener la separación de los ambientes (desarrollo, prueba y operación), para evitar fallos y problemas de seguridad, mantener separado los ambiente de (Producción, Gestión y Administración), preservar la defensa contra código malicioso, utilizando antivirus, limitaciones en los permisos de cuentas, deshabilitar la reproducción automática, verificación de integridad de los archivos.

7.1.3 Verificar

Terminada las fases de Planeación y Hacer, se debe comprobar si los controles de seguridad lógicos perimetrales fueron eficaces, realizando un plan de mantenimiento de seguridad informática, para medir su valoración y efectuar el análisis, la verificación debe de abarcar los sistemas, procesos, procedimientos y personas.

Revisar de forma periódica los permisos y privilegios de los usuarios, realizar un nuevo análisis de riesgos para evaluar el nivel de riesgos residuales, comprobar las políticas de seguridad en los sistemas y equipos, y que estos se encuentren actualizados en parches de seguridad, verificar la integridad de los sistemas con pruebas de penetración internas y externas, mantener una lista de chequeo para las

políticas de seguridad sobre las líneas bases de seguridad, que el proceso de gestión ante respuesta de incidentes se encuentre actualizado.

Evaluar los riesgos de la seguridad de la información con los controles de seguridad críticos (CIS), método gratuito para mejorar la postura frente a la seguridad con prácticas de ciberseguridad, priorizando la implementación, puede encontrar la guía en https://www.cisecurity.org/controls/v8/.

Contar con un ciclo de capacitaciones de ciberseguridad, y las formaciones que se realicen al personal deben ser evaluadas y comprobar que los conceptos, terminología y métodos fueron comprendidos.

7.1.4 Actuar

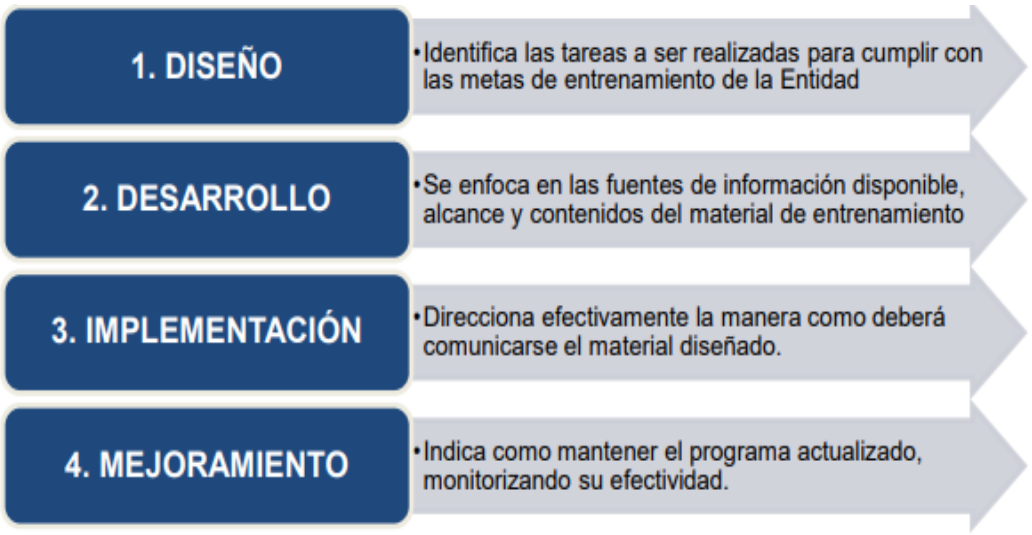
Refleja los ajustes que se deben de realizar sobre los objetivos del proceso para alcanzar los resultados que se obtuvieron de forma parcial, o que no se obtuvieron según la planeación inicial, se identifican las brechas y limitaciones de presupuesto, capacidad, sensibilización y capacitación, recurso, personal, roles y responsabilidades para alcanzar el estado deseado, ajustar los métodos de monitoreo y seguimiento, mejorar el análisis para replantear los planes de acción, para así adoptar nuevas estrategias e indicadores de seguridad de la información.

Realizar nuevamente el inventario de activos, evaluación de los riesgos y amenazas como estrategia de alcanzar el estado deseado, la organización podría llegar a los resultados no satisfactorios, por lo cual es conveniente replantear los objetivos y hoja de ruta y alinearlos sobre la defensa en profundidad, que permite una mayor protección, se centra en controles y políticas administrativas, físicas y lógicas para la protección y la ciberseguridad.

7.2 GUÍA 14 – PLAN DE COMUNICACIÓN, SENSIBILIZACIÓN Y CAPACITACIÓN.

La guía brinda una orientación para abordar el desarrollo del Plan de comunicación y sensibilización cumpliendo cuatro fases: diseño, desarrollo, implementación y mejoramiento, cumpliendo el ciclo de: Sensibilización, Entrenamiento, Educación y Desarrollo profesional, y una vez realizado el proceso se obtenga, personal capacitado en seguridad de la información y se reduzcan los riesgos informáticos.

