Importancia del uso de marcos de trabajo para la gestión de riesgos de ciberseguridad en organizaciones de salud del sector público en COLOMBIA

Jonathan Betancourt Zuñiga

Asesor

Luis Fernando Zambrano Hernandez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias, Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Con el corazón rebosante de una profunda gratitud, quiero dedicar unas palabras a quienes hicieron posible este logro.

En primer lugar, agradezco a Dios, por sentir su guía en cada paso y por la serena certeza de que este momento ya habitaba en sus planes para mí, su presencia fue la fuerza silenciosa que sostuvo mi empeño.

A la Virgen María, por su amparo de madre que me ha acompañado con infinita ternura en todas las etapas de mi vida, en ella siempre encontré un refugio para mis dudas y una luz en los momentos de incertidumbre.

Mi más sincero reconocimiento a cada una de las personas que, con su sabiduría, su paciencia y su apoyo incondicional, iluminaron el camino para la realización de este documento, sus consejos fueron el cimiento firme y su aliento el impulso necesario para llegar hasta este punto.

A todos, mi gratitud total y permanente.

Dedicatoria

Dedico estas páginas al faro de mi vida, mi hija**,** cada línea aquí escrita lleva la huella invisible de su sonrisa, esa alegría pura que le da sentido a todo, ella es mi porqué y mi para quién.

A mi esposa, la roca firme en este viaje, quien ha sido el apoyo silencioso y constante que sostuvo mis horas de dedicación, gracias por creer en este sueño, incluso cuando el camino se hacía largo, y por ser el equilibrio perfecto en mi vida.

A mis padres, las raíces que me sostienen, les debo el privilegio de haber llegado hasta aquí, cada sacrificio suyo fue un peldaño que me permitieron subir, y su apoyo incondicional es la herencia más valiosa que jamás podré recibir.

Resumen

Actualmente existen diferentes marcos de trabajo para mejorar la postura de ciberseguridad de las organizaciones de todos los tamaños, la adecuada gestión de riesgos es crucial para la seguridad cibernética en las entidades de salud públicas, ya que protege la información y los datos.

La protección de datos es vital para el correcto funcionamiento dentro de la política pública y su relación con el ciudadano, teniendo en cuenta la ley estatutaria 1581 de 2012 que se refiere a las disposiciones legales aplicables a los datos personales registrados en cualquier base de datos y que son susceptibles de tratamiento por entidades de naturaleza pública o privada.

Por su parte, el anexo 3 de la resolución MinTIC 1519 del 2020 relaciona las condiciones mínimas técnicas y de seguridad digital con el fin de mitigar riesgos de incidentes cibernéticos o filtración de datos personales o sensibles, destacando la importancia de la seguridad Digital y la implementación del Sistema de Gestión de Seguridad de la Información y obliga a los sujetos obligados a implementar controles de seguridad asociados con el desarrollo de sitios web seguros.

La información pública es el eje central de toda entidad pública y de la ciudadanía, por lo cual debe ser protegida, asegurando su confidencialidad, integridad y disponibilidad. En Colombia, el Ministerio de Tecnología de la Información y las Comunicaciones ha avanzado significativamente en la implementación de sistemas de gestión de seguridad de la información. Desde 2018, se han realizado esfuerzos sustanciales para proteger la información mediante estos sistemas, respondiendo a las necesidades de los ciudadanos y las entidades públicas.

Palabras clave: Gestión de Riesgos, Protección de datos, Seguridad Cibernética.

Abstract

Currently there are different frameworks to improve the cybersecurity posture of organizations of all sizes, proper risk management is crucial for Cybernetics Security in public health entities, as it protects information and data.

Data protection is vital for the proper functioning within public policy and its relationship with the citizen, taking into account the statutory law 1581 of 2012 which refers to the legal provisions applicable to personal data recorded in any database and which are susceptible to processing by entities of a public or private nature.

For its part, Annex 3 of MinTIC resolution 1519 of 2020 relates the minimum technical and digital security conditions in order to mitigate risks of cyber incidents or leakage of personal or sensitive data, highlighting the importance of Digital security and the implementation of the Information Security Management System and obliges the obliged subjects to implement security controls associated with the development of secure websites.

