ANÁLISIS DE LOS ESTÁNDARES Y BUENAS PRÁCTICAS DE CIBERSEGURIDAD UTILIZADOS POR LA INDUSTRIA COLOMBIANA

RODRIGO DÍAZ CHANTRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ZCSUR CALI

2023

ANÁLISIS DE LOS ESTÁNDARES Y BUENAS PRÁCTICAS DE CIBERSEGURIDAD UTILIZADOS POR LA INDUSTRIA COLOMBIANA

RODRIGO DIAZ CHANTRE

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMATICA

Edgar Mauricio López Rojas

Director de trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

ZCSUR CALI

2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Cali, 2023

DEDICATORIA

Antes que nada, quiero agradecer a Dios por haberme permitido llegar hasta este punto de mi carrera donde comienzo a superar el nivel profesional y me encamino a tener un enfoque más agudo en una de las cosas que más me apasiona como lo es la ciberseguridad.

En segunda instancia, dedico este logro a mi familia que siempre me han dado su apoyo incondicional, mi madre, mi padre, mi hermana, mi hija y mi esposa que nunca dudaron de mis capacidades y entendiendo los esfuerzos de tiempo que requiere este proyecto académico, han comprendido siempre mi limitado tiempo para actividades familiares pero que habrán valido la pena, a todos les agradezco y les dedico esta nueva etapa de mi vida como profesional especializado.

AGRADECIMIENTOS

Quiero agradecer a todo el equipo de tutores de la Universidad Nacional Abierta y a Distancia UNAD, equipo que ha sido parte fundamental en este proceso aportando con su experiencia la orientación que he necesitado para lograr el cumplimiento de esta nueva meta, agradecerles también todo el material de apoyo entregado durante el proceso, las conferencias grupales donde han despejado dudas y brindado una guía clara sobre todo el tema de la correcta presentación de las actividades.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

RESUMEN

A pesar de la forzada transformación digital que han sufrido la mayoría de empresas, muchas no le han dado la suficiente importancia al tema de ciberseguridad, el elevado número de ciberataques ha hecho que las organizaciones comiencen a pensar en hacerse a una dependencia de seguridad cibernética para contrarrestar esta creciente oleada, por tal razón, es necesario que se revisen los controles de seguridad que se deben aplicar a nivel de infraestructura cibernética en general, al mismo tiempo se requiere una adecuada gestión de riesgos que puedan ayudar a identificar y mitigar estas vulnerabilidades.

La implementación de controles de seguridad informática ayuda a todas las áreas de la organización a mantener la integridad, disponibilidad y confidencialidad de la información, los tres grandes pilares de la seguridad de la información, por eso podemos decir que seguridad informática y seguridad de la información tienen mucha relación, aunque no signifiquen lo mismo.

Todos los colaboradores de una organización son actores base que contribuyen a un sistema de gestión de seguridad de la información, pero se cuenta con un oficial de seguridad responsable de ese sistema y de dejarle saber a cada colaborador como aportar a ese sistema y a cuidar su propia información.

Expertos también hacen sus aportes a la ciberseguridad en las organizaciones con sus propias investigaciones, toda esta recolección de experiencias y de buenas prácticas, son de gran ayuda para el mejoramiento continuo del SGSI y a las técnicas de ciberdefensa que tiene una estrecha relación con el sistema.

ABSTRACT

Despite the forced digital transformation that most companies have undergone, many have not given enough importance to the issue of cybersecurity, the high number of cyber-attacks has made organizations begin to think about becoming a cybersecurity unit to counteract this growing wave, for this reason, it is necessary to review the security controls to be applied at the level of cyber infrastructure in general, at the same time it requires proper risk management that can help identify and mitigate these vulnerabilities.

The implementation of IT security controls helps all areas of the organization to maintain the integrity, availability and confidentiality of information, the three main pillars of information security, so we can say that IT security and information security are closely related, although they do not mean the same thing.

All the employees of an organization are key players who contribute to an information security management system, but there is a security officer responsible for this system and for letting each employee know how to contribute to this system and how to take care of their own information.

Experts also make their contributions to cybersecurity in organizations with their own research, all this collection of experiences and good practices, are of great help for the continuous improvement of the ISMS and cyber defense techniques that have a close relationship with the system.

INTRODUCCIÓN

En la actualidad, la seguridad de la información se ha convertido en un tema de gran importancia debido a la creciente amenaza de ciberataques y la necesidad de proteger los activos de información de las empresas. Es por eso que muchas organizaciones están implementando estándares y marcos de referencia como ISO 27001, NIST y COBIT para asegurar la confidencialidad, integridad y disponibilidad de su información.

En este documento se llevará a cabo un análisis documental de las tres normas mencionadas, identificando sus ventajas en la gestión de la seguridad de la información. Se examinarán los requisitos clave de cada norma y se proporcionará una guía de la documentación necesaria para cumplir con estos requisitos. Se espera que los resultados de este trabajo sean de utilidad para las empresas colombianas que estén considerando la implementación de alguna de estas normas en su gestión de seguridad de la información, ya que proporcionará información valiosa sobre las características y beneficios de cada una de ellas.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El uso de las tecnologías de la información y la comunicación (TIC) se ha convertido en una parte integral de la mayoría de las organizaciones no solo en Colombia sino en todo el mundo. La creciente dependencia de las TIC para la realización de procesos empresariales críticos ha llevado a un aumento en el número de amenazas cibernéticas. Las amenazas cibernéticas incluyen virus, malware, phishing, robos de identidad, ataques de denegación de servicio (DoS), entre otros.

Estos ataques cibernéticos pueden ser extremadamente costosos y peligrosos para las organizaciones, ya que pueden resultar en la pérdida de datos valiosos, dañar la reputación de la empresa, y en casos extremos, incluso poner en peligro la seguridad física de las personas. Por lo tanto, es esencial que las organizaciones cuenten con medidas de seguridad adecuadas para proteger sus activos de la amenaza cibernética.

A medida que las organizaciones se han vuelto más conscientes de los riesgos asociados con la seguridad cibernética, ha habido un aumento en la adopción de estándares y buenas prácticas de ciberseguridad. Estos estándares y prácticas incluyen ISO 27001, NIST, COBIT, entre otros. Si bien estas iniciativas pueden ayudar a mejorar la seguridad cibernética de una organización, todavía hay desafíos significativos que enfrentan las empresas en la implementación efectiva de estas medidas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede optimizar la ciberseguridad en las organizaciones del sector industrial en Colombia mediante un análisis integral de los frameworks, metodologías y estándares de ciberseguridad utilizados, considerando sus ventajas y desventajas, para finalmente diseñar una estructura de controles y buenas prácticas específicamente adaptados a las necesidades de la industria colombiana?

2 JUSTIFICACIÓN

La documentación sobre ciberataques y sus nuevas técnicas, ofrece una base importante para brindar una orientación efectiva a la industria Colombiana en la identificación concreta de sus necesidades de seguridad y la mejor manera de aplicarlas a sus propios contextos, es muy importante que en todas las áreas de una organización entiendan de qué manera los puede afectar una amenaza informática y como pueden prevenir la materialización de la misma.

Este estudio también abarca todas las recomendaciones que presentan las máximas autoridades de seguridad a nivel mundial, todo esto permite que se tenga una visión más clara sobre el panorama de ciberseguridad y como puede ser aplicada en las organizaciones teniendo en cuenta la necesidad actual de protección a los sistemas de información de las entidades.

Este análisis debe tener un resultado positivo en materia de ciberseguridad, es decir, que una vez revisado todo el contenido de este documento, se puedan generar planes de acción, de implementación o de mejora para las áreas encargadas de ciberseguridad en caso de que la organización cuente con una, de lo contrario, se tendría una idea clara de por dónde empezar a desarrollar el área en mención además de definir unas tareas puntuales y otras no tan recurrentes pero igualmente importantes para la seguridad digital.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Estructurar un análisis general de los estándares de ciberseguridad y seguridad de la información mas usados en la industria colombiana en la actualidad, revisando a un mayor nivel de detalle las buenas prácticas que se describen en estas normas.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar la ciberseguridad en las organizaciones del sector industrial basado en documentos, artículos, encuestas del sector industrial con el ánimo de reconocer los más adecuados a la industria

- Examinar Los Frameworks, metodologías, estándares de ciberseguridad Validando sus ventajas y desventajas como una guía práctica de apoyo a las industrias

- Estructurar Controles y buenas prácticas Basados en los diferentes framework, estándares del mercado

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El análisis de los estándares y buenas prácticas de ciberseguridad utilizados por la industria colombiana tiene dos componentes importantes que lo integran, la seguridad de la información y la ciberseguridad, si bien son dos conceptos que tienen mucha relación, tienen enfoques teóricos diferentes:

4.1.1 Seguridad de la información

Busca establecer una política de seguridad de la información que proteja los activos de información con la definición general de directrices para la implementación de seguridad de la información en los demás procesos organizacionales internos.

El cumplimiento de esta política de seguridad es alcanzable mediante procedimientos, controles, instructivos, publicaciones y en la definición y asignación de roles y responsabilidades.

4.1.2 Ciberseguridad

La ciberseguridad en teoría son un conjunto de prácticas destinadas a proteger las infraestructuras tecnológicas incluyendo, dispositivos móviles, sistemas electrónicos, redes de computadoras de los diferentes tipos de ataques, dentro del marco teórico de ciberseguridad, encontramos varias categorías:

- Seguridad en redes:

En esta rama se hace referencia a los procesos de Hardening de todo el proceso de comunicaciones apoyándose en herramientas de tipo Hardware como Firewalls y Switch Administrable y configuraciones como segmentaciones de red, filtro de contenido, bloqueo de sitios maliciosos, detección y prevención de intrusos, entre otras configuraciones.

- Seguridad en aplicaciones:

Teóricamente en este aspecto se pretende aplicar procesos de seguridad durante el desarrollo de software y aplicaciones como tal, teniendo en cuenta los riesgos más críticos de la organización que pretende hacerse con la aplicación.

- Seguridad de las operaciones:

Este proceso es importante, es aquí donde se clasifica información y se determina cuáles son las necesidades para proteger la información confidencial, se requiere de mucho análisis en esta fase para evitar que la información termine en manos equivocadas.

4.2 MARCO CONCEPTUAL

Se deben tener muy claros todos los conceptos usados en ciberseguridad para lograr un entendimiento completo de esta monografía:

- [1]Los UTM Por sus siglas en ingles “Gestión unificada de amenazas” son dispositivos tipo hardware que como su nombre lo dice, realiza una gestión centralizada de amenazas cibernéticas que puedan tener un impacto negativo en la organización, estos dispositivos incorporan mínimamente las siguientes funcionalidades:

  - IDS e IPS: Sistemas de prevención y detección de intrusos.
  - Firewall.
  - Antivirus.
  - Antispam.
  - Filtrado de contenido.
  - Conexiones VPN (Túnel y cliente).
  - Anti-phishing.

- Seguridad de la información es básicamente la conservación de la integridad, confidencialidad y disponibilidad de la información según la norma ISO 27001, esta norma contiene unas pautas y controles que ayudan a preservar esos tres grandes pilares.

- Amenazas informáticas se les llama a todas aquellas situaciones que podrían permitir la materialización de un ciberataque a causa de vulnerabilidades en los sistemas informáticos o por desconocimiento de los colaboradores de las organizaciones que sean objetivo de los piratas informáticos.

- Malware es un término se usa para señalar un tipo de software invasivo, abarca una gran cantidad de variantes, entre ellos, caballos de troya, gusanos, virus, etc. Generalmente, usan scripts o código ejecutable que a su vez puede descargar otro software o enviar información a otro sitio, de acuerdo con su parametrización.

[1] Infobae. UTM, un firewall que ha ido al gimnasio [en línea]. 28 de febrero de 2019. [Consultado el 9 de abril de 2023]. Disponible en: https://www.incibe.es/empresas/blog/utm-firewall-ha-ido-al-gimnasio

- Criptografía se le llama al mecanismo para proteger la información que viaja a través de redes de comunicaciones, se protege usando claves y algoritmos que solamente conocen el receptor y el emisor.

- ISP es un “Proveedor de servicios de internet” encargada de suministrar internet a organizaciones como tal y a personas de manera residencial.

- Cloud Computing es la “Computación en la nube” un servicio de infraestructura tecnológica ofertado haciendo uso de la conectividad a internet, es decir, es una infraestructura que puede ser accedida a través de la conexión a internet desde cualquier ubicación, los más grandes proveedores en la actualidad son GOOGLE y AWS.

- Las vulnerabilidades son las debilidades o deficiencias de un sistema informático que se constituye en un riesgo de seguridad comprometiendo la integridad, disponibilidad y confidencialidad de la información aprovechable por un pirata informático.

- La Ciberseguridad es la actividad que se realiza para proteger o defender las infraestructuras tecnológicas y todas las categorías que esta contiene

4.3 MARCO HISTÓRICO

A lo largo del tiempo y el incremento del uso de tecnologías de la información en Colombia, también se ha incrementado el número de ataques a diferentes entidades, el colectivo activista conocido como “Anonymous” se ha adjudicado muchos de los ataques históricos en Colombia y a nivel mundial, en el año 2011 fueron atacados varios portales gubernamentales en protesta por leyes de

antipiratería, estas leyes intentaban establecerse no solo a nivel nacional sino mundial, en muchos otros países también este colectivo “Anonymous” lanzo diferentes ataques a sitios web de distintos gobiernos y firmas disqueras.

Durante la pandemia se dieron a conocer un sin número de ataques principalmente de tipo ransomware, la empresa de seguridad Fortinet asegura que Colombia tuvo 3.700 millones de intentos de ataques en el transcurso del semestre 1 de 2021, Colombia es uno de los países top en intentos de ataque en la región. Según la revista Semana indica que el sector industrial y manufacturero presento el número más alto de ataques ejecutados por piratas informáticos a nivel global superando incluso al sector financiero que ha sido sin duda el blanco más apetecido por estos ciberdelincuentes.

4.4 ANTECEDENTES O ESTADO ACTUAL

En la actualidad, Colombia es uno de los países de la región que más ha avanzado en la implementación de políticas y regulaciones en materia de ciberseguridad. Sin embargo, aún existen importantes desafíos en este campo, como el aumento de los ataques cibernéticos y la falta de conciencia y capacitación de los usuarios finales.

La industria colombiana se encuentra en la necesidad de establecer medidas de seguridad efectivas para proteger su información y sus sistemas ante la creciente amenaza de los ciberataques. En este sentido, los estándares y buenas prácticas de ciberseguridad se han convertido en una herramienta esencial para lograr una protección adecuada.

Existen diferentes estándares y marcos de buenas prácticas para la implementación de medidas de ciberseguridad, como ISO/IEC 27001, NIST, COBIT, entre otros. Sin

embargo, aún hacen falta recomendaciones efectivas para la implementación de estas medidas, como la falta de recursos y la resistencia al cambio en las empresas.

Es necesario destacar que la pandemia de COVID-19 ha tenido un impacto significativo en la ciberseguridad en Colombia y en todo el mundo. La aceleración de la digitalización ha aumentado el riesgo de ataques cibernéticos y ha evidenciado la necesidad de fortalecer las medidas de seguridad en las empresas.

4.5 MARCO LEGAL

Colombia con el claro objetivo de robustecer la capacidad del estado y proteger al ciudadano de los ciber delitos, ha gestionado algunas legislaciones importantes en el aspecto de seguridad de la información y protección a las infraestructuras de tecnología, con base en lo anterior, se menciona la normatividad vigente:

Ley No 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley No 599 de 2000: Art 192: *Violación ilícita de comunicaciones*. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

Ley No 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y

de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley No 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Decreto No 2364 de 2012: Que se hace necesario reglamentar la firma electrónica para generar mayor entendimiento sobre la misma, dar seguridad jurídica a los negocios que se realicen a través de medios electrónicos, así como facilitar y promover el uso masivo de la firma electrónica en todo tipo de transacciones.

Ley No 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto No 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.

Decreto 1078 de 2015: Este decreto establece la regulación para la seguridad de la información en las entidades públicas de Colombia, incluyendo los estándares y buenas prácticas que deben seguirse para proteger la información.

Ley 1753 de 2015: Esta ley regula el sistema de salud en Colombia y establece las obligaciones y derechos de los prestadores de servicios de salud y los usuarios del sistema, incluyendo la protección de la información de los pacientes.