Imagen 9: Plan de sensibilización



fuente: Fase plan de sensibilización, capacitación y comunicación del Mintic, disponible en: HTTPS://mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

El primer paso es seleccionar el modelo para la creación de las políticas y estrategias, la implementación puede ser centralizado o parcialmente descentralizado, dependiendo del tipo de organización y las estrategias que necesite buscar dependiendo a sus objetivos.

Seguir con la identificación de necesidades o debilidades, que permitirá la justificación de implantar el plan de comunicación y sensibilización, los métodos para identificar las necesidades:

- Entrevistas de grupos.
- Encuestas.
- Procedimientos de ingeniería social.
- Verificación de comportamiento.
- Análisis de los incidentes de seguridad ocurridos.
- Análisis de log de las herramientas de seguridad.
- Tendencia de ataques sobre el sector que se desarrolla la entidad.

Identificadas las necesidades, crear un documento que contenga la estructura del plan que se va a aplicar:

- Dar a conocer la política de seguridad de la información de la empresa.
- Fijar el alcance del programa.
- Determinar los roles y responsabilidades.
- Cuál es el propósito de aplicar el programa o meta a cumplir.
- Curso de preparación que debe de ser presentado por el personal.

- Temática a desarrollo
- Periodo de las capacitaciones.
- Documentos de evidencias

Debe de haber un plan de monitoreo para el desarrollo de las capacitaciones que permita medir y crear reportes para la alta gerencia, que se esté cumpliendo con el cronograma de actividades, que el personal esté asistiendo las capacitaciones entre otras. El desempeño del programa también se debe evaluar, saber si está creando un valor agregado y cumpliendo el alcance, la meta y determinar si es necesario modificaciones, una vez terminado se puede aplicar nuevamente la identificación de necesidades o debilidades.

7.3 MODELO DE CIS CONTROL

Conjunto de mejores prácticas en seguridad cibernética y que permite acciones defensivas para previenen o mitigar ataques comunes a los sistemas y redes, desarrollado por el Center for Internet Security y grupos expertos en seguridad y tecnología que recopilan la documentación de ataques reales y las medidas que utilizaron para corregirlo; Le aportará a la organización fundamentos para el plan de seguridad de la información, medidas más efectivas, mejorar la gestión del riesgo y ajustarse a otros marcos regulatorios.

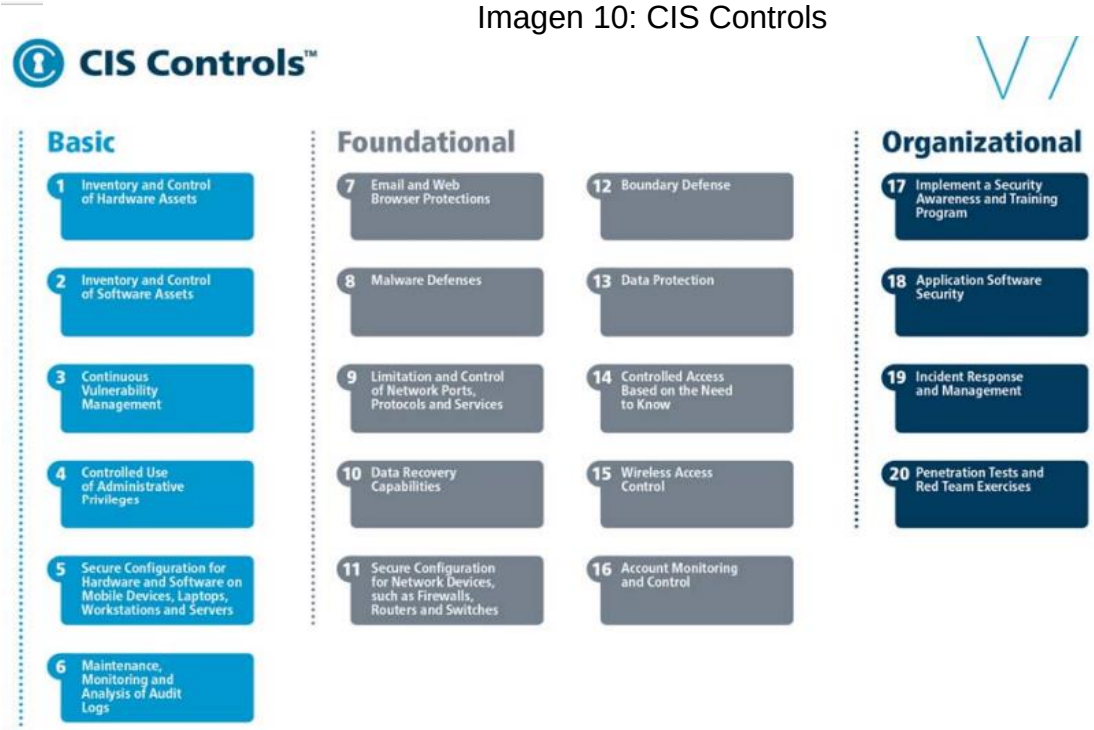
La versión 7 del CIS controls está compuesta en tres grupos:

- Básico: Hace referencia a los controles de uso general, que toda organización necesita implementar para garantizar la disponibilidad y mantener una defensa informática esencial.