Public information is the backbone of all public entities and citizens, and therefore must be protected, ensuring its confidentiality, integrity and availability. In Colombia, the Ministry of Information Technology and Communications has made significant progress in the implementation of information security management systems. Since 2018, substantial efforts have been made to protect information through these systems, responding to the needs of citizens and public entities.

Keywords: Cybernetics Security, Data Protection, Risk Management.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Glosario

Amenaza: cualquier tipo de acción que pueda lograr causar daño a los activos de una organización, mediante la pérdida o destrucción de la información lo cual puede ocasionar que los servicios que presta la entidad tanto externo, como internos dejen de funcionar, también económicas y de prestigio.

"Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información." (Departamento de Seguridad Informática, 2014).

ASRM: Gestión de Riesgos de la superficie de ataque, es una solución de seguridad Trend Vision One - Attack Surface Risk Management, que reduce drásticamente el riesgo cibernético con detección continua, evaluaciones en tiempo real y mitigación automatizada en entornos locales, híbridos o en la nube.

Hacktivismo: ocurre cuando activistas políticos o sociales hacen uso de la tecnología informática para hacer una declaración en apoyo de una de sus causas.

Riesgo: se define el riesgo como la posibilidad de que la entidad a nivel de información sufra daños o perdidas, y el impacto que este pueda tener sobre los activos que forman parte de tecnologías de la información y que tengan valor para la organización.

Vulnerabilidad: fallo informático que pone en peligro los activos de información de las entidades, en seguridad de la información los malware están diseñados para atacar las vulnerabilidades y aprovecharse de estos para realizar ataques sobre los activos de información,

"Las vulnerabilidades se corresponden con fallos en los sistemas físicos y/o lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de equipos." (Gómez Vieites, 2014).

Introducción

La presente monografía consiste en entender de manera general la gestión de riesgos de seguridad informática en las organizaciones de salud del sector público en Colombia, las cuales contribuyen al bienestar y la salud de millones de colombianos, entidades que tienen la obligación constitucional de garantizar el derecho a la salud de los ciudadanos en todo el territorio nacional.

El papel que cumple la Superintendencia Nacional de Salud en la supervisión de los recursos del gasto público destinados a la salud, ya que, de acuerdo con lo consultado en el sitio oficial de la misma entidad en su columna (*Conozca más de la Superintendencia Nacional de Salud*, s. f.), dentro de sus funciones, se encuentra, inspeccionar, vigilar y controlar los recursos del sistema de salud. Así como también, examinar, exigir y controlar las actividades en salud de las compañías de seguros, incluyendo las que administran el Seguro Obligatorio de Accidentes de Trámites (Soat) y las Administradoras de Riesgos Laborales.

En los últimos años, la tecnología ha cambiado y avanzado significativamente y estos cambios han expuesto a las entidades a riesgos tanto internos como externos que pueden impactar el logro de sus objetivos (Smith & Jones, 2020). Las amenazas cibernéticas, las vulnerabilidades en los sistemas y la rápida evolución de las tecnologías emergentes han creado un entorno en el que la gestión de riesgos es más crítica que nunca (Doe, 2018). Las organizaciones deben adaptarse continuamente a estos cambios para proteger sus activos y asegurar la continuidad de sus operaciones (National Institute of Standards and Technology, 2018).

Se han acrecentado los riesgos y las potenciales vulnerabilidades con el desarrollo de las nuevas tecnologías como es el caso de la inteligencia artificial que debido a su utilización

indebida como lo indica el boletín académico Número 20 del (CSIRT Académico UNAD, 2024) los ciberdelincuentes pueden manipular los algoritmos y los datos de entrenamiento para mejorar actividades ilícitas, como la creación de desinformación y contenido falso, la explotación de sesgos, la recopilación de biometría y otros datos sensibles.