5 DESARROLLO DE LOS OBJETIVOS

La seguridad informática en las organizaciones del sector industrial ha adquirido una importancia cada vez mayor en un entorno digital altamente interconectado. La creciente dependencia de sistemas y tecnologías en el ámbito industrial ha generado nuevos desafíos en términos de ciberseguridad, ya que las amenazas y vulnerabilidades específicas de este sector pueden tener un impacto significativo en la integridad de los procesos, la confidencialidad de la información y la continuidad operativa.

El presente documento tiene como objetivo abordar la evaluación y fortalecimiento de la ciberseguridad en las organizaciones del sector industrial. Para ello, se llevará a cabo una exhaustiva revisión de documentos, artículos y encuestas relacionados con la ciberseguridad en este ámbito, con el propósito de identificar los enfoques más adecuados y pertinentes a la industria. Esta evaluación permitirá comprender el estado actual de la seguridad informática en el sector industrial y reconocer las mejores prácticas y enfoques exitosos implementados en organizaciones similares.

Además, se examinarán los frameworks, metodologías y estándares de ciberseguridad disponibles, validando sus ventajas y desventajas como una guía práctica de apoyo a las industrias. Mediante esta revisión exhaustiva, se pretende ofrecer a las organizaciones del sector industrial una visión clara de los marcos de referencia y herramientas disponibles para fortalecer su postura de seguridad cibernética. Se analizarán los beneficios y limitaciones de cada enfoque, considerando su aplicabilidad, adaptabilidad y eficacia en entornos industriales específicos.

Por último, se estructurarán controles y buenas prácticas basados en los diferentes frameworks y estándares del mercado. Estos controles y prácticas serán diseñados

para abordar los desafíos específicos del sector industrial y ayudar a las organizaciones a establecer medidas sólidas de protección cibernética. Se brindará una guía práctica para la implementación y gestión de controles de seguridad, con el objetivo de salvaguardar los activos digitales, mitigar los riesgos y promover una cultura de seguridad en el entorno industrial.

A través de este documento, se busca contribuir al fortalecimiento de la ciberseguridad en las organizaciones del sector industrial, proporcionando un análisis completo de la situación actual, así como recomendaciones prácticas para mejorar la protección cibernética. La seguridad informática se ha convertido en una prioridad estratégica en el ámbito industrial, y es fundamental contar con enfoques y prácticas eficaces que permitan a las organizaciones enfrentar los desafíos actuales y futuros en materia de seguridad cibernética.

5.1 EVALUAR LA CIBERSEGURIDAD EN LAS ORGANIZACIONES DEL SECTOR INDUSTRIAL BASADO EN DOCUMENTOS, ARTICULOS, ENCUESTAS DEL SECTOR INDUSTRIAL CON EL ANIMO DE RECONOCER LOS MAS ADECUADOS A LA INDUSTRIA.

Con base en la acelerada digitalización en Colombia los últimos años, la seguridad digital ha adquirido una importancia bastante alta y crece conforme avanza todo este proceso de transformación digital.

[2]Es cierto que las empresas en Colombia han invertido significativamente en seguridad digital, esto debido en gran parte a la pandemia del COVID-19, finalizando

[2] Portafolio. La demanda de servicios de ciberseguridad creció 40%. [en línea]. 8 de febrero de 2022. [Consultado 6 de noviembre de 2023]. Disponible en: https://www.portafolio.co/innovacion/la-demanda-de-servicios-de-ciberseguridad-crecio-40-561523

el trimestre 1 de 2020, la necesidad de ciberseguridad tuvo un incremento del 40% reporto la cámara colombiana de informática y telecomunicaciones.

Por otra parte, el centro cibernético de la policía nacional informo que en el semestre 1 de 2020 hubo un alza del 59% en las denuncias relacionadas con ciber delitos comparado con el año pasado.

Aparte de la seguridad que puedan implementar las empresas, sus colaboradores son parte esencial para evitar ciber ataques, [3]de acuerdo con una encuesta realizada por Kaspersky con una firma consultora CORPA se pudo determinar que:

- En Latinoamérica el 33% de las personas no conoce los impactos que pueden causar los ataques informáticos, el porcentaje para Colombia es del 31%, un poco menor pero sigue siendo relativamente alto.

- Hay un alto desconocimiento de conceptos y términos muy comunes de ciberseguridad como lo son phishing, Ransomware y malware.

- En Colombia el 60% de las personas tienen cuidado al momento de usar el correo corporativo.

- El 90% de empleados en Colombia saben que los ciber ataques tienen impactos fuertes en las empresas.

- Solo el 10% considera improbable que se ataque digitalmente a las pymes porque estas no manejan grandes sumas de dinero comparadas con otras organizaciones.

[3] DIAZ Granados H. KASPERSKY. Un tercio de latinos desconoce daños que ciberataques podrían ocasionar en empresas [en línea]. 07de julio de 2020. [Consultado el 9 de abril de 2023]. Disponible en: https://latam.kaspersky.com/blog/un-tercio-de-latinos-desconoce-danos-que-ciberataques-podrian-ocasionar-en-empresas/19600/

A lo largo de este numeral se estará revisando de manera general el estado actual y direccionamiento de la seguridad digital en Colombia y las empresas que pretenden digitalizar sus procesos para que tengan en cuenta los riesgos que esto conlleva.

[4]En la actualidad, vemos que los procesos de digitalización se están llevando a cabo de una manera muy rápida en todos los países y en organizaciones de todos los sectores. Estas organizaciones están trabajando en diferentes iniciativas para la transformación digital de sus procesos y servicios, incrementando su eficiencia, mejorando sus vínculos con el cliente y adoptando el uso de nuevas herramientas para análisis. Estos excelentes beneficios con los que podría contar una organización sometida a procesos generales de digitalización también elevan drásticamente su superficie de ataque, esto como consecuencia de que en muchas de estas transiciones no se contemplan múltiples factores de riesgo. Por esta razón, es altamente recomendado que todas las organizaciones cuenten con ciberseguridad en su infraestructura para que se pueda entender los riesgos asociados a este proceso de digitalización.

El afán de estos procesos de digitalización ha hecho que se dejen los aspectos de seguridad digital o ciberseguridad para lo último y más desde el momento en que forzosamente hubo la necesidad de realizar jornadas de teletrabajo a raíz de la pandemia de 2020, las organizaciones han tenido que hacer procesos de innovación durante la transición, a medida que las áreas de TI (Tecnologías de la información) y TO (Tecnologías operativas) han ido uniendo esfuerzos, la seguridad digital ha detectado la necesidad de adicionar riesgos a los objetivos de estas áreas que no tuvieron en cuenta durante sus configuraciones.

[4] BELTRÁN Simó. Revista Semana: Tendencias en ciberseguridad para el 2022. [en línea]. 4 de abril de 2022. [Consultado el 23, octubre de 2022]. Disponible en: https://www.semana.com/economia/empresas/articulo/tendencias-en-ciberseguridad-para-el-2022/202240/

La amenaza más común en la actualidad es llamada Ransomware, es un software dañino que una vez ha logrado infectar un sistema, secuestra la información mediante algoritmos de cifrado, restringiendo el acceso para extorsionar al propietario con sumas de dinero en algunos casos millonarias, a pesar de que el Ransomware tiene varios años de ser conocido a nivel informático, ha evolucionado a tal punto que no ha sido fácil su detección en numerosas víctimas.

Para hacerle frente a esta problemática, se requiere que las organizaciones hagan uso de estrategias de prevención, divulgación y notificaciones, generación de planes de respuesta organizacional y coordinación, y aplicación de fundamentos como segmentar las redes para contar con una infraestructura resiliente.

Otro ataque bastante común es a software de uso gratuito como por ejemplo, las nubes públicas (para citar algunos: Nextcloud, Owncloud) en este caso el riesgo está centrado en las configuraciones por defecto, es decir, se implementan estas aplicaciones pero no se cambian las configuraciones que traen por defecto lo que hace fácil para los atacantes, acceder a estas aplicaciones para diferentes propósitos delictivos, el uso de este tipo de software implica el uso de buenas prácticas de seguridad como por ejemplo, contraseñas robustas, uso de WAF (Web Application Firewall), Antivirus, estos son los requisitos mínimos a aplicar antes de publicar estos servicios hacia internet.

Con base en lo anterior, es de suma importancia que los lideres de proceso de las empresas, tengan presente todos estos riesgos, los conozcan en cierta medida y tengan planes de acción para mitigar o eliminar estos riesgos; claramente necesitan apoyo del personal de TI, TO y ciberseguridad, la junta directiva de cada organización debe considerar estos primordiales puntos:

1. **Generar conciencia entre los miembros de la junta directiva:** Dado que la seguridad digital es un reto que a voluntad o a fuerza muchas organizaciones asumieron implícitamente con la aplicación de teletrabajo, ahora deben entender y valorar los riesgos a los que expusieron la organización con estos nuevos procesos.

2. **Asegurar los procesos críticos de la organización y sus activos:** Es de vital importancia la conformación de un equipo con personal de conocimiento técnico y personal administrativo para mantener un equilibrio de controles técnicos y productividad del activo asegurado para no impactar la misma productividad e innovación de los procesos.

3. **Desarrollar cultura y habilidades de seguridad digital en todos los colaboradores de la organización:** El ultimo, pero no menos importante aspecto a tener en cuenta es que la seguridad es responsabilidad de todos, es decir, cada integrante de la organización tiene un cierto porcentaje de responsabilidad de asegurar la información o activos bajo su dominio, por esto es importante que tenga fundamentos de seguridad digital y tenga claridad de donde puede recibir ayuda o asesoría en este aspecto cuando la situación o problema tenga una dimensión mayor a la de su conocimiento.

[5]XXII Encuesta Nacional de Seguridad Informática

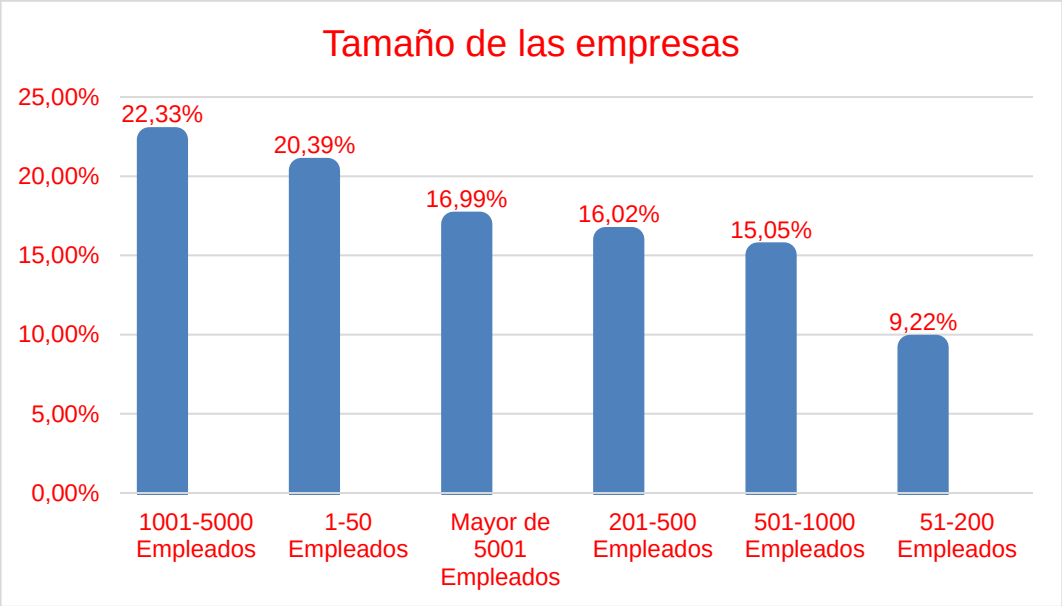
El sondeo sobre la seguridad informática en Colombia, respaldado por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y ejecutado online entre marzo y mayo de 2022, registró la participación de 206 individuos. Las respuestas obtenidas brindan una perspectiva sobre el estado actual de la seguridad informática en el

[5] ALMANZA Andrés. XXII Encuesta Nacional de Seguridad Informática.s-f. [Consultado el 6 de noviembre de 2023]. Disponible en: *https://sistemas.acis.org.co/index.php/sistemas/article/download/186/146*

país. La convocatoria para participar en la encuesta se realizó a través de diversas redes sociales y grupos comunitarios. Los datos recopilados reflejan un cambio en las prácticas de seguridad y gestión dentro de Colombia, los cuales se han comparado con estándares internacionales escogidos para esta edición del estudio.

A continuación se relaciona el tamaño de las diferentes empresas que hicieron parte de la encuesta realizada, la figura 1 nos muestra que hay un cierto nivel de proporcionalidad de ciberseguridad en las empresas de acuerdo con su tamaño:

Figura 1: Tamaño de las empresas encuestadas



Fuente: *https://sistemas.acis.org.co/index.php/sistemas/article/download/186/146*

La Figura 2 ilustra los diversos tipos de incidentes ocurridos en las organizaciones. Se identifica que los errores humanos constituyen el 38%, el phishing el 32%, y los ataques de ingeniería social representan el 25%, siendo estos últimos los tres más frecuentes.

Figura 2: Principales tipos de incidentes de seguridad a nivel general

Fuente: *https://sistemas.acis.org.co/index.php/sistemas/article/download/186/146*

Pero como están invirtiendo las empresas en ciberseguridad? La encuesta nos permite tener un panorama un poco mas claro a nivel general, la figura 3 indica que un numero importante de organizaciones va por el camino correcto pero debido al incremento de ciber delitos, se debe reforzar esta inversión:

Figura 3: Inversiones en ciberseguridad de las organizaciones encuestadas

Fuente: *https://sistemas.acis.org.co/index.php/sistemas/article/download/186/146*

Uno de los datos mas relevantes para esta investigación es conocer un porcentaje de uso de estándares de ciberseguridad y marcos de trabajo que más usan las organizaciones:

Tabla 1: Marcos y estándares de ciberseguridad mas usados en las organizaciones

Marco de referencia	Porcentaje
ISO 27001	69%
Guías NIST (National Institute of Standards and Technology)	37%
ITIL	26%
COBIT	20%
PCI-DSS	17%
Ninguna	6%
Guías ENISA (European Network of Information Security Agency)	6%
ISM3 – Information Security Management Maturity Model	3%

Fuente: *https://sistemas.acis.org.co/index.php/sistemas/article/download/186/146*

Reseña de principales ataques a empresas en Colombia

[6]En Colombia el fenómeno de los ciberataques va en aumento, el registro en el centro cibernético de la policía nacional en el lapso de enero a octubre de 2022 se conocieron 54.000 ciberataques.

RAMSONWARE

Es por mucho, el ataque más común entre los muchos reportes en Colombia y a nivel mundial también, este básicamente consiste en el secuestro de información y el pago del afectado al ciberdelincuente por la recuperación de esta información, una de las recomendaciones que hacen los principales proveedores de seguridad es la realización de copias de respaldo regulares, esto hace parte también de uno de los controles de seguridad de la norma ISO 27001.

PHISHING

Podríamos afirmar que esta se cuenta entre las estrategias más frecuentemente empleadas para dirigir ataques contra empresas en términos generales. Esencialmente, implica el envío de comunicaciones fraudulentas que en ocasiones contienen archivos dañinos, con la intención de obtener credenciales o, en situaciones más críticas, adueñarse de sistemas informáticos y servidores para llevar a cabo la sustracción de datos.

DoS DENEGACIÓN DE SERVICIO

[6] VARGAS Natalia. Las empresas que han sido blanco de ciberataques en Colombia en el último año. [en línea]. 25 de enero de 2023. [Consultado el 6 de noviembre de 2023]. Disponible en: https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667

[7]Este tipo de ataque también es muy común, no tiene intenciones de algún tipo de robo, la intención de este ataque es causar afectación al servicio prestado por un activo de información (principalmente dirigido a portales web), para evitar este tipo de ataques, se requiere contar con servicios de protección especializados. Actualmente los más eficientes son los WAF (Web Application Firewall) de los proveedores AWS, AZURE, CLOUDFLARE.

Empresas que fueron víctimas de ciberataques en Colombia 2022

Al finalizar el año 2022 en Colombia, se registraron ciberataques importantes en empresas pequeñas y en otros casos de mayor dimensión, entre los casos más sonados se encuentra el caso de EPM (Empresa Pública de Medellín) y el caso de la EPS SANITAS, en total fueron 34 las empresas en general que sufrieron ese tipo de afectación en su infraestructura tecnológica.