- Fundamentales: Controles de seguridad para contrarrestar amenazas técnicas específicas.

- Organizacionales: Enfocado al personal como también a los procesos de seguridad informática, mantener la calidad de la seguridad.

Imagen 10: CIS Controls



Fuente: cisecurity. Hacer del mundo conectado un lugar seguro. [sitio web]. Disponible en: HTTPS://www.cisecurity.org/

7.3.1 Control 1: Inventario y control de activos hardware

Se debe de mantener actualizado el inventario de hardware que se conecta a la red, y que solo garantizar los dispositivos identificados tenga acceso y se identifiquen y bloqueen aquellos que traten de acceder, algunas de las acciones que se deben garantizar son:

- Emplear herramienta de descubrimiento de activos.
- Utilizar DHCP logginp.
- Control de acceso a nivel de puerto.
- Gestión de activos no autorizados.
- Inventario detallado de los activos.
- Utilizar la autenticación de activos por medio de certificados.
- Herramientas pare este control: Desktop Center y Oputils

7.3.2 Control 2: Inventario de software autorizados y no autorizados.

Garantizar la gestión (inventario, seguimiento y corrección) de software que están instalados en los equipos que se conectan a la red y que solo los autorizados se

puedan ejecutar, esto para evitar que los atacantes encuentren versiones de software vulnerables, controles que se deben aplicar.

- Inventario de software instalados (autorizados).
- Soporte del fabricante
- Herramienta para inventariar software
- Utilizar listas blancas de app, script, librerías
- Identificar las aplicaciones que tienen alto riesgo.
- Herramientas que pueden utilizar: Firewall, antispyware, Desktop center

7.3.3 Control 4: Uso controlado de privilegios administrativos

Hacer seguimiento y mantener gestionados a los usuarios con cuentas que tengan privilegios altos en las aplicaciones, BD y sistemas, garantizar que los usuarios utilicen las cuentas con privilegios para casos específicos y se deslogee, evitara la manipulación a sistemas críticos, y que un atacante tenga acceso por elevación de privilegios.

Controles

- Inventario de las cuentas.
- Cambiar contraseñas por defecto y por periodo de 2 meses.
- Utilizar multi factor de autenticación.
- Alertar sobre cambios de privilegios de un usuario.
- Registrar y alertar sobre intentos fallidos de acceso.
- Herramientas que se pueden utilizar: Desktop center, password manager pro, aDaudit plus, política de contraseña

7.2.4 Control 7: Protección de correo electrónico y navegadores web.

Se debe de garantizar la seguridad en los correos y navegadores web con una adecuada gestión, esto minimiza el compás de ataque, y evita que los usuarios sean engañados (spoofing, phishing o ingeniería social), controles a utilizar.

- Garantizar el soporte en la contratación de dominios de correo
- Deshabilitar plugins.
- Categorización y Filtrado de URL.
- Utilizar servidores DNS.
- Implemente políticas de autenticación en el correo.
- Aplicar técnicas sandbox.

- Herramientas para este control: Mantener los navegadores actualizados con los parches de seguridad, utilice en su correo (DMARC, SPF, DKIM) disminuye tipos de correos spam y el phishing, Firewall analyzer

7.2.5 Control 10: Capacidad de recuperación de datos.

Se debe garantizar el respaldo y la recuperación de la información crítica, con metodología y herramientas fiables apoyado con un procedimiento, y políticas de copia de seguridad, con el fin de evitar pérdida de información, garantizar la integridad de los datos.
Controles recomendados:

- Realizar respaldos de datos, archivos y sistemas completos.
- Verificar los medios donde se está respaldando.
- Que las copias de seguridad tengan un destino discontinuo.
- Validar de forma aleatoria copias de seguridad en ambientes de prueba.
- Herramientas para el control: Recovery mangerplus, network configuration manager

7.2.6 Control 11: Configuración segura de los equipos de red, como los cortafuegos, enrutadores y conmutadores.

La configuración segura de la infraestructura y dispositivos de red, garantizar el control de cambios de versiones, deshabilitar la configuración predeterminada aplicando líneas base de seguridad, evita que un atacante pueda acceder a dispositivos vulnerables.

Controles de seguridad:

- Mantener la seguridad estandarizada en los equipos de la red.
- Realizar el control de versiones e instalación de parches de seguridad.
- Utilizar la autenticación multi factor.
- Administrar la infraestructura.
- Herramienta: Network configuration manager, lista de control de acceso (ACL)

7.2.7 Control 12: Defensa de borde.

Se requiere el control de la información en el perímetro de la red, aplicar multi capaz de seguridad en las redes perimetrales, previene que atacantes accedan a los sistemas evadiendo los controles perimetrales.