La Inteligencia Artificial Disruptiva enfocada a la mejora de los ataques cibernéticos haciendo especial referencia al riesgo generado por la inteligencia artificial (IA) al ser utilizada para llevar a cabo ataques cibernéticos de manera sofisticada y efectiva. La IA puede ser utilizada tanto por los ciberdelincuentes o por equipos de ciberseguridad para mejorar sus capacidades y estrategias. Los atacantes pueden utilizar la IA para automatizar y agilizar sus ataques, identificar vulnerabilidades en los sistemas objetivo, desarrollar malware más avanzado y adaptarse rápidamente a las defensas implementadas. Por ejemplo, pueden utilizar algoritmos de aprendizaje automático para realizar acciones de phishing más convincentes y personalizados, o para identificar y explotar debilidades en los sistemas de seguridad. Por otro lado, los equipos de respuesta a incidentes informáticos también pueden utilizar la IA para detectar y prevenir explotaciones, analizar grandes cantidades de datos en busca de patrones y anomalías, con el fin de fortalecer las defensas de los sistemas.

Se recuerda como en Colombia se expidió en 2011 el Documento CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa, cuyo objetivo era fortalecer las capacidades del Estado para enfrentar las amenazas en el ámbito cibernético, creando así el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. En este documento CONPES se determinaron estrategias para enfrentar las amenazas que atentan contra la seguridad y defensa del Estado relacionadas con la ciberseguridad y la ciberdefensa, tales como la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT),

el Centro Cibernético Policial, CECIP y el Comando Conjunto Cibernético CCOCI, bajo un modelo de coordinación intersectorial.

Planteamiento del problema

A finales del 2023 se desplego el ataque cibernético bajo la modalidad ransomware dirigido a IFX Network como lo indica consultorsalud.com en su noticia titulada (*Sector salud afectado en ciberataque a entidades del Estado*, 2023), compañía prestadora de servicios de Computación, y que a su vez prestó en su estos servicios a las entidades que reportaron el ciberataque, la Superintendencia Nacional de Salud y la herramienta MIPRES del Ministerio de Salud, con la que esa cartera garantiza el acceso, reporte de prescripción, suministro, verificación, control, pago y análisis de la información de las tecnologías en salud que no son pagadas con dinero proveniente del plan de beneficios (PBS).

De acuerdo con (SonicWall, 2022), editor de la información sobre amenazas de ransomware, en su reporte del 2022 indica que el ransomware subió un 105% sin precedentes en 2021, y el crecimiento explosivo de estrategias como la extorsión doble e incluso la triple extorsión garantizaron que estos ataques tuvieran más exitosos que nunca. Pero a medida que los ciberdelincuentes se han vuelto más sofisticados y exitosos, también se han vuelto más despiadados: muchos de los ataques de ransomware más en 2021 parecían más que nunca actos de guerra, poniendo en peligro nuestro suministro de alimentos, agua, combustible, nuestros hospitales y nuestros municipios.

Según Sonic Wall (SonicWall, 2023) reporta que, un total de 26.448 Vulnerabilidades y Exposiciones Comunes (CVE) se publicaron en 2022, según el NIST. Representando el duro trabajo que los miembros de la industria de la ciberseguridad están haciendo para identificar vulnerabilidades más rápida y eficazmente. También refleja las tendencias perniciosas que hacen necesario un trabajo más rápido y eficaz en el sector de la ciberseguridad.

Sonic Wall en su informe (SonicWall, 2024) da a conocer que el volumen del

ransomware aumenta en las Américas y específicamente en LATAM: 51%, sin embargo, a nivel mundial, registra un -49%, lo que sugiere que se debe de propender por implementar medidas de ciberseguridad más efectivas orientadas al ramsonware para LATAM.

La (Función Pública, s. f.) en el decreto 338 de 2022 plasma en su ARTÍCULO 2.2.21.1.4.3. Obligaciones de seguridad de las autoridades titulares de infraestructura crítica, o que presten servicios esenciales. Las autoridades, definidos como titulares de infraestructura crítica o que presten servicios esenciales, propenderán por contar con un plan de seguridad digital, protección de las redes, las infraestructuras críticas cibernéticas, los servicios esenciales y los sistemas de información en el ciberespacio y deberán hacer periódicamente una evaluación del riesgo de seguridad digital.

El Gobierno Nacional ha promovido activamente la alineación de las organizaciones estatales con las directrices emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), incorporando prácticas recomendadas en seguridad de la información y lineamientos estratégicos en concordancia con normas internacionales, como la ISO/IEC 27001 y el uso de la metodología MAGERIT para la gestión de riesgos de TI.