El listado de empresas víctimas de ciberataques que se dio a conocer se relaciona en la tabla 1 a continuación:

Tabla 2. Empresas víctimas de ciberataques en Colombia 2022

Salud Total.	Viva Air.	Independence.	Red de Salud de Ladera.
Universidad Javeriana.	Carvajal.	Cachibi.	SiesaCloud.
Invima.	Outsourcing IT.	Comfacundi.	Famisanar.
GHT Corp.	Emtelcom.	Newhotel Software.	Gas Caribe.
Universidad Piloto.	CIELD.	Flores Funza.	Procaps Laboratorios.
EPM Medellín.	Codifer SAS.	AcciónPlus.	OpenGroup SAS.
Caracol TV.	Clínica Laura.	FebanColombia.	Corferias.
Claro Colombia.	Quintal.	Club Campestre.	Red de Salud de Ladera.
Electricaribe.	Grupo Sanford.	Keralty (Sanitas).	SiesaCloud.

Fuente: *https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/*

[7] CLOUDFLARE. ¿Qué es un ataque de denegación de servicio (DoS)? [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

CASO KERALTY SANITAS

Los hackers expusieron datos adicionales confidenciales de la EPS.

[8]El grupo de hackers Ransomhouse, que atacó el sistema Keralty de Sanitas en noviembre de 2022, ha publicado más información confidencial de la Entidad Promotora de Salud (EPS). Aunque no es la primera vez que esto ocurre, esta vez los hackers publicaron la mitad de los archivos secuestrados debido a que la EPS no pagó el rescate. Ransomhouse hizo esta determinación pública a través de su canal de Telegram. Sanitas no ha emitido un comunicado oficial para dar más detalles sobre lo sucedido. En noviembre de 2022, varias empresas, incluyendo Sanitas, informaron de un ciberataque. Keralty, que alojaba los datos de Sanitas, publicó un comunicado sobre un plan de contingencia para aliviar las afectaciones que los cinco millones de usuarios estaban experimentando. La entidad confirmó que se podía acceder al portal web para solicitar citas médicas, pero el grupo de ciberdelincuentes ya tenía en su poder información importante de usuarios y colaboradores de la entidad, y sigue pidiendo una gran suma de dinero para no revelarla. Entre las publicaciones de Ransomhouse, hay archivos con información personal de pacientes, funcionarios de la EPS y proveedores, así como historias clínicas.

La Superintendencia Nacional de Salud hizo comentarios sobre el asunto.

Durante el tiempo en que la EPS Sanitas se encontraba en estado de contingencia después de un ciberataque que afectó su capacidad para brindar servicios, la Superintendencia de Salud expresó su preocupación. A finales de 2022, la entidad de vigilancia y control respondió a las solicitudes de la EPS y otorgó plazos para la

[8] Infobae. Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS [en línea]. 14 de marzo de 2023. [Consultado el 9 de abril de 2023]. Disponible en: https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/

presentación de informes y la supervisión de las quejas recibidas durante la contingencia.

La propia EPS confirmó que la información personal de 241.589 usuarios había sido vulnerada, por lo que la Superintendencia señaló que era necesario que Sanitas informara oportunamente y de manera completa a cada uno de los afectados por esta situación específica.

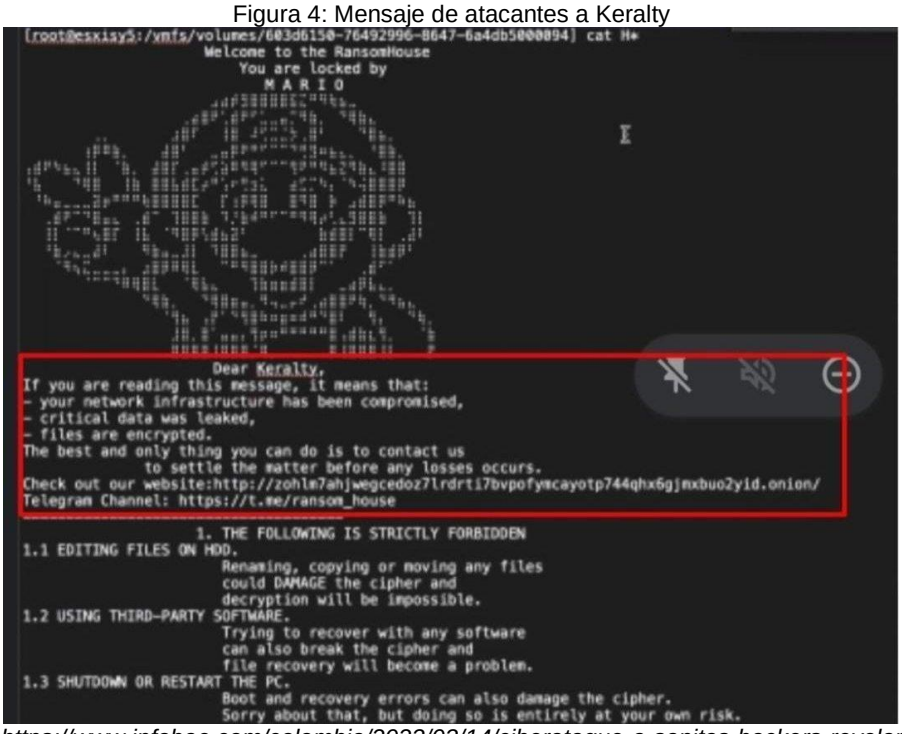
Posibilidad de ransomware

[9]Según el periodista especializado en tecnología, Camilo Andrés García, hay indicios de que el ataque cibernético sufrido por Sanitas podría tratarse de un ransomware. García presentó una captura de pantalla que aparentemente no ha sido editada digitalmente y que demuestra que los ciberdelincuentes habrían secuestrado ciertos datos de Sanitas y ahora exigen un pago de rescate para que sean desbloqueados. El ransomware es una forma de extorsión digital cada vez más común.

En la figura 1 se puede evidenciar el mensaje que le notificaba a KERALTY que su infraestructura fue comprometida con Ransomware.

[9] BENITO Luis. Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS. [en línea].14 de marzo de 2023. [Consultado el 6 de noviembre de 2023]. Disponible en: https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/

Figura 4: Mensaje de atacantes a Keralty



Fuente: *https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/*

Fuerte competencia por el talento para seguridad digital en el 2023

Otro aspecto importante para tener en cuenta es lo que se viene para el 2023, si bien, ya tenemos un panorama de la actualidad en cuanto a ciberseguridad, es fundamental contemplar las habilidades del personal que conforman el área de seguridad digital, daremos un breve vistazo del futuro de la seguridad digital y lo que deberían hacer las organizaciones para hacerse con el mejor talento.

[10]La escasez de talento en ciberseguridad es una realidad, esto no es una novedad, ha sido una problemática con varios años de antigüedad, en el año 2013, solo un

[10] CHANAGA Jaime. ACIS – Asociación colombiana de ingenieros de sistemas: La competencia por el talento en ciberseguridad en el 2023. [en línea]. Octubre de 2022. [Consultado el 30, octubre, 2022]. Disponible en Internet: https://acis.org.co/portal/content/la-competencia-por-el-talento-en-ciberseguridad-en-el-2023

4% lograron encontrar personal capacitado para este rol, para el 2017 la cifra se elevó a un 30% y finalmente para el 2022 el incremento de profesionales en este ámbito fue de 60%, se ve un crecimiento significativo en la última década, sin embargo, la demanda de estos profesionales se ha incrementado al punto de superar la oferta.

De acuerdo con el [11]informe sobre la fuerza laboral en ciberseguridad del año 2021, la fuerza disponible para la seguridad digital debe incrementarse en al menos el 65% para defender o contener con eficiencia los ataques a organizaciones, entre el Caribe y América Latina se requieren al menos 701.000 profesionales en este campo para reducir la brecha.

Los factores a destacar en esta demanda se deben principalmente al cambio de ritmo de esta área, teniendo en cuenta las nuevas modalidades de trabajo (Teletrabajo) y las buenas prácticas de seguridad que evolucionan muy rápidamente, incluso algunos profesionales con cierto recorrido, les cuesta trabajo mantenerse actualizados con estas constantes actualizaciones.

Lo que deberían hacer las organizaciones para hacerse con el mejor talento

Aparte de ofrecer unos salarios acordes o superiores al promedio, algunas tácticas clave son:

Enfocarse en el crecimiento profesional: brindar oportunidades de crecimiento profesional tanto académicamente como laboralmente ayuda a atraer y mantener el personal con el que se cuente en el momento.

[11] ISC. Inspire a Safe and Secure Cyber World: Cybersecurity Workforce Study Sheds New Light on Global Talent Demand Amid a Lingering Pandemic. [Consultado el 30 de octubre de 2022]. Disponible en Internet: https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand

Favorecer la armonía entre la vida personal y la laboral: Mantener y proponer horarios flexibles combinando opciones de trabajo remoto, hace sumamente atractivo el cargo ofertado por una organización, teniendo en cuenta que estas actividades de seguridad digital se pueden ejecutar y coordinar de manera remota.

Inversión en la certificación de empleados: Este aspecto es favorable tanto para la organización como para el profesional, porque mantiene actualizado sus conocimientos y la organización puede disfrutar de este conocimiento en la aseguranza de sus activos o de sus clientes.

Dar importancia al bienestar del profesional: Ofrecer beneficios de salud y generar una cultura de bienestar motiva a la llegada de nuevos profesionales y mantener los que ya hacen parte de la organización, dado el efecto de escasez de profesionales en ciberseguridad, los que ya conforman los grupos de trabajo de las organizaciones, se encuentran con una sobrecarga laboral muy alta que les genera estrés y algunas otras complicaciones de salud.

La escasez de este tipo de profesionales es una situación que va en aumento y que solamente empeorara conforme pase el tiempo, las organizaciones deben asegurarse de crear estas condiciones mencionadas para que sean lugares de trabajo más atractivos para los nuevos talentos y agradable para el personal antiguo.

5.2 EXAMINAR LOS FRAMEWORKS, METODOLOGÍAS, ESTANDARES DE CIBERSEGURIDAD VALIDANDO SUS VENTAJAS Y DESVENTAJAS COMO UNA GUÍA PRACTICA DE APOYO A LAS INDUSTRIAS.

La ciberseguridad se ha convertido en un aspecto crítico en el entorno empresarial y, en particular, en el sector industrial. Con el avance constante de las tecnologías

de la información y la interconexión de sistemas, las organizaciones enfrentan amenazas cada vez más sofisticadas que pueden comprometer la integridad, confidencialidad y disponibilidad de sus activos digitales.

Ante este panorama, contar con un marco de referencia sólido y metodologías adecuadas se vuelve fundamental para establecer una postura de seguridad cibernética efectiva. En este contexto, tres enfoques ampliamente reconocidos y utilizados son el NIST (National Institute of Standards and Technology), COBIT (Control Objectives for Information and Related Technologies) e ISO 27001.

El NIST ha desarrollado una serie de documentos y estándares ampliamente aceptados y utilizados en todo el mundo, como el NIST Cybersecurity Framework. Este marco de trabajo ofrece una estructura y guía práctica para que las organizaciones puedan gestionar y mejorar su ciberseguridad. Además, proporciona un enfoque basado en el riesgo que permite adaptarse a las necesidades y características específicas de cada industria.

Por otro lado, COBIT se centra en la gobernanza y gestión de tecnología de la información. Proporciona un conjunto de objetivos y controles que permiten a las organizaciones garantizar un gobierno efectivo de la seguridad informática. COBIT se basa en un enfoque de proceso y se alinea con otros marcos y estándares internacionales, lo que lo convierte en una valiosa herramienta para la gestión integral de la ciberseguridad.

Otro marco ampliamente utilizado es la norma ISO 27001, que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). ISO 27001 proporciona un enfoque estructurado y sistemático para identificar, evaluar y gestionar los riesgos de seguridad de la información. Al cumplir con esta norma, las organizaciones pueden demostrar su compromiso con la seguridad de la

información y establecer un marco de trabajo para mejorar continuamente su postura de ciberseguridad.

En este trabajo, se realizará un examen detallado de los tres enfoques mencionados: NIST, COBIT e ISO 27001. Se analizarán sus ventajas y desventajas como guías prácticas de apoyo a las industrias en la implementación de medidas de ciberseguridad efectivas. Además, se evaluará su aplicabilidad en diferentes contextos y se proporcionarán recomendaciones para maximizar su eficacia en el sector industrial.

A través de este estudio comparativo, se busca proporcionar una visión completa de los marcos de referencia y metodologías disponibles, brindando a las organizaciones del sector industrial una base sólida para tomar decisiones informadas y estratégicas en materia de ciberseguridad. La comprensión de las características y beneficios de cada enfoque permitirá a las industrias mejorar su capacidad para prevenir, detectar y responder a las amenazas cibernéticas en constante evolución.

5.2.1 12METODOLOGIA NIST. El Instituto Nacional de Estándares y Tecnología (NIST) es una entidad gubernamental de los Estados Unidos que se enfoca en generar sabiduría, crear herramientas y brindar oportunidades educativas en diversas disciplinas, como química, energía y seguridad informática en la era moderna. Sus guías y marcos de referencia para la seguridad de software y hardware se han convertido en normas globales, por eso NIST tiene un papel muy importante para las organizaciones y expertos en ciberseguridad debido a su base de conocimiento.

[12] NIST. About NIST. [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://www.nist.gov/about-nist

¿Cuál es la definición de guías del NIST?

[13]NIST tiene una serie de guías que proporcionan un compendio de buenas prácticas en diferentes campos de la seguridad digital, desde la gestión de riesgos hasta la gobernanza de la ciberseguridad, incluyendo pruebas de penetración y gestión de incidentes. La literatura del NIST en ciberseguridad es muy amplia, con cientos de documentos que conforman un estándar global reconocido. Aunque estas guías no abordan cuestiones técnicas específicas, son esenciales como base metodológica y se actualizan constantemente. Las guías ofrecen una visión global y establecen recomendaciones genéricas para llevar a cabo diferentes procedimientos, como las pruebas de intrusión. Tres guías NIST importantes son la 800-115, 800-94 y 800-61.

5.2.1.1 La Guía Técnica NIST 800-115 enfocada en la evaluación y prueba de seguridad de la información, proporcionando directrices y recomendaciones en este ámbito. La primera guía NIST ofrece una base metodológica para implementar servicios avanzados de prueba de intrusión o Pentesting. Aunque no se centra en aspectos técnicos específicos, es esencial porque establece las fases y revisa las características de las diferentes técnicas utilizadas para evaluar la seguridad de la información. Sirve como guía general en el proceso para desarrollar y planificar metodologías específicas adaptadas a los sistemas y objetivos establecidos. El documento examina las diversas técnicas y fases necesarias para realizar una evaluación de seguridad.

[13] Un abordaje integral de la Ciberseguridad. 2019. [Consultado el 6 de noviembre de 2023]. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

¿Cuáles son las técnicas de revisión?

Este artículo aborda técnicas de revisión pasiva que resultan fundamentales para identificar vulnerabilidades de seguridad y recopilar datos para el desarrollo de enfoques avanzados de intrusión. Estas técnicas minimizan el riesgo para las redes y sistemas evaluados. La guía del NIST resalta varias estrategias de revisión, como la evaluación de documentación, registros, conjuntos de reglas y configuraciones de sistemas, además de la exploración de redes y la verificación de la integridad de archivos. La revisión de documentación analiza los procedimientos y las políticas desde una visión técnica. La revisión de registros verifica si los controles de seguridad implementados están registrando información suficiente y detallada. La revisión de conjuntos de reglas identifica deficiencias en los controles de seguridad. La evaluación de las configuraciones de sistemas analiza la adecuada aplicación de configuraciones fuertes en dichos sistemas. El escaneo de la red controla el flujo de datos en la red para obtener datos e inspeccionar la encriptación de las comunicaciones. Por último, la verificación de archivos debe buscar que estén íntegros para identificar que archivos cruciales no hayan sido alterados.

Métodos para reconocer y examinar objetivos

Este artículo describe cómo los analistas de ciberseguridad utilizan técnicas para identificar dispositivos activos en una red, así como sus puertos y servicios asociados. El objetivo es detectar posibles vulnerabilidades en dichos dispositivos. La información recopilada mediante estas técnicas es utilizada para planificar y aplicar técnicas de validación de vulnerabilidades, como actividades de tipo Pentesting o pruebas de penetración avanzadas. NIST ha destacado específicamente cuatro técnicas para identificar y analizar los sistemas a evaluar: Detección de red, reconocimiento de puertos y servicios, escaneo de vulnerabilidades e inspección inalámbrica.