Controles requeridos:

- Inventario de bordes de red.

- Denegar la conexión de IP maliciosa y de puertos no autorizados.
- Implementar sistema de monitoreo de paquetes.
- Utilización de multifactorial en inicio de sesión.
- Desplegar proxy en la capa de aplicación.
- Utilizar sistema de IDS basados en red.
- Herramientas que se pueden utilizar: protección multi capa, firewall, proxies, DMZ, IDS/IPS, oputils, netFlow analyzer, eventlog analyzer.

7.2.8 Control 13: Protección de datos.

Realizar etiquetado y clasificación de la información, identificar datos sensibles y aplicar controles más fuertes para acceder a ellos, aplicar encriptación y prevención de pérdida de datos, identificar donde se almacena y quien tiene acceso, esto permite una mayor protección a la prevención de pérdida de datos.

Controles

- Inventario de información sensible.
- Monitorear tráfico de red
- Permitir el servicio de nube o correo autorizados
- Cifrar los discos duros y los datos almacenados.
- Gestión de dispositivos USB.
- Herramientas: Data security plus, device control plus, movile device manager plus, garantizar el acceso a la información solo al personal requerido.

7.2.9 Control 17: Implementar un programa de concienciación y entrenamiento de seguridad.

Elaborar y desarrollar un plan integral de capacitación para todos en la organización, identificar conocimientos, habilidades, actualizar periódicamente o actualizar el contenido.

Controles

- Realizar un análisis de las debilidades que tiene.
- Implementar el programa de concienciación en seguridad
- Capacitación en el manejo de datos sensibles.
- Capacitación de cómo identificar y reportar incidentes.
- Capacitación de autenticación segura
- Capacitación sobre ingeniería social

7.2.10 Control 18: Seguridad del software de aplicación

Gestionar el ciclo de vida del software para prevenir, detectar y corregir vulnerabilidades, ejecutar pruebas de testing, estar actualizado con el top ten de OWASP, verificar errores de programación y errores lógicos.

Controles que se pueden utilizar

- Verificar que el software tenga soporte
- Que tenga prácticas seguras de programación.
- Realizar análisis de código
- Separar los entornos de producción
- Implementar WAF
- Usar plantillas de hardening para BD

7.3 CYBERSECURITY FRAMEWORK VERSIÓN 1.1

El marco de ciberseguridad del NITS es una guía basada en: (estándares, pautas, prácticas) que contribuyen a las organizaciones a la gestión y reducción del riesgo de ciberseguridad, está compuesto por cinco funciones: identificar, proteger, detectar, responder, recuperar que componen el ciclo de vida de la administración de la ciberseguridad.

Imagen 11 - Framework

fuente: csrc.nist. marco de ciberseguridad. [sitio web]. [12, octubre, 2021]. Disponible en: HTTPS://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

Se realizará una descripción de cada uno de los elementos que componen el ciclo de vida.

7.3.1 Identificar.

Comprender el desarrollo organizacional para gestión del riesgo de ciberseguridad en los sistemas, activos, información y capacidades, se componen de cinco ítems

- Identifique los procesos y activos críticos de la empresa, identificar los procesos misionales y procesos o actividades que la organización siga funcionando.

- Documentar los flujos de información, Una vez identificada y clasificada la información se debe de tener claro la ubicación donde se almacena, cual es el ciclo de flujo de datos, y quienes intervienen en ese flujo.

- Mantenga un inventario de hardware y software, identificar todos los dispositivos de hardware que se conectan a la red, quien es el responsable de ese activo, inventariar los softwares que están instalados y autorizados.

- Establezca políticas para la ciberseguridad que incluya roles y responsabilidades, estas políticas debe de estar el alcance, cómo se protegerá la información y sistemas, medios de respaldos utilizados y el medio de almacenamiento y actores que intervienen.

- Identifique amenazas, vulnerabilidades y riesgo para los activos, conociendo el listado de los activos se debe identificar los riesgos a los que están expuestos, se pueden utilizar la Magerit.

7.3.2 Protección

Tener herramientas apropiadas para asegurar los servicios y los sistemas de información, se compone de seis ítems

- Administre el acceso a los activos y la información, la administración es debe realizar por cuentas de usuarios agregados a un grupo de trabajo previamente verificando los permisos asignados, y el ingreso sea por autenticación para acceso a los sistemas.

- Proteja los datos confidenciales, con método de cifrado en tránsito y pasivo, tener un control de verificación de integridad para garantizar solo los cambios autorizados, garantizar la eliminación de datos de forma segura.

- Realice copias de seguridad periódicas, se debe de crear una política de respaldo de información (completa, diferencial, incremental) garantizar la frecuencia de las copias y restauraciones funcionales.