Existen desafíos persistentes y significativos en la implementación efectiva de los marcos de trabajo propuestos, puesto que la ineficacia en la adopción de un marco de trabajo estructurado para la gestión de riesgos de TI puede resultar en una evaluación incompleta de los riesgos, lo que a su vez puede conducir a impactos negativos, incluyendo pérdidas de recursos tanto para las organizaciones como para el estado colombiano, es importante recordar que los recursos del gasto público provienen de impuestos y deducciones fiscales, lo que afecta directamente a los ciudadanos colombianos.

A partir de la problemática descrita es posible consolidar la pregunta de investigación

asociada al presente trabajo:

¿Porque es Importante el uso de marcos de trabajo para la gestión adecuada de Riesgos de ciberseguridad en Organizaciones de Salud del sector Público en Colombia?

Justificación

En Colombia, las entidades públicas del sector salud manejan un volumen significativo de información proveniente de diferentes sistemas lo que contribuye al funcionamiento de una amplia gama de servicios para la comunidad, esta información abarca diversos sectores, incluido el los recursos destinados a la salud y que son vigilados por parte de la Supersalud; cualquier vulnerabilidad en la seguridad de esta información podría comprometer su integridad, disponibilidad y confidencialidad, lo que destaca la importancia de implementar medidas de seguridad adecuadas para proteger los activos de información contra posibles amenazas que podrían afectar la continuidad operativa de los sistemas e infraestructura tecnológica.

El desarrollo de este documento monográfico brinda un entendimiento profundo sobre la gestión de riesgos en la seguridad de la información dentro de las entidades públicas del sector salud, se indaga sobre los marcos de trabajos internacionales que pueden mejorar su postura de ciberseguridad.

Dada la situación actual de las entidades de salud, nace la necesidad de llevar a cabo la revisión documental de marcos de trabajo de trabajo sobre los cuales se alinea el MINTIC, junto el análisis de casos de ciberataques asociados a entidades de salud, y recomendar normativas y estándares internacionales que pueden influir en la mejora de las capacidades de las organizaciones para mejorar la postura en seguridad cibernética; también, es esencial comprender cómo los casos de ataques informáticos pueden aportar a la gestión de riesgos de TI efectiva para afrontar los desafíos de la ciberseguridad.

Objetivos

Objetivo general

Analizar la relevancia de los marcos de trabajo en la gestión de riesgos de ciberseguridad en las organizaciones del sector público de salud en Colombia, con el fin de identificar cómo estos contribuyen a la protección de sus activos de información.

Objetivos específicos

Indagar sobre el uso de marcos de trabajo en la gestión de riesgos de ciberseguridad en organizaciones estatales colombianas del sector salud, mediante la identificación de sus principales componentes y la comparación con estándares internacionales.

Analizar los casos de ciberataques y determinar cómo los marcos de trabajo en ciberseguridad influyen en la mitigación del riesgo y la recuperación ante un incidente.

Proponer recomendaciones basadas en la evaluación de la efectividad de los marcos y el análisis de los casos de ciberataques que sirvan como contribución para la mejora y la resiliencia del entorno digital del sector salud público en Colombia.

Marco Referencial

Antecedentes

Colombia es un país que como muchos maneja información de diferente tipo, con el enfoque según el tipo de entidad pública, y dependiendo del Ministerio al que pertenezca.

Esa información es vital para estas Entidades públicas son propensas a ataques a su información, en Colombia se registran más de 542.465 ataques informáticos diarios (El Tiempo, 2017), las entidades públicas algunas veces no cuenta con un área o responsable en la toma de decisión sobre la herramientas para el manejo de los riesgo, lo que implica que ante una afectación todo se escala al jefe de TI, es el que toma la decisión a su vez estima los pasos que se deben seguir para no impactar los servicios. El personal de Tecnología se encarga de soportar, sin embargo, no se cuenta con procesos establecidos, por lo que no se aplican estándares.

Con el fin de minimizar la materialización de los riesgos en la seguridad de la información se han definido los siguientes modelos o estándares.

En el 2005 se crea el MECI Modelo Estándar de Control Interno para el estado Colombiano, creado con la promulgación del decreto 1599 (Función Pública, 2005), es el fundamento en el que se estructura, documenta e implementa el sistema de control interno de las entidades, este está basado en los principios del autocontrol, la autorregulación y la autogestión.