La técnica de descubrimiento de la red se utiliza para identificar los dispositivos en la red, determinar cómo se comunican entre sí y proporcionar una visión general de la arquitectura de la red. La identificación de puertos de red, servicios y detalles relacionados con ellos también es importante para la detección de vulnerabilidades.

El escaneo de vulnerabilidades implica diferentes técnicas para analizar vulnerabilidades en sistemas y servicios, utilizando herramientas automatizadas o manuales.

Por último, **el escaneo inalámbrico** se utiliza para identificar equipos inalámbricos no permitidos, descubrir señales inalámbricas más allá de los límites de la entidad y posibles accesos ocultos que podrían ser aprovechados por agentes malintencionados.

Técnicas para comprobar la vulnerabilidad del objetivo

En este apartado se explica que la guía del NIST establece que los métodos para verificar las vulnerabilidades del objetivo utilizan la información recopilada durante el reconocimiento y análisis del objetivo para evaluar de manera exhaustiva la posible presencia de vulnerabilidades. Estos mecanismos ayudan a confirmar la existencia de vulnerabilidades y lo que sucede cuando son aprovechadas por ciber atacantes. Es por ello que estos métodos pueden tener un impacto mayor sobre la red o el sistema que esta bajo evaluación que las técnicas anteriores. Las técnicas de validación de la vulnerabilidad del objetivo incluyen la vulneración de contraseñas, los tipos de ingeniería social como el Pentesting y correos falsos, según establece la guía del NIST.

Pruebas de intrusión o Pentesting

En este punto se explica en detalle las fases y acciones necesarias para llevar a cabo pruebas de intrusión, las cuales se utilizan para validar la vulnerabilidad del objetivo:

La planificación es el primer paso, en el cual se establecen los objetivos y se prepara el entorno técnico para realizar la prueba.

La fase de descubrimiento consiste en recopilar información para identificar posibles vulnerabilidades.

La fase de ejecución es la fase clave del proceso, durante la cual se realizan acciones de ataque, como obtener acceso y escalar privilegios, moverse lateralmente en la infraestructura, instalar herramientas adicionales y documentar todo el proceso.

La publicación del NIST 800-115 enumera las vulnerabilidades más comunes que se explotan en las pruebas de intrusión, como configuraciones incorrectas, fallos en el kernel, desbordamiento de buffer y privilegios erróneos en carpetas y archivos.

Estudio de seguridad

NIST en su guía, presenta un par de secciones que tratan sobre la evaluación de seguridad de la información, una enfocada en la planificación y otra en la ejecución. Es importante considerar la organización, los sistemas y las técnicas que se utilizarán. En la fase de planificación, se deben desarrollar políticas de evaluación, priorizar y programar las evaluaciones, seleccionar técnicas personalizadas, definir aspectos logísticos, desarrollar el plan y considerar los aspectos legales. En cuanto

a la fase de ejecución, se compone de coordinación, evaluación, análisis y gestión de datos.

5.2.1.2 Prevención y detección de intrusos en sistemas: guía práctica NIST 800-94. La segunda guía de NIST se enfoca en los programas de prevención y detección de intrusos (IDS/IPS), los cuales automatizan la detección de intrusiones.

Principales IDS/IPS

[14]El NIST ha publicado una guía en la que se establecen consejos prácticos para planificar, ejecutar, ajustar, asegurar, vigilar y preservar cuatro categorías de IDS/IPS. Estos sistemas son: **Estructurado en la red (NIDS/NIPS), Evaluación de red inalámbrica (WIDS/WIPS), Análisis del comportamiento de la red (NBA) y Basado en el host (HIDS/HIPS).** La guía incluye un texto introductorio a los conceptos clave sobre la prevención y detección de intrusos, una óptica global de los componentes más comunes de este tipo de tecnologías, mecanismos típicos para detectar intrusos y consejos de como operar e implementar. Además, la guía se enfoca en el análisis de cada tecnología IDS/IPS, describiendo sus componentes y arquitectura, sus capacidades de seguridad y su gestión. De este modo, la guía proporciona una base metodológica para que las organizaciones puedan estructurar y ejecutar sistemas IDS/IPS seguros que ayuden a identificar intrusos.

Combinación de mecanismos IDS/IPS

A continuación se mencionan los cuatro tipos principales de tecnologías IDS/IPS (NIPS, WIPS, NBA y HIPS) que existen y cómo difieren entre sí en términos de la detección de intrusiones, precisión y análisis profundo sin afectar el rendimiento del

[14] CONCHA Felipe. Sistemas IDS, IPS, HIDS, NIPS, SIEM ¿Qué son? [en línea]. 12 de febrero de 2019. [Consultado el 6 de noviembre de 2023]. Disponible en: https://www.a2secure.com/blog/ids-ips-hids-nips-siem-que-es-esto/

sistema. La guía NIST recomienda el uso de varias tecnologías IDS/IPS al mismo tiempo para una detección y prevención más completa de ataques maliciosos.

La guía aconseja una mezcla de tecnologías IDS/IPS basadas en redes y en los hosts, y sistemas de evaluación inalámbrica si se necesitan supervisar redes inalámbricas. La tecnología NBA (Análisis de comportamiento de la red) es útil para la seguridad adicional para afrontar ataques de tipo Malware.

La unión de varios sistemas IDS/IPS podría ser de manera directa o de manera indirecta. La manera directa se utiliza cuando se emplean tecnologías IDS/IPS del mismo proveedor y la manera indirecta se lleva a cabo con una herramienta de gestión de eventos y datos de seguridad (SIEM) para correlacionar los diferentes eventos que fueron registrados por los sistemas involucrados.

Además de las tecnologías IDS/IPS principales, existen otras herramientas para hacer análisis forense en la red, sistemas antimalware y Firewall que pueden complementar la seguridad de la organización. La guía NIST no incluye aún los sistemas EDR/xEDR en sus publicaciones, pero se espera que sean contemplados en el futuro como sistemas de defensa adicionales.

5.2.1.3 Manual para administrar incidencias de ciberseguridad NIST 800-61. La adecuada administración de situaciones problemáticas es fundamental en el ámbito de la protección de datos y sistemas informáticos. No es suficiente realizar pruebas preventivas o tener sistemas automáticos para detectar intrusos, sino que es importante tener herramientas adecuadas para manejar cualquier incidente que pudiera ocurrir. El NIST ha desarrollado una guía para ayudar a los equipos de respuesta, administradores de sistemas, expertos en seguridad y otros profesionales relacionados a gestionar eficazmente incidentes de ciberseguridad. La guía se divide en tres temas principales: plan de respuesta, gestión y coordinación de incidentes.

Planes de respuesta

NIST en sus guías, proporcionan recomendaciones sobre cómo diseñar las políticas y los planes de respuesta para abordar temas de ciberseguridad. Estas pautas cubren aspectos como la jerarquía, los servicios y el personal de los grupos de respuesta de las entidades. Las sugerencias incluyen la necesidad de establecer un plan formal de respuesta ante incidentes, diseñar una política que defina los eventos considerados como incidentes y las funciones de cada miembro del grupo, y elaborar un plan de respuesta claro con objetivos y métricas. También es importante establecer procedimientos detallados para cada fase del proceso, incluyendo el intercambio de información y la selección de profesionales con habilidades técnicas, de comunicación y pensamiento crítico. Además, es recomendable nombrar otros equipos en la entidad que deberían colaborar en la gestión de incidentes, así como establecer el catálogo de servicios que cubra otros aspectos más profundos que simplemente la respuesta a incidentes, como el monitoreo de tecnologías para detectar intrusos o la formación en ciberseguridad del personal.

Gestión de incidentes

La guía del NIST proporciona una estructura para la gestión de incidentes que consta de cuatro fases principales: planificación, identificación y examen, control, eliminación y restauración., y ejercicios posteriores al incidente. Cada fase está interrelacionada y no sigue una progresión lineal, sino más bien circular. La evaluación realizada después de ocurrido el incidente es crucial para preparar mejor la organización. La guía ofrece recomendaciones para la gestión de incidentes, como la utilización de herramientas y software adecuados, la evaluación continua de riesgos, la detección de indicios de incidentes a través de herramientas de

seguridad, el establecimiento de metodologías para que actores ajenos a la entidad notifiquen sobre incidentes, y la creación de una directiva para registrar información acerca de incidentes. Además, es importante establecer estrategias para priorizar la gestión de incidentes y contenerlos rápidamente y de manera eficaz.

Colaboración e intercambio de datos entre diferentes partes

La guía NIST se enfoca en cómo los grupos dentro en la entidad se coordinan para proporcionar respuestas congruentes a los incidentes reportados y en los mecanismos utilizados para documentar esa información. En sus sugerencias, se incluyen la planificación previa de la gestión de incidentes con terceros, otros grupos de respuesta a incidentes, autoridades o proveedores, y el intercambio de información acerca de incidentes durante su ciclo. También se aconseja automatizar el intercambio de información y evaluar de manera precisa las ventajas y dificultades que pueden surgir a raíz de compartir información confidencial con otras partes, compartiendo toda la información que sea posible con otras entidades mientras se consideran los intereses y las razones de seguridad de la organización. Además, se recomienda tener una consultoría frecuente del equipo legal para asegurar que todas las actividades que se coordinan se están ejecutando dentro del marco normativo.

En resumen:

En este numeral hemos señalado que las guías NIST, proporcionan metodologías generales para el diseño, la planificación e implementación de diferentes estrategias o procedimientos en ciberseguridad. A diferencia de otras guías, estas recomendaciones no se aplican directamente a sistemas o aplicaciones específicos, sino que sirven como un procedimiento estandarizado al que los profesionales pueden adherirse.

La utilización de las guías NIST proporciona garantía en las acciones que se ejecutan, ya que se convierte en un requisito metodológico. Además, muchas regulaciones exigen que las prácticas de ciberseguridad estén respaldadas por una metodología específica, como la que ofrece el NIST.

Las empresas proveedoras de servicios de ciberseguridad que cumplen con las metodologías del NIST aumentan la protección y simplifican el seguimiento de las normativas para las entidades y organizaciones que adquieren sus prestaciones.

En resumen, la gran cantidad de documentación producida por el NIST proporciona un marco metodológico estándar reconocido y utilizado a nivel mundial para la prevención, detección y resolución de vulnerabilidades.

5.2.2 [15]ISO 27001 – SEGURIDAD DE LA INFORMACIÓN. La norma ISO 27001 es un estándar internacional establecida por la Organización Internacional de Normalización (ISO) con el propósito de dar pautas sobre buenas prácticas de seguridad de la información. Esta norma proporciona herramientas útiles que ayudan a las organizaciones a gestionar la información de forma segura y confiable. La norma ISO 27001 propone un patrón uniforme para las entidades, permitiéndoles crear, ejecutar, supervisar, evaluar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). Su primera versión fue publicada en 2005, enfocándose en la norma británica BS 7799-2, mientras que en 2013 se actualizó para adaptarse a las nuevas tecnologías del mercado y basarse en otras normas y directrices de seguridad de la información. Este estándar es aplicable a cualquier tipo de empresa, independientemente de su tamaño o actividad.

[15] PIRANI. ISO 27001: de qué se trata y cómo implementarla. [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

¿Cuál es la importancia de esta norma?

Como se ha mencionado anteriormente, las empresas pueden ser víctimas de diferentes tipos de delitos informáticos que comprometen su información, lo cual puede dañar su reputación. Estos delitos son perpetrados por ingenieros, piratas informáticos, colaboradores o grupos dedicados al robo de información. Por tal razón, es crucial contar con soluciones que puedan prevenir estos incidentes. Un Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental para cumplir con los requisitos legales, ya que en muchos países es una exigencia. La norma ISO 27001 proporciona la metodología necesaria para implementar un SGSI y cumplir con los requisitos legales. Lograr una certificación en ISO 27001 aporta más valor a la empresa en comparación con sus competidores e incrementa el nivel de confianza entre los clientes y posibles clientes futuros. Asimismo, minimiza la probabilidad de ocurrencia de incidentes que puedan generar enormes pérdidas económicas, evitando así efectos secundarios perjudiciales y ahorrando dinero.

¿Qué es y para qué sirve un SGSI (Sistema de gestión de seguridad de la información)?

La norma ISO 27001 se basa en el Sistema de Gestión de Seguridad de la Información (SGSI), que tiene como objetivo la preservación de la confidencialidad, integridad y disponibilidad de la información. Para lograr esto, se ejecuta un análisis y evaluación de activos de información, lo que permite documentar el proceso para que toda la organización pueda conocer y actuar adecuadamente ante posibles amenazas.

La información es un activo importante para las empresas, y un SGSI es una herramienta esencial para protegerla y cumplir con la reglamentación y protección de datos vigente. Establecer políticas y controles adecuados permite mantener la

seguridad de la información, conocer los riesgos que la empresa puede enfrentar y saber cómo mitigarlos.

¿Qué elementos están incluidos en un SGSI?

La norma ISO 27001 establece que un Sistema de Gestión de Seguridad de la Información debe contener los siguientes componentes:

1. Manual de seguridad: Este manual presenta las directrices para la ejecución y supervisión del Sistema de Gestión de Seguridad de la Información, abarcando aspectos como metas, alcance, obligaciones, directivas y demás tareas realizadas.

2. Procedimientos: Estos definen las pautas a seguir para asegurar que la administración sea efectiva y que se alcance una planificación, ejecución y supervisión adecuadas en los procedimientos relativos a la seguridad de la información.

3. Instrucciones: Estas detallan de manera secuencial las labores y acciones que deben ejecutarse con el fin de lograr una administración efectiva.

4. Registros: Estos constituyen el registro tangible de los datos producidos durante la administración, utilizados para confirmar el cumplimiento de las metas previamente fijadas.

5. [16]Anexo A: El Anexo A de la norma ISO/IEC 27001 presenta una serie de prácticas o acciones que las organizaciones deberían considerar para enfrentar

[16] EEE Escuela Europea de Excelencia. Controles del Anexo A de ISO 27001: guía completa actualizada a la versión de 2022. [en línea]. 23 de marzo de 2023. [Consultado el 6 de noviembre de 2023]. Disponible en: https://www.escuelaeuropeaexcelencia.com/2023/03/controles-del-anexo-a-de-iso-27001-guia-completa-actualizada-a-la-version-de-2022/

amenazas de seguridad de la información. No obstante, no todos estos controles son mandatorios. La organización solo debe implementar aquellos que considere pertinentes según los riesgos identificados, su magnitud y la probabilidad de que sucedan.

Aspectos para tener en cuenta al implementar un SGSI

Aquí se presentan de manera resumida los pasos necesarios para la implementación de un Sistema de Gestión de Seguridad de la Información:

1. Definir la política de seguridad: Esto involucra definir los propósitos, el contexto general, las obligaciones legales, los estándares para valorar riesgos y el enfoque avalado por los lideres o la junta directiva.

2. Definir el alcance del SGSI: Es fundamental considerar los recursos, las tecnologías y una descripción para cada activo.

3. Identificar los riesgos: Reconocer las posibles amenazas, los responsables directos, las vulnerabilidades y el impacto en caso de violación de la confidencialidad, integridad y disponibilidad de los activos de información.

4. Analizar y evaluar los riesgos: Hacer evaluación del impacto, identificar la probabilidad de ocurrencia, verificar si se puede aceptar o mitigar el riesgo.

5. Tratamiento de riesgos: Implementar las medidas de control apropiadas, categorizar los niveles de riesgo, prevenirlos o delegarlos a terceros en caso de ser viable.

6. Declarar la aplicabilidad: Definir los propósitos de regulación y elegir las medidas de control que serán aplicadas teniendo en cuenta los 114 controles del Anexo A contenidos en la norma.

7. Realizar la gestión: Establecer la gestión de los riesgos, ejecutar el enfoque considerando los controles señalados, implantar los controles, especificar el sistema de medición, promover la concienciación y cultivar una mentalidad en la que todos los colaboradores estén informados sobre el SGSI, adicionalmente, manejar su funcionamiento y emplear los recursos requeridos para cumplirlo.

8. Monitorear: Realizar evaluaciones regulares del SGSI con el fin de determinar si se ajusta a los estándares ISO 27001 y a los objetivos establecidos, comunicar las mejoras detectadas y determinar las medidas que se deben implementar. A través del módulo de seguridad de la información de Pirani, puedes analizar de manera sencilla y eficiente las diversas amenazas.