- Proteja sus dispositivos de forma segura, las medidas de protección como el firewall se debe de garantizar, verificación de log ante posibles cambios de configuración en los dispositivos de seguridad

- Administre las vulnerabilidades de los dispositivos, el responsable de la administración de los sistemas debe de garantizar que los sistemas operativos, aplicaciones estén actualizados, utilizar herramientas para el escáner de vulnerabilidades en los dispositivos.

- Capacitar a los usuarios, organizar un programa de capacitación periódicas, que cubra temas de políticas de ciberseguridad, medidas de protección, funciones y responsabilidades para el desarrollo del empleo.

7.3.3 Detección

Desarrollar estrategias apropiadas para la identificación de eventos de ciberseguridad.

- Probar y actualizar procesos de detección, procesos y herramientas para la detección de acciones no autorizadas en las redes, sistemas como en el entorno físico.

- Mantenga y supervise los registros, los registros son utilizados para verificar anomalías, cambios en los sistemas, cambios en privilegios de cuentas, por los cual es de importancia y ayuda en los procesos de seguridad.

- Conozca los flujos de datos esperados para su empresa, conocer el flujo de los procesos ayudan en la seguridad, debido si existe algún cambio es más probable que se note en el resultado, esta identificación de flujo se debe hacer interna como con proveedores.

- Comprender el impacto de los eventos de ciberseguridad, tener identificado el impacto, procesos involucrados ante un evento de seguridad pueda ayudar a disminuir la amplitud y profundidad.

7.3.4 Responder

Tener documentado los procedimientos ante eventos de ciberseguridad, personal a informar y acciones a seguir.

- Asegúrese de que se prueben los planes de respuesta, asegurarse que se aprueben por la alta dirección los planes de respuesta, estar organizados y preparados para actuar de forma más eficaz.

- Asegúrese de que los planes de respuesta estén actualizados, realizar pruebas ante incidentes permitirá mejorar y actualizar los planes.

- Coordinar las partes interesadas internas y externas, que todo el personal involucrado conozco su responsabilidad y las acciones que debe ejecutar.

7.3.5 Recuperar

Tener los planes de procedimientos actualizados para restaurar los sistemas afectados ante un ataque cibernético.

- Comunicarse con las partes interesadas internas y externas, la parte de la recuperación depende de la comunicación asertiva entre las partes.

- Asegúrese de que los planes de recuperación estén actualizados, asegurar que los planes de recuperación se encuentren actualizados, esto mejorará la conciencia de los empleados y socios.

- Gestionar las relaciones públicas y la reputación de la empresa, se debe garantizar la reputación de la organización con información precisa, completa y oportuna y permitir que se generen comentarios.

8 CONCLUSIONES

Las Pymes, siguen aportando a la seguridad de la información con políticas y herramientas, como a la construcción y puesta en marcha el Sistema De Gestión De Seguridad De La Información (SGSI), la mayor preocupación es la falta de presupuesto destinado a protección de la infraestructura como la de recurso humano calificado en seguridad informática, por debilidades que se presentan en las PYMES por falta de herramientas de seguridad, las grandes empresas corren riesgos de sufrir ciberataques, porque muchas de estas Pymes son proveedores o comparten algún servicio con grandes empresas.

El mercado tecnológico de seguridad informática para la protección de la información y ante ciberataques es muy amplio, existen muchos productos, de protección, respaldo y recuperación, monitoreo, físicos, virtuales, híbridos, entre otros; El inventario de activos (La identificación de activos informáticos y de información, aplicaciones, usuarios) es la política de seguridad que toda empresa debe de mantener actualizada; Se hace necesario para determinar cuáles son las estrategias y herramientas de seguridad perimetral que deben utilizar, para la detección, prevención y recuperación de la información y conocer el estado actual de los activos administrados, identificar en qué etapa del ciclo de vida se encuentra un activo, poder clasificarlo según su nivel de riesgo y protección, para determinar el análisis de inversión en seguridad informática requerida y contar con la ingeniera de detalle clara.

Las empresas tienen a la mano herramientas para implementar mejores prácticas en la ciberseguridad, protección de redes, datos y los riesgos asociados a la seguridad informática, cuentan con guías, marcos, controles que ayudan a las organizaciones a establecer los procesos de construcción de las políticas de seguridad, entre ellos los Controles De Seguridad Critica (CIS), Marco De Ciberseguridad Cibernética (NIST) y las guías del MINTIC; Los beneficios que obtienen, que les facilita la construcción del Sistema de Gestión de Seguridad de la Información, la elaboración de líneas bases de seguridad informática, protección de los datos, software, permite mejorar la postura como el nivel de seguridad sobre riesgos conocidos.