Esta es una lista que resume todas las actividades que debes considerar:

- Obtener el respaldo de los líderes empresariales, directivos y la junta directiva.
- Definir la metodología a implementar.
- Establecer un alcance para el Sistema de Gestión de Seguridad de la Información (SGSI).
- Construir una política de seguridad de la información.
- Identificar y evaluar los riesgos.
- Realizar el tratamiento de riesgos para abordar los riesgos identificados.
- Comunicar cómo se aplicará el SGSI.
- Establecer un plan de tratamiento de riesgos claro.
- Definir las métricas para evaluar la efectividad de los controles.

- Implementar controles y procedimientos de acuerdo con las necesidades.
- Fomentar conciencia de seguridad de la información mediante sesiones de capacitación y charlas.
- Hacer seguimiento y medición del SGSI para verificar su efectividad.
- Realizar auditorías internas.
- Implementar mejoras en caso de ser necesario en alguna de las fases.

5.2.3 COBIT (Objetivos de Control para la Tecnología de la Información y las Tecnologías Relacionadas). [17]La importancia de la tecnología y la información en las empresas ha aumentado significativamente debido a la transformación digital. En tiempos anteriores, los ejecutivos de negocios podían pasar por alto o asignar la responsabilidad de las decisiones sobre Información y Tecnología (I&T). Sin embargo, en la época actual, esta actitud no es aconsejable en la mayoría de los campos y sectores.

Las compañías que aspiran a generar valor para sus involucrados, persiguiendo la maximización de ganancias y la reducción de riesgos, deben adaptarse a la digitalización para alcanzar nuevos enfoques de operación, procedimientos más efectivos y lograr éxito en las innovaciones.

En consecuencia, la supervivencia y el crecimiento de las empresas están cada vez más vinculados con la información y la tecnología.

El gobierno de TI es ahora fundamental en el gobierno corporativo y es ejercida desde una junta directiva. Su función es supervisar la creación y puesta en marcha

[17] Ciberseguridad.com. COBIT [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://ciberseguridad.com/normativa/espana/sgsi/cobit/

de procedimientos, sistemas y enlaces dentro de la empresa para respaldar tanto a los trabajadores en áreas empresariales como en tecnología de la información, con el propósito de alcanzar los fines corporativos y generar valor en términos comerciales.

COBIT es un marco para gobierno de TI y gestión completo y amplio que tuvo origen en la comunidad de auditoría de TI y se convirtió en recurso esencial para las empresas que buscan mejorar su gobierno de TI y gestión de información y la tecnología.

Definición de COBIT

El marco COBIT se utiliza para gestionar la información y la tecnología, también para gobernanza empresarial, y puede ser implementada en cualquier tipo de organización. Se caracteriza a la información y tecnología (I&T) como el conjunto de tecnologías y procesamiento de datos que la organización emplea con el propósito de lograr sus metas, independientemente del área de la organización en el que se implemente. Dicho de otra manera, la I&T organizacional va más allá del área de TI de una empresa, aunque sí este incluido.

En el marco COBIT se hace una clara distinción entre la gestión y la gobernanza. Estas categorías requieren diferentes unidades organizativas, ya que se usan para propósitos distintos y están compuestas por diferentes actividades.

La gobernanza pretende garantizar:

- La valoración de las situaciones, requisitos y elecciones de las partes involucradas, con el propósito de definir metas empresariales claras y mutuamente acordadas.

- La dirección establecida mediante una toma de decisiones y la asignación de prioridades.

- La supervisión del acatamiento y el rendimiento en consonancia con los objetivos establecidos.

En la mayoría de las compañías, el consejo de administración asume la responsabilidad de la dirección general, bajo la guía del presidente. En estructuras organizativas específicas, especialmente en empresas de mayor envergadura y complejidad, es posible asignar tareas concretas de gobernanza a instancias especializadas.

Mediante una adecuada gestión, se planifican, construyen, ejecutan y supervisan las acciones relacionadas con la gestión de información y tecnología que persiguen alcanzar los propósitos empresariales.

COBIT detalla los componentes esenciales para establecer y conservar un sistema de gobernanza, que abarca estructuras organizativas, aptitudes y recursos, procedimientos y políticas, cultura y conductas, así como la fluidez de la información.

Además, establece los elementos de diseño que la organización debe tener en cuenta al edificar un sistema de gobernanza más alineado con sus metas.

Cuáles son las características y principios de COBIT 5

La rápida evolución de las tecnologías y la informática ha llevado a la aparición de sistemas nuevos y formas de ofrecer servicios no considerados en COBIT 5. Actualmente, gestionar la información es fundamental para el proceso de

digitalización de una empresa, lo que ha dado lugar a un nuevo marco de referencia denominado "Gobierno de la Información y Tecnología de las Empresas". A diferencia de "TI", que se refiere al departamento de tecnología de una empresa, "I&T" abarca el total de información recopilada, procesada y utilizada por la organización para alcanzar sus metas, así como el tipo de tecnología utilizada para tal fin. COBIT 2019, destaca la importancia crítica de la tecnología y la información organizacional.

COBIT 2019 en particular, indica seis bases esenciales que cualquier sistema de gobernanza debe considerar para la administración de la tecnología y la información. Además, señala tres principios más para un gobierno de TI que podría ser usado para la construcción de un sistema de gobierno.

Recomendaciones para implementar COBIT en la industria colombiana

[18]A continuación se presentan una serie de pasos basados en el marco COBIT 2019 que servirán como guía durante el proceso de adaptación a la era digital:

1. Formación de un equipo / comité de transformación digital: Conformado por altos directivos o ejecutivos de nivel superior.

2. Elección de factores de diseño pertinentes: Consideración de la estrategia y metas empresariales, perfil de riesgo, rol de TI, estrategia de adopción tecnológica y tamaño de la empresa.

3. Identificación de áreas de enfoque relevantes: Por ejemplo, transformación digital o ciberseguridad.

[18] ISACA. Cynthus. Transformación digital con COBIT 2019. [en línea]. 10 de febrero de 2020. [Consultado 20 de agosto de 2023]. Disponible en: https://www.cynthus.com.mx/transformacion-digital-con-cobit-2019/

4. Aplicación de una cascada de objetivos: Las necesidades de las partes interesadas deben convertirse en una estrategia empresarial que se pueda implementar.

5. Creación de un modelo de gobernanza personalizado: Un sistema de gobierno adecuado en tamaño y forma... ajustado a la organización.

6. Priorización de objetivos de gobernanza y gestión: Esto se realiza en función de los objetivos seleccionados en el paso 4.

7. Selección de componentes del modelo de gobernanza aplicables.

8. Desarrollo de un plan de camino a la transformación digital: Este itinerario debe ser integral, garantizando la inclusión de todos los objetivos prioritarios de gobierno y gestión. Documentar y comunicar el plan es esencial para mantener la alineación y prevenir malentendidos entre todas las partes involucradas.

9. Preparación activa para la transformación: En este paso crucial, una matriz que evalúe el nivel de madurez de las capacidades ayudará a identificar factores y acciones clave. Las partes interesadas deben ser realistas y evitar excesivas ambiciones, sin perder de vista el verdadero alcance de la transformación.

10. Ejecución y administración de la transformación: En esta etapa, las partes interesadas comenzarán a implementar o ejecutar la estrategia diseñada.

La figura 2 representa la estrategia que propone el marco de trabajo COBIT 2019 para la transformación digital de las organizaciones y gestionar riesgos asociados a los cambios tecnológicos:

Figura 5. Estrategia de transformación digital COBIT 2019

Fuente: https://www.cynthus.com.mx/transformacion-digital-con-cobit-2019/

En cuanto al sistema de gobierno, estos son los principios que se establecen:

- Se requiere un gobierno de TI en la organización para agregar más valor mediante el uso de tecnologías de la información, también para cumplir con los requerimientos de las partes interesadas.

- El sistema de gobernanza se conforma por diversos componentes que operan de manera colaborativa y holística.

- Se requiere que el sistema de gobernanza sea adaptable y que cualquier alteración en los elementos de diseño sea considerada en relación con el impacto en la totalidad del sistema.

- El sistema de gobernanza debe distinguir claramente las acciones y las configuraciones de administración y gobernanza.

- El sistema de gobernanza debe ajustarse a los requerimientos de la organización, otorgando prioridad y adaptación a sus componentes considerando ciertos aspectos de diseño.

- El sistema de gobernanza no debe limitarse exclusivamente al entorno de TI, sino que debe cubrir la totalidad de la organización, incorporando tanto el manejo de información como la tecnología empleada.

En cuanto a los orígenes del marco de gobierno, tenemos los siguientes:

- Automatización y coherencia: la estructura de gobernanza debe fundamentarse en un enfoque conceptual que identifique los componentes esenciales y las interacciones entre ellos.

- Adaptabilidad y apertura: la estructura de gobernanza debe permitir la inclusión de nuevos contenidos y abordar nuevos desafíos de manera versátil.

- Alineación con las normativas y estándares más prominentes.

¿Cuáles son las ventajas de una implementación de COBIT 2019?

COBIT (Control Objectives for Information and related Technology) es un conjunto de principios y prácticas para administrar y gobernar las tecnologías de la información y de la empresa. La última versión de este marco, COBIT 2019, ha sido desarrollada por ISACA (Information Systems Audit and Control Association), una organización que se enfoca en crear metodologías y certificaciones para auditoría y control de sistemas de información.

COBIT 2019 tiene varios beneficios importantes. En primer lugar, ayuda a alinear los objetivos de TI con los objetivos del negocio, lo que mejora la integración comercial y de TI. Los expertos en COBIT tienen la capacidad de instaurar medidas y recursos que colaboren con los directivos de tecnologías de la información para lograr los resultados empresariales previstos. Por ejemplo, el esquema de madurez de COBIT define el nivel de desempeño que los componentes de TI deben alcanzar para satisfacer las metas organizacionales.

En segundo término, COBIT 2019 optimiza la gestión de desempeño. La Gestión del Desempeño (CPM) posibilita la evaluación del desempeño en distintas secciones del marco de trabajo y calificarlas para identificar lo que es efectivo y eliminar procedimientos redundantes.

En tercer lugar, COBIT 2019 aumenta la confianza y el valor en los sistemas de información corporativos. Faculta a las entidades a optimizar sus inversiones en tecnología de la información, al trazar y administrar un plan equilibrado entre la utilización de sus recursos y los riesgos asociados con su implementación. Este enfoque mejora la eficacia y el rendimiento de los sistemas de información sin comprometer los plazos de entrega ni la integridad de los datos.

Finalmente, COBIT 2019 es un marco de código abierto que se actualiza constantemente y se adapta fácilmente a los cambios y actualizaciones del mercado. Además, es compatible con otros frameworks como ITIL y DevOps.

5.2.4 COMPARATIVO ENTRE LOS FRAMEWORKS

En la tabla 2, se presentan las ventajas y desventajas de la ISO 27001, NIST y COBIT con el objetivo de brindar una visión clara de sus características distintivas y como pueden beneficiar a las organizaciones en la gestión de la ciberseguridad y la gobernanza de TI:

Tabla 3. Cuadro comparativo de ventajas y desventajas para los marcos de trabajo

ISO 27001		NIST		COBIT	
Ventajas:	*Desventajas:*	*Ventajas:*	*Desventajas:*	*Ventajas:*	*Desventajas:*
Amplia aceptación global: ISO 27001 es ampliamente reconocida a nivel internacional y es considerada una referencia en la industria de la seguridad de la información. **Enfoque integral:** Proporciona	**Complejidad:** La implementación de ISO 27001 puede ser compleja y requerir un esfuerzo considerable en términos de tiempo y recursos. **Costos:** La certificación y el mantenimiento pueden ser costosos debido a los requisitos de	**Enfoque práctico:** Proporciona directrices prácticas y recomendaciones detalladas para mejorar la ciberseguridad, basadas en el ciclo de vida de gestión de riesgos. **Adaptabilidad:** El marco NIST es flexible y se puede adaptar a diferentes tipos de	**Falta de certificación oficial:** A diferencia de ISO 27001, NIST no ofrece un proceso de certificación formal. **Enfoque más técnico:** Puede requerir cierto nivel de conocimientos técnicos para implementar completamente todas las	**Enfoque integral:** COBIT se enfoca en la gobernanza de TI y brinda una visión holística para la gestión de la tecnología y la información. **Marco de referencia amplio:** Aborda aspectos	**Complejidad:** Al igual que ISO 27001, COBIT puede ser complejo en su implementación y requiere una comprensión sólida de los conceptos de TI y gobernanza. **Enfoque en la gobernanza:** Si una

un enfoque completo para la gestión de la seguridad de la información, abordando aspectos como políticas, procedimientos, controles y auditorías. **Enfoque en el riesgo:** Se centra en la identificación y gestión de riesgos, lo que permite una adaptación más precisa a las necesidades de seguridad de la organización. **Certificación:** La certificación ISO 27001 puede mejorar la	auditoría y conformidad. **Adaptabilidad:** Puede requerir adaptaciones significativas para abordar requisitos específicos de la organización.	organizaciones y riesgos específicos. **Comunidad de apoyo:** NIST es respaldado por una comunidad amplia y diversa de profesionales de la ciberseguridad y la tecnología. **Enfoque en la respuesta a incidentes:** Incluye pautas claras para la preparación y respuesta ante incidentes de ciberseguridad.	recomendaciones.	como la gestión de riesgos, el cumplimiento, la auditoría y el rendimiento. **Alineación con objetivos empresariales:** Ayuda a alinear los objetivos de tecnología de la información con los objetivos de negocio más amplios.	organización busca una orientación más técnica y detallada, COBIT puede no satisfacer todas sus necesidades.

credibilidad de la organización ante clientes y socios al demostrar un compromiso con la seguridad de la información.

Fuente: *Elaboración propia*

5.3 CONTROLES TÉCNICOS MÍNIMOS BASADOS EN MARCOS DE SEGURIDAD VIGENTES PARA EL FORTALECIMIENTO DE LAS ORGANIZACIONES.

Los estándares revisados en el numeral anterior contemplan los mismos controles mínimos para preservar la seguridad en las organizaciones, a continuación se relacionan estos controles técnicos y recomendaciones de implementación:

5.3.1 19Control de acceso. La seguridad se ve sustancialmente fortalecida por medio del control de acceso, dado que determina quiénes están habilitados para ingresar a determinada información, herramientas y recursos, y bajo qué

[19] Microsoft. ¿Qué es el control de acceso? [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control

condiciones se les permite hacerlo. Esta medida guarda similitud con las llaves y las listas de invitados que resguardan lugares físicos, aunque en este contexto, las pautas de control de acceso se aplican a los entornos digitales. Este enfoque garantiza que las personas adecuadas obtengan acceso, mientras que las no autorizadas queden excluidas. Dichas pautas se sustentan en gran medida en la autenticación y la autorización, procesos que posibilitan a las compañías confirmar la identidad de sus usuarios y determinar los niveles de acceso adecuados basados en factores contextuales como el dispositivo, la ubicación y la función desempeñada.

El sistema de acceso controlado evita que personas no autorizadas o intrusos accedan a datos sensible, como información de clientes o propiedad intelectual. Además, disminuye la posibilidad de que los empleados filtren datos de manera no autorizada y reduce las amenazas provenientes de la web. En lugar de gestionar los permisos manualmente, las entidades seguras optan por emplear herramientas para gestionar la identidad y el acceso para aplicar las políticas de control de acceso.

5.3.1.1 Tipos de control de acceso

5.3.1.1.1 Control de acceso discrecional (DAC). es un modelo en el que cada objeto en un sistema protegido tiene un propietario, quien tiene el poder de conceder acceso de usuarios según su criterio. DAC controla los recursos de manera detallada y específica para cada caso.

5.3.1.1.2 Control de Acceso Obligatorio (MAC). Es un modelo en el que los usuarios obtienen acceso a través de una autorización centralizada que establece niveles de acceso uniformes para todos dentro de un ámbito determinado. Este modelo se utiliza comúnmente en contextos gubernamentales y militares.

5.3.1.1.3 [20]Control de Acceso Basado en Roles (RBAC). Los privilegios de acceso se conceden conforme a las responsabilidades laborales definidas, en vez de depender de la identidad o el tiempo de servicio de los individuos. La meta consiste en suministrar a los usuarios únicamente la información requerida para llevar a cabo sus tareas.

5.3.1.1.4 [21]Control de Acceso Basado en Atributos (ABAC). Es el más granular, ya que el acceso se otorga flexiblemente a través de una mezcla de atributos y condiciones ambientales, como su ubicación y hora. ABAC reduce la necesidad de asignar roles específicos a cada usuario.

5.3.1.1.5 [22]Factor de autenticación doble y múltiple. La empleabilidad de contraseñas se utiliza para autentificar a los usuarios en el proceso de verificación de identidad requerido por diversos servicios. Esto garantiza la veracidad de la identidad del usuario y previene la suplantación. Aunque las contraseñas no son el único método para identificar a los usuarios. Examinemos las distintas alternativas:

1. Sistemas basados en conocimientos del usuario. El más común es el uso de contraseñas.

2. Sistemas basados en posesiones del usuario. Esto incluye tarjetas de identidad o coordenadas, así como tokens físicos o virtuales.

[20] MANAGE-ENGINE. Control de acceso basado en roles (RBAC). [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://www.manageengine.com/latam/device-control/control-de-accesos-basado-en-roles.html
[21] AWS. Control de acceso basado en atributos. [en línea].s.f-[Consultado el 6 de noviembre de 2023]. Disponible en: https://docs.aws.amazon.com/es_es/singlesignon/latest/userguide/abac.html
[22] INCIBE. El factor de autenticación doble y múltiple. [en línea]. 27 de febrero de 2019. [Consultado el 6 de noviembre de 2023]. Disponible en: https://www.incibe.es/ciudadania/blog/el-factor-de-autenticacion-doble-y-multiple

3. Sistemas basados en características físicas del usuario, como huellas dactilares, reconocimiento facial o activación por voz.

La primera alternativa es la más popular y ampliamente usada. Crear una cuenta mediante un usuario y contraseña se ha vuelto una actividad rutinaria para la mayoría de los usuarios. Sin embargo, este proceso presenta vulnerabilidades:

1. Relacionadas con la capacidad de los usuarios para crear y recordar cadenas largas de caracteres, así como manejar múltiples contraseñas al mismo tiempo.

2. Relacionadas con las técnicas cada vez más sofisticadas empleadas por ciberdelincuentes, que obtienen nuestras claves con mayor facilidad.

Ahora, ¿qué es la autenticación de doble o múltiple factor? La autenticación doble, también llamada verificación en dos pasos, agrega una capa de seguridad extra junto a las contraseñas. Su propósito es asegurarse de que el usuario no solo conoce la contraseña, sino que también aporta información en el proceso de inicio de sesión, como un código, que solo él posee. Esta información puede obtenerse de las siguientes maneras:

1. A través de una llamada telefónica o mensaje de texto enviado por el servicio.

2. Mediante el uso de una tarjeta inteligente (token) física o virtual.

3. Utilizando un dispositivo biométrico.

La figura 3 nos enseña los mecanismos de autenticación mas usados en la actualidad y que para algunos sistemas, se usan dos o más mecanismos o factores:

Figura 6. Autenticación doble o múltiple factor

Fuente: *https://www.incibe.es/ciudadania/blog/el-factor-de-autenticacion-doble-y-multiple*

5.3.1.2 Como operan los controles de acceso. Básicamente, el control de acceso se refiere a la identificación de un usuario basado en sus credenciales, seguido de la autorización de su nivel de acceso correspondiente una vez que ha sido autenticado. Las credenciales utilizadas para identificar y autenticar a un usuario incluyen contraseñas, PIN, tokens de seguridad, y exámenes biométricos. Además, la autenticación multifactor (MFA) puede ser utilizada como una medida adicional de seguridad, ya que exige a los usuarios utilizar al menos dos mecanismos de verificación. Cuando la identidad del usuario ha sido confirmada, las políticas de control de acceso le otorgan privilegios específicos permitiéndole proceder según sea necesario.

5.3.1.3 Importancia de un control de acceso. La finalidad del control de acceso es evitar que los datos sensibles sean comprometidos por infiltrados y proteger los datos de las organizaciones, como la propiedad intelectual, la información confidencial de los clientes y colaboradores y la pérdida de recursos corporativos. Las organizaciones necesitan implementar medidas de seguridad como el control

de acceso para reducir los riesgos de seguridad asociados con el acceso no autorizado a la información, especialmente aquellos almacenados en la nube. Si las organizaciones no tienen directivas de control de acceso sólidas, corren el riesgo de enfrentar consecuencias graves debido a ataques a datos confidenciales. Para abordar este problema, las herramientas de gestión de identidad y acceso pueden hacer más simple la administración de esas directivas. Pero antes de implementar cualquier solución, es importante aceptar la necesidad de administrar cómo y cuándo se accede a la información.

5.3.1.4 Recomendaciones para implementar un adecuado control de acceso. Establece un acuerdo con los responsables de tomar decisiones para la implementación de una solución de control de acceso y explica por qué es importante. Una de las razones más significativas para implementar esta solución es la reducción de los riesgos para la organización. Además, otros motivos para implementarla incluyen la productividad, la seguridad y el autoservicio.

Para seleccionar una herramienta adecuada, elige una de gestión de identidad y acceso que proteja la información y brinde una gran experiencia al usuario final. Después de seleccionar la herramienta, establece directivas sólidas para decidir quién puede acceder a los recursos, cuales recursos pueden usar y bajo qué condiciones. Formúlate preguntas sobre los usuarios, grupos, roles o identidades de cargas de trabajo incluidos o exentos de la política, las aplicaciones a las que se aplica la directiva y las acciones de los usuarios sujetas a la política.

Seguir los procedimientos sugeridos, como configurar cuentas de acceso alternas para evitar posibles bloqueos y aplicar directivas de acceso condicional a todos los sistemas. Prueba las políticas antes de implementarlas y establece procedimientos para nombrarlas y hacer planes para casos de interrupción. Al aplicar estas directivas, se obtendrá mayor tranquilidad.

5.3.2 [23]Copias de respaldo. La realización de una copia de seguridad, conocida también como respaldo o backup, tiene como finalidad crear una réplica de archivos físicos o virtuales o bases de datos en un sitio alternativo para protegerlos en caso de un eventual fallo del equipo o algún otro desastre. La elaboración de una copia de seguridad es una tarea esencial para garantizar el éxito de un plan de recuperación de desastres (DRP).

5.3.2.1 ¿Cuáles son los datos más importantes a respaldar y cada cuánto tiempo se debe realizar la copia de seguridad? El proceso de copia de seguridad se enfoca en salvaguardar las bases de datos críticas o las aplicaciones esenciales para el negocio. Para llevarlo a cabo, se siguen políticas definidas de antemano que indican la frecuencia con la que se debe efectuar la copia de seguridad de los datos, la cantidad de copias duplicadas (conocidas como réplicas) y los acuerdos de nivel de servicio (SLA) que establecen los tiempos de restauración necesarios para los datos.

5.3.2.2 Tipos de copia de respaldo. En cuanto a los tipos de copias de seguridad, se pueden identificar varias opciones. La copia de seguridad completa es la más confiable, pero también la más lenta y costosa en términos de recursos. Las organizaciones suelen realizar copias de seguridad completas solo de manera periódica.

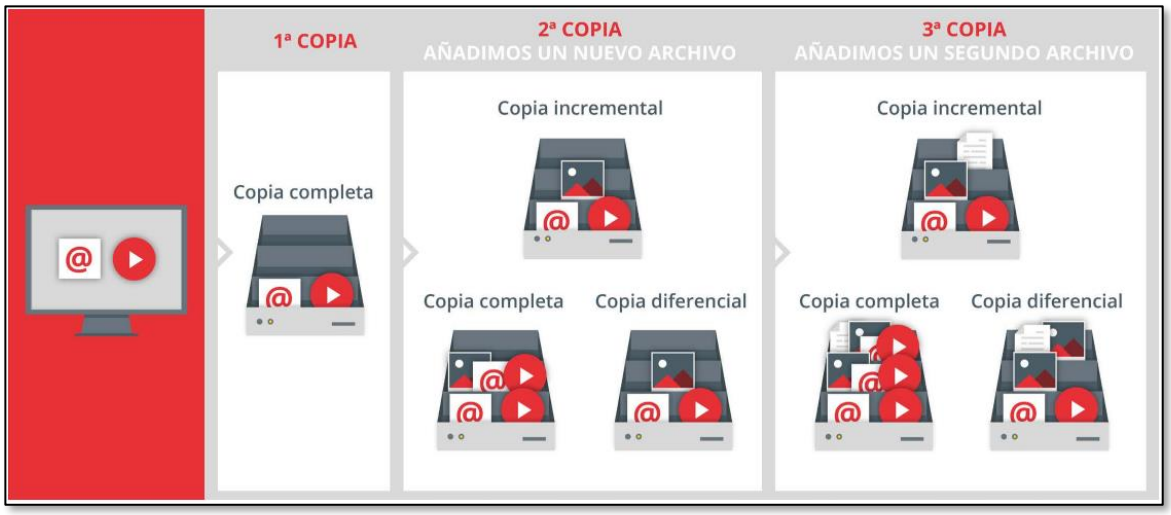
La copia de seguridad incremental solo respalda los datos que han cambiado desde la última copia completa, mientras que la copia diferencial respalda los datos cambiados desde la última copia completa y permite una restauración más rápida.

[23] ROUSE Margaret. Computer Weekly. Copia de seguridad o respaldo [en línea].s.f-[Consultado 21 de abril de 2023]. Disponible en: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

La copia de seguridad completa sintética combina una copia completa original y datos de copias incrementales.

Las copias de seguridad incrementales continuas respaldan los datos completos y luego se complementan con copias incrementales en tiempo real. Las copias de seguridad inversas respaldan solo los cambios realizados entre dos instancias de un espejo, mientras que la copia de seguridad en caliente permite que los usuarios accedan a los datos mientras se están respaldando, aunque puede haber riesgos si los datos se modifican durante el proceso de respaldo.

Figura 7. Tipos de copias de seguridad



Fuente: *https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf*

5.3.2.3 Respaldo en la nube. El respaldo y almacenamiento en la nube se refiere a la práctica de enviar copias de datos a una ubicación remota, lo que puede incluir el centro de datos secundario de una empresa o la instalación de colocación arrendada. Cada vez más, esta práctica se está convirtiendo en un servicio basado en suscripción que proporciona una capacidad escalable y de bajo costo, lo que elimina la necesidad del cliente de comprar y mantener hardware de respaldo. Sin

embargo, es importante que los usuarios cifren los datos y tomen otras medidas para salvaguardar la integridad de los datos.

El respaldo en la nube se divide en tres categorías: almacenamiento público, almacenamiento privado y almacenamiento híbrido. El almacenamiento público implica enviar datos a un proveedor de servicios en la nube, mientras que el almacenamiento privado implica realizar un respaldo de los datos en diferentes servidores dentro del firewall de la compañía. Por último, el almacenamiento híbrido implica que una empresa use tanto el almacenamiento local como el externo, dependiendo de sus necesidades específicas.

5.3.3 Seguridad en las comunicaciones. [24] En el actual contexto caracterizado por la rápida adopción de la digitalización, compañías de diversos sectores y magnitudes se enfrentan a un nuevo reto que tal vez antes no habían considerado de tal gravedad: la urgencia de enfrentar los riesgos de seguridad que emergen a raíz de la incorporación de procedimientos digitales. Por ejemplo, resulta esencial determinar cómo salvaguardar una red de mayor alcance debido al trabajo en modalidad híbrida, o cómo asegurar los límites entre los servicios y las aplicaciones en la nube, los cuales se han vuelto más difusos. A pesar de esto, se observa cierta resistencia a trazar una estrategia debido a la escasa comprensión sobre las amenazas cibernéticas vigentes en el panorama global. Vamos a examinar detenidamente esta problemática.

Es común que los propietarios de pequeñas y medianas empresas colombianas no consideren la transformación digital de su negocio como un proyecto que requiere proteger la información que manejan, ya que no se ven como un objetivo claro de

[24] SANCHEZ Agudo, Jesus. CISCO. La importancia de la seguridad en las comunicaciones de las pequeñas y medianas empresas [en línea]. 12 de abril de 2022. [Consultado 21 de abril de 2023]. Disponible en: https://gblogs.cisco.com/es/2022/04/la-importancia-de-la-seguridad-en-las-comunicaciones-de-las-pequenas-y-medianas-empresas/

ciberamenazas o creen que la información que manejan no es lo suficientemente atractiva para los ciberdelincuentes. Sin embargo, esto es un gran error, ya que en la actual era de los datos, toda la información es valiosa. La ciberdelincuencia es un negocio de todos los tamaños, y no es necesario ser una empresa grande para sufrir un ataque de ransomware en el que se exige dinero para recuperar los datos. Por lo tanto, la transformación digital de cualquier empresa, independientemente de su tamaño, debe incluir una estrategia de ciberseguridad que la proteja.

- **[25]Seguridad de datos mediante la ingeniería**

La ingeniería en seguridad de datos tiene como objetivo construir sistemas defensivos para proteger la red de amenazas potenciales. Además de permitir ciertas actividades, también evita la realización de otras mediante el diseño de sistemas seguros con arquitecturas específicas y diseños que bloquean la red para proteger los datos, computadoras y servidores.

- **Protección a través de encriptación**

La encriptación es una herramienta esencial para la protección de datos y archivos almacenados o en tránsito a través de Internet. Esta técnica dificulta el acceso no autorizado y solo permite la lectura con la clave correspondiente. Para garantizar la seguridad en las comunicaciones, la encriptación debe ser una parte integral de la red y del proceso de trabajo.

- **Control de intrusos y análisis de vulnerabilidad**

[25] MPMSOFTWARE. La seguridad en las comunicaciones. [en línea]. 25 de abril de 2019. [Consultado 21 de abril de 2023]. Disponible en: https://www.mpmsoftware.com/es/blog/seguridad-en-las-comunicaciones/

Los sistemas de detección de intrusos, conocidos como NIDS, detectan actividades sospechosas y recopilan información sobre el tráfico anómalo para su revisión por parte de los administradores. En cuanto al análisis de vulnerabilidad, los analistas de seguridad en las comunicaciones buscan y cierran agujeros en el sistema que los hackers podrían utilizar para acceder de manera no autorizada.

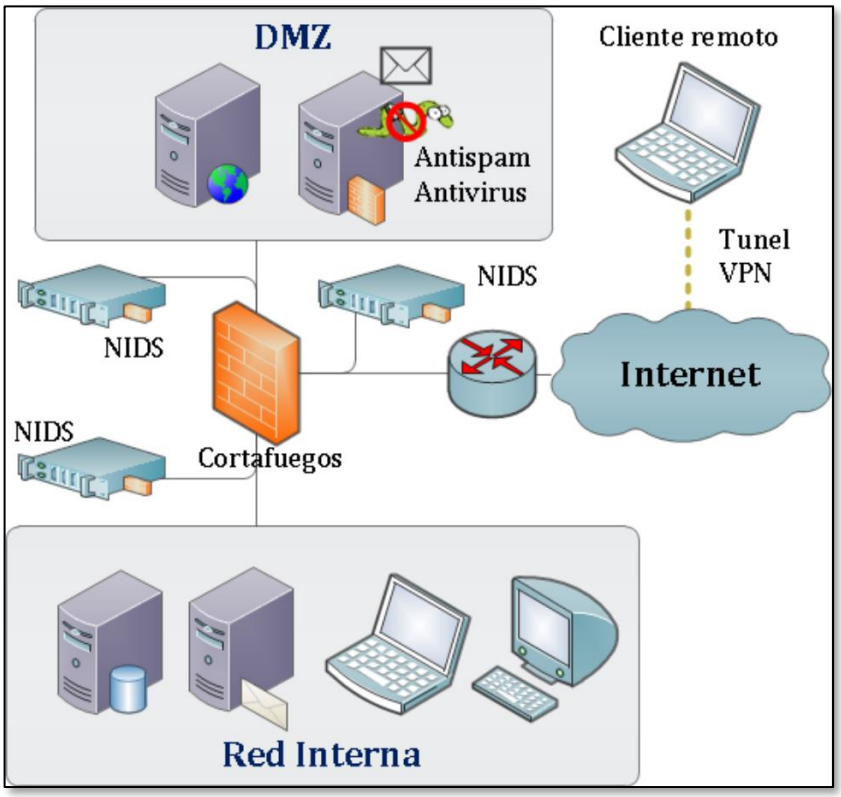
5.3.3.1 SD-WAN: una solución de red automática, ágil y segura para empresas de todos los tamaños. Las soluciones de red SD-WAN ofrecen una protección integral en múltiples áreas clave para empresas de cualquier tamaño, incluyendo:

- Seguridad en la navegación por Internet desde la sede de la empresa
- Funciones avanzadas de firewall de aplicaciones
- Filtros web
- Protección contra intrusos
- Antimalware
- Conexión segura a la VPN para teletrabajadores

Además, SD-WAN proporciona una comunicación totalmente encriptada entre las sedes de la empresa y los teletrabajadores, lo que garantiza la confidencialidad total de los datos que se transmiten. Esto es especialmente importante para sectores de PYMEs que manejan información crítica y sensible, como gestorías contables, pequeños centros de salud privados o despachos de abogados.
Además de adoptar una estrategia de protección, es importante tener en cuenta otros consejos útiles para proteger el negocio:

1. Buscar asesoramiento específico de profesionales8
2. Prestar mucha atención a los correos electrónicos sospechosos
3. Trabajar siempre con copias de seguridad
4. Mantenerse informado

Figura 8. Topología básica de seguridad perimetral de red.