9 RECOMENDACIONES

Realizar una revisión periódica para mantener actualizado el inventario de activos informáticos que se encuentran asignados, como también ejecutar pruebas de Plan de recuperación de Desastres (DRP), le permitirá a la empresa garantizar la continuidad de los servicios, realizar pruebas de restauración aleatorias para comprobar la integridad y disponibilidad de la información, garantizar que el usuario se le otorguen los privilegios mínimos de acceso a las herramientas y documentar y revisar periódicamente el control y política de acceso.

Garantizar la seguridad informática con protección externa e interna, con herramientas de tipo hardware y/o software y con políticas de seguridad, reforzar la seguridad lógica perimetral con la utilización de firewall, entre ellos los de tipo WAF, que permite mayor protección de la red, aplicaciones y canales digitales, utilizar sistemas SIEM, Arbor, Nagios que le permiten monitore y respuesta ante incidentes, recomendado mantener actualizada las herramientas con las últimas versiones de los parches de seguridad, asegurar los puntos de acceso a la red y la señales WIFI con contraseñas, instalación de antivirus en los equipos, así mismo el personal de seguridad informática debe de estar actualizado sobre las nuevas vulnerabilidades, se recomienda estar incluido en grupos o comunidades de seguridad, como recomendación de factibilidad de presupuesto para obtener la mejor alternativa, analizar entre las opciones de: compra, alquiler y contratación con un tercero los servicios de seguridad, como también la administración de los servicios.

El Sistema De Gestión De Seguridad De La Información (SGSI)es un documento que toda empresa debe de contar, la elaboración requiere la ejecución de unas etapas según su alcance, se recomienda utilizar la norma ISO/IEC 27001 como guía que explica de forma clara cada una de las actividades para el desarrollo del SGSI, con el fin de mantener el sistema, la norma ISO/IEC 27002 brinda recomendaciones de controles de seguridad, utilizar los Controles de Seguridad Críticos (CIS) y el marco de ciberseguridad (NIST), con los cuales las empresas obtienen herramientas para la gestión de riesgos de seguridad informática y protección ante ciberataques conocidos, brindando una guía para la aplicación de líneas base de seguridad.

10 BIBLIOGRAFÍA

Acis. Ciberseguridad: la aliada de las PyMEs durante la realidad actual. [sitio web]. Bogotá D.C. [junio, 2020]. Disponible en: HTTPS://www.acis.org.co/portal/content/noticiasdelsector/ciberseguridad-la-aliada-de-las-pymes-durante-la-realidad-actual.

Acunetix. ¿Qué es la inclusión remota de archivos (RFI)?. [sitio web]. Ian Muscat. [2, abril, 2020]. Disponible en: HTTPS://www.acunetix.com/blog/articles/remote-file-inclusion-rfi/

Openwebinars. Diferencias entre amenazas y vulnerabilidades. [sitio web]. [14, octubre, 2020]. Disponible en: HTTPS://openwebinars.net/blog/diferencias-entre-amenazas-y-vulnerabilidades/

avansis. seguridad perimetral informática. qué es, definición y métodos para proteger tu negocio. [sitio web]. Disponible en: HTTPS://www.avansis.es/ciberseguridad/que-es-seguridad-perimetral/

backtrackacademy. Explotando la Vulnerabilidad LFI. [sitio web]. [4, octubre, 2016]. Disponible en: HTTPS://backtrackacademy.com/articulo/explotando-la-vulnerabilidad-lfi

bsigroup. Norma ISO/IEC 27017 - Controles de Seguridad para Servicios Cloud. [sitio web]. Disponible en: HTTPS://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

btob. ¿Qué es ISP o sistema de prevención de intrusos?. [sitio web]. [6, enero, 2021]. Disponible en: HTTPS://btob.com.mx/ciberseguridad/que-es-ips-o-sistema-de-prevencion-de-intrusosintrusion-prevention-system/

copro. Activo. [sitio web]. Disponible en: HTTPS://copro.com.ar/Activo_(seguridad_informatica).html

digicert. ¿QUÉ SON SSL, TLS Y HTTPS…?. [sitio web]. Disponible en: HTTPS://www.digicert.com/es/what-is-ssl-tls-HTTPS/

electrodata. 3 Tips de Seguridad en Aplicaciones Web. [sito web]. [21, abril, 2021]. Disponible en: HTTPS://www.electrodata.com.pe/tips-de-seguridad-en-aplicaciones-web/

Fortinet. ¿Qué es la seguridad de red? Tipos, soluciones y dispositivos. [sitio web]. Disponible en: HTTPS://www.fortinet.com/lat/solutions/enterprise-midsize-business/network-security

gb-advisors. Clickjacking: ¿Cómo protegerse de forma efectiva del UI redressing?. [sitio web]. [15, marzo, 2019]. Disponible en: HTTPS://www.gb-advisors.com/es/clickjacking-ui-redressing/

geekflare. Los 8 mejores firewalls de código abierto para proteger su red. [sitio web]. [8, junio, 2020]. Disponible en: HTTPS://geekflare.com/es/best-open-source-firewall/

hostdime. ¿Qué es una vulnerabilidad en seguridad informática?. [sitio web]. [22, junio, 2020]. Disponible en: HTTPS://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/
Incibe. Amenazas vs vulnerabilidades. [sitio web]. [20, marzo, 2017]. Disponibel en: HTTPS://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
infotecs. IDS - Sistema de Detección de Intrusos. [sitio web]. [12, marzo, 2019]. Disponible en: HTTPS://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html
intedya. ISO 27000 y el conjunto de estándares de Seguridad de la Información. [sitio web]. [1, septiembre, 2015]. Disponible en: HTTPS://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html
internet. Qué es el E-Mail o Correo electrónico. [sitio web]. Disponible en HTTPS://www.internet-didactica.es/e-mail-correo-electronico/
normas-ISO. ISO 27001 SEGURIDAD DE LA INFORMACIÓN. [sitio web]. Disponible en: HTTPS://www.normas-iso.com/iso-27001/
isotools. Sistemas de Gestión de Riesgos y Seguridad. [sitio web]. Disponible en: HTTPS://www.isotools.org/normas/riesgos-y-seguridad/iso-27001
itroque. Cómo mantener la seguridad de la red. [sitio web]. Disponible en: http://itroque.edu.mx/cisco/cisco1/course/module11/11.2.1.3/11.2.1.3.html
jtsec. SEGURIDAD OFENSIVA EN LA WEB. [sitio web]. Universidad nueva granada. Disponible en: HTTPS://www.jtsec.es/papers/Technical/hackingweb18.pdf
kal3bistruehacking. Ataques LFI (Local File Include) y RFI (Remote File Include). [sitio web]. Anonymous. [25, junio, 2014]. Disponible en: http://kal3bistruehacking.blogspot.com/2014/06/ataques-lfi-local-file-include-y-rfi.html
kaspersky. ¿Qué es la gestión unificada de amenazas (UTM)?. [sitio web]. Disponible en: HTTPS://latam.kaspersky.com/resource-center/definitions/utm
latinpymes. mas-del-60-de-las-brechas-de-seguridad-involucran-aplicaciones-web. [sitio web]. [19, junio, 2019]. Disponible en: HTTPS://www.latinpymes.com/mas-del-60-de-las-brechas-de-seguridad-involucran-aplicaciones-web/
malwarebytes. suplantación de identidad (phishing). [sitio web]. Disponible en HTTPS://es.malwarebytes.com/phishing/
manageengine. ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS?. [sitio web]. Disponible en: HTTPS://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html
NCSI. Indice nacional de seguridad cibernetica. [sitio web]. Disponible en: HTTPS://ncsi.ega.ee/ncsi-index/?order=rank
Nectec. ¿Qué es seguridad informática?. [sitio web]. Disponible en: HTTPS://www.netec.com/que-es-seguridad-informatica
ticnegocios. ¿Cuál es el coste de los ciberataques y de los hackers malignos en la economía mundial?. [sitio web]. Disponible en:

HTTPS://ticnegocios.camaravalencia.com/servicios/tendencias/cual-es-el-coste-de-los-ciberataques-y-de-los-hackers-malignos-en-la-economia-mundial/
nist. CYBERSECURITY FRAMEWORK. [sitio web]. Disponible en: HTTPS://www.nist.gov/cyberframework
nsit. ¿Qué es SIEM en seguridad informática?. [sitio web]. [9, junio]. Disponible en: HTTPS://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/
nmap. Guía de referencia de Nmap. [sitio web]. Disponible en: HTTPS://nmap.org/man/es/
north-networks. ¿Que es Nagios?. [sitio web]. [26, febrero, 2021], Disponible en: HTTPS://www.north-networks.com/que-es-nagios/
oracle. ¿Qué es un WAF?. [sitio web]. Disponible en: HTTPS://www.oracle.com/es/database/security/que-es-un-waf.html
Ostec. Seguridad perimetral, entienda los principales conceptos. [sitio web]. [9, noviembre, 2016]. Disponible en: HTTPS://ostec.blog/es/seguridad-perimetral/seguridad-perimetral-conceptos/
owasp. Los diez mejores de OWASP. [sitio web]. Disponible en: HTTPS://owasp.org/www-project-top-ten/
pandasecurity. Un millón de ataques de fuerza bruta a RDP cada día. [sitio web]. [18, mayo, 2020]. Disponible en: HTTPS://www.pandasecurity.com/es/mediacenter/seguridad/fuerza-bruta-rdp/
pmg-ssi. Blog especializado en Sistemas de Gestión. [sitio web]. [14, septiembre, 2017]. Disponible en: HTTPS://www.pmg-ssi.com/2017/09/iso-27001-clasificacion-de-la-informacion-2/
PROFITLINE. Actualmente cómo se encuentra Colombia en seguridad informática. [sitio web]. [26, febrero, 2019]. Disponible en: HTTPS://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/
larepublica, L. ¿Cuánto gastan las empresas para recuperarse después de un ciberataque?. [sitio web]. [27, julio, 2019]. Disponible en: HTTPS://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536
scielo. POLITICAS Y SEGURIDAD DE LA INFORMACION. [sitio web]. Fides [septiembre, 2008]. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008#:~:text=Una%20pol%C3%ADtica%20de%20seguridad%20es,los%20ambientes%20donde%20se%20crearon.
seas. Hardening: qué es y cómo endurecer las medidas de seguridad informáticas. [sitio web]. [9, marzo, 2021]. Disponible en: HTTPS://www.seas.es/blog/informatica/hardening-que-es-y-como-endurecer-las-medidas-de-seguridad-informaticas/
securityartwork. OWASP TOP 10 (III): Pérdida de autenticación y Gestión de Sesiones. [sitio web]. [24, marzo, 2010]. Disponible en