Fuente: *https://repositorio.untels.edu.pe/jspui/bitstream/123456789/800/1/T088A_48457169_T.pdf*

5.3.3.2 Solución WAF. Una solución de seguridad conocida como Firewall de Aplicaciones Web (WAF) es capaz de proteger las aplicaciones web de ataques comunes mediante la supervisión y filtrado del tráfico. Este sistema de seguridad tiene la capacidad de bloquear el tráfico malicioso que intenta ingresar a una aplicación web o salir de ella sin autorización, lo que ayuda a prevenir fugas de información.

5.3.4 26Gestión de parches de seguridad. La aplicación de actualizaciones de software, controladores y firmware para proteger contra vulnerabilidades se conoce como gestión de parches. Además de mejorar la seguridad, una gestión de parches

[26] INTEL. ¿Qué es la gestión de parches?. [en línea].s.f-[Consultado 21 de abril de 2023]. Disponible en: https://www.intel.es/content/www/es/es/business/enterprise-computers/resources/patch-management.html

efectiva también contribuye a un mejor rendimiento del sistema, lo que aumenta la productividad. Todos los sistemas informáticos, desde los portátiles de los empleados hasta los dispositivos especializados como terminales y señalización digital, deben ser seguros. No prestar atención a la gestión de parches puede poner en riesgo la empresa, exponiéndola a filtraciones y vulnerabilidades, pérdida de productividad y daño a la reputación.

5.3.4.1 Ventajas: ¿Por qué es importante la gestión de parches? La gestión de parches es crucial para proteger sus terminales contra los hackers y mantener sus sistemas en óptimas condiciones. Pero también ofrece otras ventajas importantes, que incluyen:

- Mejora la productividad dentro de la organización: Aunque a menudo se piensa que la gestión de parches es un obstáculo para la productividad, la realidad es que el software bien gestionado y actualizado puede mejorar el rendimiento de los empleados y, por lo tanto, la productividad en general.

- Reduce el costo del ciclo de vida de los dispositivos: Dado que muchas empresas tienen empleados que trabajan en remoto, las herramientas de gestión remota pueden ampliar las capacidades de la TI, lo que reduce la necesidad de costosos envíos de hardware o visitas de servicio técnico.

- Ayuda a cumplir con leyes, regulaciones y estándares de cumplimiento: Muchas empresas tienen que cumplir con normativas locales o federales de protección de datos, como la Ley de Transferencia y Responsabilidad de Seguro Médico (HIPAA) para registros de pacientes, el Reglamento General de Protección de Datos (GDPR) para información personal recopilada durante las interacciones con los clientes y normativas similares. La gestión de parches ayuda a cumplir con estas normativas.

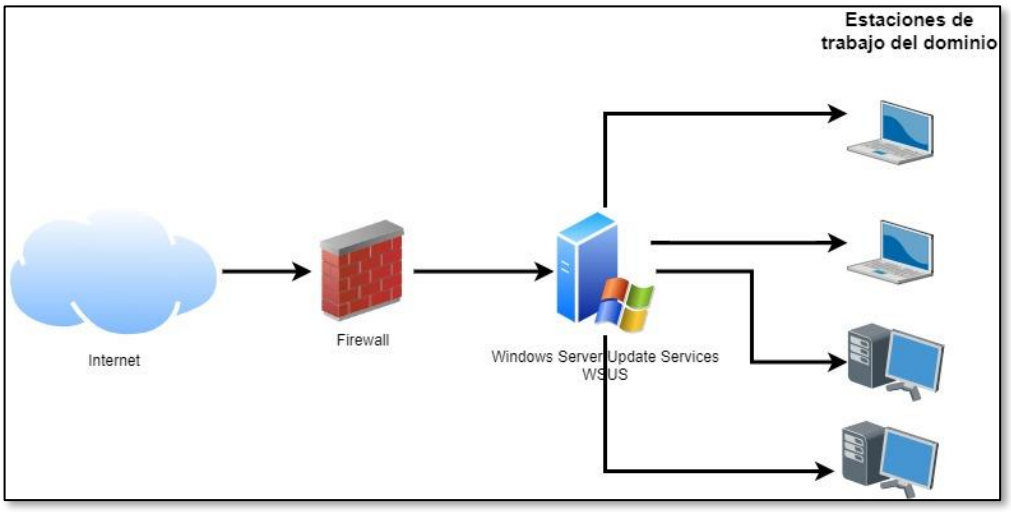
5.3.4.2 Buenas prácticas en gestión de parches de seguridad. La gestión de parches es crucial para proteger los sistemas informáticos y garantizar la productividad en una organización. Aquí hay algunas razones por las que es importante y cómo aplicar las mejores prácticas:

1. **Ventajas de la gestión de parches:** además de proteger los sistemas informáticos de los hackers, la gestión de parches también fomenta la productividad y ayuda a reducir los costos de gestión y reparación. También ayuda a cumplir con las normativas y regulaciones.

2. **Mejores prácticas:** la gestión de parches no se limita a la actualización del sistema operativo y las aplicaciones, sino que también incluye la actualización del firmware y los controladores. La gestión de parches debe ser rutinaria y predecible para toda la organización. Los parches deben implementarse primero en un pequeño grupo de usuarios antes de aplicarlos a toda la organización. Los departamentos de TI deben saber quién es responsable de parchear las vulnerabilidades conocidas, y se recomienda la utilización de sistemas de gestión de parches.

La figura 6 nos representa de manera grafica un esquema básico de actualizaciones de sistemas operativos Windows en una red local LAN donde llegan todas las actualizaciones de Microsoft al servidor de actualizaciones y este a su vez, las envía a las estaciones de trabajo mediante las políticas de actualización establecidas:

Figura 9. Esquema básico de gestión de actualizaciones y parches de seguridad centralizado



Fuente: *Elaboración propia*

5.3.5 Gestión de incidentes. La gestión de incidentes implica el proceso que las compañías siguen para identificar, responder, registrar y analizar los riesgos de salud y seguridad a los que se enfrentan sus empleados en el lugar de trabajo. Desafortunadamente, los accidentes laborales son un problema muy frecuente.

5.3.5.1 La importancia de la gestión efectiva de incidentes en las empresas. La gestión de incidentes, que consiste en identificar, prevenir, responder, registrar y analizar los riesgos asociados a la salud y seguridad en el lugar de trabajo, tiene como objetivo garantizar la seguridad de los empleados y el medio ambiente, a la vez que mantiene la productividad de la organización y reduce los costos innecesarios. Un incidente de salud y seguridad no solo afecta el bienestar y la moral de los trabajadores, sino que también puede tener consecuencias financieras para la empresa. Los incidentes en el lugar de trabajo pueden interrumpir las operaciones y resultar en costosas indemnizaciones laborales, reclamaciones por daños a la propiedad, gastos de limpieza ambiental y aumentos en las primas de seguros. Además, pueden causar daños incalculables a la reputación de la empresa.

5.3.5.2 La gestión de incidentes, pasos fundamentales:

En la figura 7 se establecen las fases primordiales de una adecuada gestión de incidentes o también llamado ciclo de vida de la gestión de incidentes:

Figura 10. El ciclo de vida de la gestión de incidentes

Fuente: *https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf*

- [27]Registro del reporte de incidente: La documentación de un incidente puede llevarse a cabo a través de comunicaciones telefónicas, mensajes de correo electrónico, SMS, la cumplimentación de formularios web disponibles en el portal de autoayuda o por medio de conversaciones mediante chat en tiempo real.

- Categorización del incidente: Los incidentes tienen la capacidad de ser clasificados y subdivididos según el ámbito de tecnología de la información o

[27] MANAGEENGINE. ¿Qué es la gestión de incidentes ITIL. [en línea].s.f-[Consultado 19 de agosto de 2023]. Disponible en: https://www.manageengine.com/latam/service-desk/gestion-de-incidentes-itil/guia-definitiva-que-es-la-gestion-de-incidentes-itil.html

sector empresarial en el cual el incidente causa una interrupción. Esto abarca áreas como la red, el hardware, entre otros.

- Establecimiento de prioridad del incidente: La importancia de un incidente puede ser evaluada tomando en cuenta su efecto y urgencia mediante el uso de una matriz de prioridades. El impacto del incidente denota el nivel de perjuicio que el problema ocasionaría al usuario o a la empresa. La urgencia de un incidente señala el lapso en el cual el incidente debe ser solventado. En función de su prioridad, los incidentes se pueden clasificar de la siguiente manera:

    - Crítico
    - Alto
    - Medio
    - Bajo

- Asignación y direccionamiento de incidentes: Una vez que el incidente ha sido categorizado y priorizado, se asigna de manera automática a un técnico con la experiencia pertinente para su resolución.

- Creación y administración de tareas: Según la complejidad del incidente, este puede dividirse en subactividades o tareas más pequeñas. Por lo general, estas tareas son generadas cuando se necesita la participación de varios técnicos de distintos departamentos para resolver el incidente.

- Gestión y escalada de los Acuerdos de Nivel de Servicio (SLA): Durante el proceso de manejo del incidente, es esencial que el técnico cumpla con los términos del Acuerdo de Nivel de Servicio (SLA, por sus siglas en inglés) sin infringirlos. El SLA representa el tiempo aceptable para responder (SLA de respuesta) o resolver (SLA de resolución) un incidente. Estos acuerdos pueden asignarse a los incidentes basándose en sus características, como la categoría,

el solicitante, el impacto, la urgencia, etc. En situaciones en las que el SLA está por ser incumplido o ya ha sido incumplido, el incidente puede ser escalado a nivel funcional o jerárquico con el propósito de asegurar una resolución lo más pronta posible.

- Resolución del incidente: Un incidente se considera resuelto cuando el técnico ha encontrado una solución provisional o definitiva para el problema en cuestión.

- Cierre del incidente: Una vez que el problema ha sido solventado y el usuario está satisfecho con la solución propuesta, el incidente puede ser dado por cerrado.

6 CONCLUSIONES

Después de realizar una investigación exhaustiva sobre el estado actual de la seguridad digital en las empresas de Colombia, y de examinar diferentes metodologías y normas para la gestión de la seguridad digital, se han identificado varias conclusiones importantes.

Primero, se identificaron las principales amenazas a las que se enfrentan las empresas en cuanto a la seguridad digital, incluyendo ataques de phishing, malware y vulnerabilidades en la red. Estas amenazas son especialmente preocupantes para las empresas que no cuentan con medidas de seguridad adecuadas.

En segundo lugar, la exploración de diferentes iniciativas para la gestión de la seguridad digital reveló la viabilidad de su adopción por parte de las empresas. Se encontró que la adopción de marcos de seguridad vigentes es una estrategia efectiva para fortalecer las organizaciones y mitigar los riesgos de seguridad digital.

Tercero, se recomendaron controles técnicos mínimos basados en marcos de seguridad vigentes para fortalecer la seguridad digital en las empresas de Colombia. Estos controles incluyen la implementación de medidas de autenticación fuertes, la actualización regular de software y hardware, la monitorización continua de la red y la gestión de vulnerabilidades.

Además, se recomendó la ISO 31000 como la guía a seguir para la gestión del riesgo. Esta norma proporciona un marco completo y sistemático para la gestión de riesgos en cualquier tipo de organización, independientemente de su tamaño, sector o ubicación geográfica.

Siguiendo los principios y directrices establecidos en la norma ISO 31000, las organizaciones pueden identificar, evaluar y tratar los riesgos que enfrentan de manera más efectiva y eficiente. Además, esta norma también promueve una cultura de gestión de riesgos en toda la organización, lo que puede mejorar la toma de decisiones y aumentar la resiliencia de la empresa.

En conclusión, es fundamental que las empresas en Colombia tomen medidas para fortalecer su seguridad digital y mitigar los riesgos a los que se enfrentan. La adopción de marcos de seguridad vigentes y la implementación de controles técnicos mínimos son esenciales para proteger los datos y la información de las empresas y garantizar su éxito a largo plazo.

7 RECOMENDACIONES

De manera muy puntual y teniendo en cuenta lo que se ha relacionado a lo largo de la investigación, se ha considerado traer algunas recomendaciones clave en el aspecto técnico para los ataques mas comunes a nivel nacional:

Contra Ransomware

- Copias de Seguridad Regularmente: Realizar copias de seguridad frecuentes y seguras de todos los datos importantes, manteniéndolas desconectadas de la red principal para evitar su contaminación.

- Actualizaciones de Seguridad: Mantener todos los sistemas operativos, software y aplicaciones actualizados con los últimos parches de seguridad para cerrar posibles vulnerabilidades.

- Capacitación y Concienciación del Personal: Educar continuamente a los empleados sobre los riesgos del ransomware, enseñándoles a reconocer señales de alerta y a evitar prácticas riesgosas.

Contra Phishing

- Formación en Conciencia de Seguridad: Capacitar a los empleados regularmente para reconocer y manejar adecuadamente los intentos de phishing, especialmente en correos electrónicos y mensajes.

- Autenticación de Dos Factores (2FA): Implementar la autenticación de dos factores para todas las cuentas importantes, proporcionando una capa adicional de seguridad.

- Soluciones Anti-phishing: Utilizar herramientas de filtrado de correo electrónico y software Anti-phishing para detectar y bloquear activamente intentos de phishing.

Contra Ataques de Denegación de Servicio (DoS)

- Sistemas de Mitigación de DoS: Implementar soluciones específicas para mitigar ataques DoS, como firewalls de aplicación web y sistemas de prevención de intrusiones.

- Plan de Respuesta a Incidentes: Desarrollar y mantener un plan de respuesta a incidentes que incluya procedimientos claros para actuar rápidamente en caso de un ataque DoS.

- Monitoreo y Análisis Continuos: Establecer un sistema de monitoreo constante del tráfico de red para detectar y responder a patrones inusuales que puedan indicar un ataque DoS.

Para el caso de los marcos de ciberseguridad que se han citado, podemos mencionar generalidades a tener en cuenta al momento de optar por la implementación de alguno de estos (COBIT, NIST e ISO 27001):

Comprensión Detallada del Marco

- Educación y Formación: Antes de iniciar la implementación, es crucial que los miembros del equipo involucrados comprendan a fondo el marco elegido. Esto puede incluir formación formal, talleres y sesiones de estudio de material relacionado.

- Análisis de Alineación con la Organización: Evaluar cómo el marco se alinea con los objetivos de negocio, la estructura organizacional y los procesos existentes. Esto facilita una integración más suave y eficiente.

Evaluación de la Situación Actual y Planificación

- Evaluación de Riesgos y Necesidades: Realizar una evaluación exhaustiva de los riesgos actuales, las necesidades de seguridad y el estado de las prácticas y políticas existentes. Esta evaluación debe alinearse con los principios y objetivos del marco elegido.

- Planificación Estratégica: Desarrollar un plan estratégico que detalle los pasos específicos, los recursos necesarios, los plazos y los responsables de cada etapa del proceso de implementación.

Involucramiento de la Alta Dirección

- Compromiso de la Dirección: Asegurar el compromiso y el apoyo de la alta dirección. Su participación activa es crucial para asignar recursos, establecer la importancia del proyecto y resolver obstáculos organizacionales.

- Comunicación Clara: Mantener una comunicación abierta y regular con todas las partes interesadas, incluyendo la dirección, los empleados y, si es necesario, los clientes o socios. Esto ayuda a garantizar la transparencia y el apoyo continuo.