HTTPS://www.securityartwork.es/2010/03/24/owasp-top-10-iii-perdida-de-autenticacion-y-gestion-de-sesiones/
Semana. Una empresa puede tardar hasta 7 meses en detectar un ataque cibernético. [sitio web]. [10, septiembre, 2020]. Disponible en: HTTPS://www.semana.com/tecnologia/articulo/cuanto-tiempo-tarda-una-empresa-en-detectar-un-ataque-cibernetico/299701/
Semana. Empresa pagó un millonario rescate por un ciberataque, pero el mismo hacker volvió a atacar en menos de dos semanas. [sitio web]. [2, febrero, 2021]. Disponible en: HTTPS://www.semana.com/tecnologia/articulo/empresa-pago-un-millonario-rescate-por-un-ciberataque-pero-el-mismo-hacker-volvio-a-atacar-en-menos-de-dos-semanas/202131/
sic. Ley1273. [sitio web]. [5, enero, 2009]. Disponible en: HTTPS://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
SOFISTIC. Colombia ocupa el puesto 39 en el ranking mundial sobre ciberseguridad. [sitio web]. [2, junio. 2020]. Disponible en: HTTPS://www.larepublica.co/globoeconomia/ciberseguridad-otro-reto-que-deben-enfrentar-las-empresas-en-el-mundo-por-covid-3013083
spri. NAGIOS: Herramienta para gestión-diagnóstico de Red en Linux. [sitio web]. Disponible en: HTTPS://www.spri.eus/euskadinnova/es/enpresa-digitala/agenda/nagios-herramienta-para-gestion-diagnostico-linux/3909.aspx
strato. ¿Qué es SPAM y cómo puedo protegerme?. [sitio web]. Disponible en HTTPS://www.strato.es/faq/correo/que-es-spam-y-como-puedo-protegerme/
synopsys. Inyección LDAP. [sitio web]. Disponible en: HTTPS://www.synopsys.com/glossary/what-is-ldap-injection.html
computerweekly. Cómo desarrollar e implementar un plan de seguridad de red. [sitio web]. [29, octubre, 2019]. Disponible en: HTTPS://searchdatacenter.techtarget.com/es/consejo/Como-desarrollar-e-implementar-un-plan-de-seguridad-de-red
tecnoseguro. ¿Qué es un Sistema de Control de Acceso?. [sitio web]. Disponible en: HTTPS://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso
tpempresas. Los 10 mejores firewalls de hardware para redes domésticas y de pequeñas empresas (2019). [sitio web]. [14, noviembre, 2019]. Disponible en: HTTPS://tpempresas.com/los-10-mejores-firewalls-de-hardware-para-redes-domesticas-y-de-pequenas-empresas-2019
welivesecurity. Ataque de ransomware afecta a BancoEstado en Chile. [sitio web]. [8, septiembre, 2020]. Disponible en: HTTPS://www.welivesecurity.com/la-es/2020/09/08/ataque-ransomware-afecta-bancoestado-chile/#:~:text=El%20pasado%20fin%20de%20semana,Sodinokibi%2C%20tambi%C3%A9n%20conocido%20como%20Revil.
Welivesecurity. Ataques al RDP crecieron 768% entre el primer y el último trimestre de 2020. [sitio web]. [8, febrero, 2020]. Disponible en:

HTTPS://www.welivesecurity.com/la-es/2021/02/08/ataques-rdp-crecieron-entre-primer-ultimo-cuatrimestre-2020/
Workspace, Conceptos básicos de DNS. [sitio web]. Disponible en: HTTPS://support.google.com/a/answer/48090?hl=es
xataka. Servidores NAS. [sitio web]. [8, octubre, 2018]. Disponible en: HTTPS://www.xataka.com/basics/servidores-nas-que-como-funcionan-que-puedes-hacer-uno
zdnet. Los principales exploits utilizados por las bandas de ransomware son errores de VPN, pero RDP sigue reinando. [sitio web]. [23, agosto, 2020]. Disponible en: HTTPS://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/