Implementación y Capacitación

- Implementación Gradual y Priorizada: Empezar con las áreas más críticas o vulnerables. Una implementación gradual permite ajustar y aprender del proceso a medida que se avanza.

- Capacitación Continua: Capacitar al personal en las prácticas, políticas y herramientas relevantes del marco. La capacitación debe ser continua para adaptarse a los cambios en el marco y en el entorno de seguridad.

Auditoría, Monitoreo y Mejora Continua

- Auditorías Internas y Externas: Realizar auditorías regulares para evaluar la efectividad de la implementación y para identificar áreas de mejora.

- Monitoreo y Revisión Continua: Establecer un proceso de revisión y actualización constante para asegurarse de que el marco se mantenga relevante y efectivo frente a las nuevas amenazas y cambios en el negocio.

- Cultura de Mejora Continua: Fomentar una cultura organizacional que valore y apoye la mejora continua en la gestión de la seguridad de la información.

La implementación exitosa de cualquier marco de ciberseguridad requiere una planificación cuidadosa, compromiso organizacional y una adaptación constante a las nuevas circunstancias y desafíos, por esto se considera que estas recomendaciones son fundamentales para garantizar que la implementación sea efectiva, independientemente del marco específico elegido.

BIBLIOGRAFÍA

AKAMAI. ¿Qué es un firewall de aplicaciones web (WAF)?s.f-{Consultado 21 de abril de 2023}. Disponible en: https://www.akamai.com/es/glossary/what-is-a-waf

AREVALO, María Camila. Pirani. Todo lo que debe saber sobre la norma ISO 31000. 13 de octubre de 2022. {Consultado 22 de abril de 2023}. Disponible en: https://www.piranirisk.com/es/blog/todo-lo-que-debe-saber-sobre-la-norma-iso-31000

Ascontroltech. La importancia de la ciberseguridad en las organizaciones {Sitio web}. Bogotá, Colombia: Ascontroltech, 8 de febrero de 2021. {Consultado el 9 de abril de 2023}. Disponible en: https://ascontroltech.com/la-importancia-de-la-ciberseguridad-en-las-organizaciones/

Beltrán, S. Semana. Tendencias en ciberseguridad para el 2022. Semana. 2 de enero de 2022. {Consultado el 9 de abril de 2023}. Disponible en: https://www.semana.com/economia/empresas/articulo/tendencias-en-ciberseguridad-para-el-2022/202240/

Ciberseguridad.com. COBIT {en línea}.s.f-{Consulta: 21 de abril de 2023}. Disponible en: https://ciberseguridad.com/normativa/espana/sgsi/cobit/

Ciberseguridad.com. Controles de seguridad CIS {en línea}.s.f-{Consulta: 9 de abril de 2023}. Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/

Chanaga, J. Asociación Colombiana de Ingenieros de Sistemas - ACIS. La competencia por el talento en ciberseguridad en el 2023. {Sitio web}. Octubre de 2022. {Consultado el 9 de abril de 2023}. Disponible en: https://acis.org.co/portal/content/la-competencia-por-el-talento-en-ciberseguridad-en-el-2023

DIAZ Granados H. KASPERSKY. Un tercio de latinos desconoce daños que ciberataques podrían ocasionar en empresas {en línea}. 07de julio de 2020. {Consultado el 9 de abril de 2023}. Disponible en: https://latam.kaspersky.com/blog/un-tercio-de-latinos-desconoce-danos-que-ciberataques-podrian-ocasionar-en-empresas/19600/

Escuela Europea de Excelencia. Cómo realizar la evaluación de riesgos según ISO 31000:2018. 16 de mayo de 2018. {Consultado 22 de abril de 2023}. Disponible en: https://www.escuelaeuropeaexcelencia.com/2018/05/como-realizar-la-evaluacion-de-riesgos-segun-iso-310002018/

Esan. Controles de seguridad CIS {en línea}. 27 de mayo de 2021. {Consulta: 21 de abril de 2023}. Disponible en: https://www.esan.edu.pe/conexion-esan/cobit-2019-como-beneficia-a-una-organizacion

INCIBE. El factor de autenticación doble y múltiple {en línea}. 27 de febrero de 2019. {Consultado 19 de agosto de 2023}. Disponible en: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

INFOMAE. Ciberataque a Sanitas: hackers revelaron más información clasificada de la EPS {en línea}. 14 de marzo de 2023. {Consultado el 9 de abril de 2023}. Disponible en: https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/

Infobae. Las 34 empresas que fueron hackeadas en Colombia durante 2022 {en línea}. 2 de enero de 2023. {Consultado el 9 de abril de 2023}. Disponible en: https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/

INTEL. ¿Qué es la gestión de parches?.s.f-{Consultado 21 de abril de 2023}. Disponible en: https://www.intel.es/content/www/es/es/business/enterprise-computers/resources/patch-management.html

Interpolados. ISO/IEC 31000:2018: 6.5. TRATAMIENTO DEL RIESGO. 16 de mayo de 2018. {Consultado 22 de abril de 2023}. Disponible en: https://interpolados.wordpress.com/2020/11/12/iso-iec-310002018-6-5-tratamiento-del-riesgo/

ISACA. Cynthus. Transformación digital con COBIT 2019 {en línea}. 10 de febrero de 2020. {Consultado 20 de agosto de 2023}. Disponible en: https://www.cynthus.com.mx/transformacion-digital-con-cobit-2019/

ISC. Inspire a Safe and Secure Cyber World: Cybersecurity Workforce Study Sheds New Light on Global Talent Demand Amid a Lingering Pandemic. {Consultado el 30 de octubre de 2022}. Disponible en Internet: https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand

Jimenez, D. Viafirma Colombia. Ciberseguridad en Colombia: riesgos y oportunidades {en línea}.s.f-{Consultado el 9 de abril de 2023}. Disponible en: https://www.viafirma.com.co/blog/ciberseguridad-colombia/

MANAGEENGINE. ¿Qué es la gestión de incidentes ITIL.s.f-{Consultado 19 de agosto de 2023}. Disponible en: https://www.manageengine.com/latam/service-desk/gestion-de-incidentes-itil/guia-definitiva-que-es-la-gestion-de-incidentes-itil.html

MPMSOFTWARE. La seguridad en las comunicaciones. 25 de abril de 2019. {Consultado 21 de abril de 2023}. Disponible en: https://www.mpmsoftware.com/es/blog/seguridad-en-las-comunicaciones/

Microsoft. ¿Qué es el control de acceso? {en línea}.s.f-{Consulta: 21 de abril de 2023}. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control

Pastor Carrasco, Carlos Alberto. La ciberseguridad en las organizaciones {en línea}.s.f-{Consultado el 9 de abril de 2023}. Disponible en: http://contadores-aic.org/la-ciberseguridad-en-las-organizaciones/

Pirani Risk. ISO 27001: ¿Qué es y cómo implementarla? {en línea}.s.f-{Consultado el 9 de abril de 2023}. Disponible en: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

ROUSE Margaret. Computer Weekly. Copia de seguridad o respaldo {en línea}.s.f-{Consultado 21 de abril de 2023}. Disponible en: https://www.computerweekly.com/es/definicion/Copia-de-seguridad-o-respaldo

Romero, S. Xataka Colombia. Estos son los tipos de ciberataques más frecuentes en Colombia {en línea}.s.f-{Consultado el 9 de abril de 2023}. Disponible en:

https://www.xataka.com.co/seguridad/estos-tipos-ciberataques-frecuentes-colombia

SANCHEZ Agudo, Jesus. CISCO. La importancia de la seguridad en las comunicaciones de las pequeñas y medianas empresas {en línea}. 12 de abril de 2022. {Consultado 21 de abril de 2023}. Disponible en: https://gblogs.cisco.com/es/2022/04/la-importancia-de-la-seguridad-en-las-comunicaciones-de-las-pequenas-y-medianas-empresas/

SPHERA'S, Editorial Team. ¿Qué es la gestión de incidentes?. 21 de junio de 2022. {Consultado 21 de abril de 2023}. Disponible en: https://sphera.com/glosario-es/que-es-la-gestion-de-incidentes/?lang=es

Tarlogic. Guías NIST en ciberseguridad {en línea}. 14 de junio de 2022. {Consultado el 9 de abril de 2023}. Disponible en: https://www.tarlogic.com/es/blog/guias-nist-ciberseguridad/

Universidad Piloto de Colombia. Ciberseguridad en las organizaciones, el personal {Documento electrónico}. Bogotá, Colombia: Universidad Piloto de Colombia, 2017. {Consultado el 9 de abril de 2023}. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2C%20el%20personal.pdf.

Xataka Colombia. Controles de seguridad CIS {en línea}.s.f-{Consulta: 21 de abril de 2023}. Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/

Xataka Colombia. COBIT {en línea}.s.f-{Consulta: 21 de abril de 2023}. Disponible en: https://ciberseguridad.com/normativa/espana/sgsi/cobit/

Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Fecha de Realización:	**12/12/2023**
Programa:	**Especialización en Seguridad Informática**
Línea de Investigación:	Estándares y buenas prácticas de seguridad
Título:	ANÁLISIS DE LOS ESTÁNDARES Y BUENAS PRÁCTICAS DE CIBERSEGURIDAD UTILIZADOS POR LA INDUSTRIA COLOMBIANA
Autor(es):	Diaz Chantre Rodrigo
Palabras Claves:	COBIT, NIST, ISO 27001, Ciberataques, Ciberseguridad
Descripción:	Este documento ofrece un análisis conciso de tres marcos fundamentales en la seguridad de la información y gobernanza de TI: COBIT, NIST e ISO 27001, centrándose en sus aspectos más relevantes. COBIT es examinado por su enfoque en la gobernanza de TI, destacando cómo ayuda a las organizaciones a alinear sus procesos de TI con sus objetivos de negocio, enfatizando su adaptabilidad a los desafíos actuales. El marco del NIST se analiza en relación a la ciberseguridad, mostrando su utilidad en la gestión de riesgos cibernéticos a través de un conjunto de estándares y prácticas recomendadas, aplicable a diferentes sectores y tamaños de organizaciones. Por último, ISO 27001 es presentado por su enfoque sistemático en la gestión de la seguridad de la información. Se enfatiza su importancia en el establecimiento de controles de seguridad y gestión de riesgos, siendo un marco de trabajo reconocido internacionalmente. En conjunto, el documento demuestra cómo COBIT, NIST e ISO 27001 se complementan para reforzar la seguridad de la información y la

	gobernanza de TI en las organizaciones modernas.

Fuentes bibliográficas destacadas:

Ascontroltech. La importancia de la ciberseguridad en las organizaciones {Sitio web}. Bogotá, Colombia: Ascontroltech, 8 de febrero de 2021. {Consultado el 9 de abril de 2023}. Disponible en: https://ascontroltech.com/la-importancia-de-la-ciberseguridad-en-las-organizaciones/

DIAZ Granados H. KASPERSKY. Un tercio de latinos desconoce daños que ciberataques podrían ocasionar en empresas {en línea}. 07de julio de 2020. {Consultado el 9 de abril de 2023}. Disponible en: https://latam.kaspersky.com/blog/un-tercio-de-latinos-desconoce-danos-que-ciberataques-podrian-ocasionar-en-empresas/19600/

ISACA. Cynthus. Transformación digital con COBIT 2019 {en línea}. 10 de febrero de 2020. {Consultado 20 de agosto de 2023}. Disponible en: https://www.cynthus.com.mx/transformacion-digital-con-cobit-2019/

Pastor Carrasco, Carlos Alberto. La ciberseguridad en las organizaciones {en línea}.s.f-{Consultado el 9 de abril de 2023}. Disponible en: http://contadores-aic.org/la-ciberseguridad-en-las-organizaciones/

Universidad Piloto de Colombia. Ciberseguridad en las organizaciones, el personal {Documento electrónico}. Bogotá, Colombia: Universidad Piloto de Colombia, 2017. {Consultado el 9 de abril de 2023}. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2C%20el%20personal.pdf.

Contenido del documento:	Este documento analiza la implementación de COBIT, NIST e ISO 27001 en la ciberseguridad de la industria colombiana, destacando cómo estos marcos se adaptan a las necesidades específicas de seguridad de la información y gobernanza de TI en Colombia. Se enfoca en el uso de COBIT para alinear los procesos de TI con los objetivos empresariales, la aplicación del NIST en la mejora de la ciberseguridad adaptable a diferentes

	organizaciones, y la importancia de ISO 27001 en la gestión sistemática de la seguridad de la información y control de riesgos. El documento concluye resaltando la integración de estos estándares como clave para fortalecer las prácticas de ciberseguridad en la industria colombiana, subrayando la importancia de una comprensión adaptada a las particularidades del contexto colombiano.
Marco Metodológico:	El marco metodológico de este documento es de naturaleza mixta, combinando enfoques cualitativos y cuantitativos. La investigación se caracteriza por su diseño descriptivo, centrado en detallar los aspectos necesarios para la implementación de los estándares COBIT, NIST e ISO 27001 en el contexto de la ciberseguridad colombiana. En cuanto a las fuentes de datos, se realizó una extensa recopilación de información a través de internet. Se incluyeron datos de encuestas, documentos académicos de la universidad, y estudios sobre comportamientos generales en seguridad informática en empresas colombianas y de América Latina. El análisis se centró principalmente en la revisión de documentos y publicaciones en línea. Para la selección de fuentes, se estableció como criterio principal la actualidad de la información, priorizando publicaciones del año 2019 en adelante principalmente. Se hizo especial énfasis en utilizar fuentes de sitios web y proveedores de seguridad reconocidos, incluyendo los sitios web oficiales de los estándares investigados. El estudio no incluyó el uso de herramientas de análisis estadístico o de contenido, dada la naturaleza descriptiva y teórica de la investigación. Asimismo, no se identificaron limitaciones significativas en el estudio,

	permitiendo una exploración amplia y detallada del tema. En términos éticos, la investigación se basó exclusivamente en información pública y general de los estándares y hechos noticiosos sobre ciberataques recientes, por lo que no se presentaron consideraciones éticas particulares.
Conceptos adquiridos:	**Entendimiento Integral de COBIT, NIST e ISO 27001:** Adquisición de un conocimiento profundo sobre cómo estos marcos guían la gobernanza de TI y la gestión de la seguridad de la información en las empresas. **Aplicabilidad de Estándares en el Contexto Colombiano:** Comprensión de cómo estos estándares internacionales se adaptan y aplican en el escenario específico de la industria colombiana, teniendo en cuenta sus desafíos y necesidades únicas. **Estrategias de Ciberseguridad y Gestión de Riesgos:** Aprendizaje sobre la importancia de implementar estrategias de ciberseguridad efectivas y la gestión de riesgos, basadas en las prácticas recomendadas por estos marcos. **Alineación de Objetivos de TI con Metas Empresariales:** Conocimiento adquirido sobre cómo COBIT ayuda a las organizaciones a alinear sus procesos de TI con sus objetivos estratégicos, contribuyendo al éxito global de la empresa. **Mejoras en la Ciberseguridad a través del NIST:** Comprensión de cómo el marco del NIST proporciona un conjunto de estándares y prácticas para gestionar riesgos cibernéticos de manera eficiente. **Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI):** Entendimiento del papel de ISO 27001 en el

	establecimiento de un SGSI efectivo para proteger la información y los datos críticos de la empresa. **Actualización y Relevancia de los Datos:** Conciencia de la importancia de utilizar datos y fuentes actualizadas para una investigación relevante y precisa, especialmente en un campo en rápida evolución como la ciberseguridad. **Perspectiva Global y Local en Ciberseguridad:** Reconocimiento de la importancia de considerar tanto los estándares internacionales como las particularidades locales al abordar los desafíos de ciberseguridad.
Conclusiones:	La investigación sobre la seguridad digital en empresas colombianas destaca la urgencia de abordar amenazas como phishing, malware y vulnerabilidades de red, especialmente críticas en organizaciones sin medidas de seguridad robustas. La adopción de marcos de seguridad contemporáneos emerge como una táctica clave para reforzar las empresas y mitigar riesgos. Se sugiere la implementación de controles técnicos fundamentales, incluyendo autenticación fuerte, actualizaciones regulares y gestión de vulnerabilidades. Adicionalmente, la norma ISO 31000 se presenta como un marco integral para la gestión de riesgos, aplicable a diversas organizaciones y fomentando una cultura de gestión de riesgos. La conclusión subraya la importancia crítica de que las empresas colombianas refuercen su seguridad digital y adopten estas prácticas para proteger sus datos y asegurar su éxito sostenible.