En el 2005 el termino Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas de administración de la información el cual nació de la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission, donde se especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (Vásquez Ojeda, 2020).

En el 2018 el 14 de febrero se publicó la nueva norma ISO 31000 “Gestión del riesgo. Principios y directrices”, la cual sustituye a la versión de 2009. La NTC ISO 31000 enumera 11 principios para una gestión eficaz del riesgo.

Es importante que las entidades públicas a nivel nacional conozcan, especifiquen y manifiesten todos los aspectos de la gestión, además de esto es importante que se capacite a los equipos. La NTC ISO 31000 identifica elementos de un marco de trabajo de gestión del riesgo estos deben estar integrados con la alta dirección de la entidad (Salazar, 2019).

Marco conceptual

Gestión de Riesgos: la gestión de riesgos es una parte importante en la seguridad informática ya que ahorra tiempo y recursos, ya que permite la detección temprana de riesgos o posibles omisiones de estos, brindando un análisis adecuado de información; el dato es considerando como valor y su adecuado manejo podría determinar el éxito en las entidades.

En la norma NTC ISO 31000 de la Organización Internacional de Normalización, que proporciona principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo donde se define que la gestión de riesgo es sistemática, estructurada y oportuna explicando que las entradas de los procesos de la gestión de riesgos se basan en fuentes de información como son datos históricos, experiencias, retroalimentación de las partes involucradas, observación, previsión y exámenes de expertos se puede aplicar en la seguridad de la información (Riveros, 2020).

Conceptos relacionados con riesgos como los relacionados a continuación:

Activo de información: son datos creados o utilizados por los procesos dentro de las entidades sea de modo Digital o físico, el hardware, software utilizado en el procesamiento, transporte o almacenamiento de información.

Según (Escrivá Gascó et al., 2013) en su libro Seguridad Informática define a un activo como aquel recurso del sistema informático o no, necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no. Según esta definición, se consideran activos: los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc.

Es decir que un activo son todos los elementos necesarios para que una Entidad se desempeñe de manera correcta y alcance sus objetivos y cumpla con su misión y visión , Incluye hardware infraestructura, cableado de red, equipos de cómputo, servidores, Software sistema operativo, aplicaciones, programas de cómputo y finalmente el activo más importante de una organización son los datos o la información los cuales son base de datos, paquetes de información, copias de seguridad, claves, reportes, archivos y contraseñas, en el caso de las entidades públicas sus procesos y los datos de los ciudadanos dependiendo del sector en el que estén, si es salud por ejemplo, toda la población debería estar afiliado al sistema de salud.

Los siguientes son los riesgos a los que está expuesta la información en las entidades del sector público en salud:

Riesgo Asociado a Catástrofes: estos son los riesgos relacionados con la naturaleza como: terremotos, inundaciones y entre otros.

Riesgos de Pérdida de Prestigio: estos riesgos están relacionados con la pérdida de la confiabilidad, prestigio o veracidad de una Entidad, debido a su baja credibilidad de sus servicios y productos independientemente del sector al que pertenecen.

Riesgo por Variaciones y Pérdida de Flujo Eléctrico: Estos riesgos ocurren por descargas eléctricas en el suministro de electricidad que posee la entidad.

Riesgo por Mal uso o Mala Configuración de Equipos: Estos riesgos se presentan por uso indebido de los activos de TI una organización, ejemplo borrado de información de un sistema que es core de la entidad, mala manipulación de los datos, el poco control sobre las personas que tienen permisos de administración de las bases de datos, el no manejar auditorias sobre las tablas.

Riesgos de Violación de la Integridad: este tipo de riesgo se presenta cuando se altera información o los datos de un archivo o una base de datos, modificándolos voluntaria o involuntariamente por un sujeto o una situación inesperada.

Riesgo de Pérdidas de Confidencialidad de la Información: Este tipo de riesgos se presenta cuando existe robo de la información de la institución para su posterior distribución, con el fin de dañar la entidad o a las personas involucradas a esta.

Riesgo por Vandalismo: Estos riesgos son físicos son acciones sobre la infraestructura de las entidades.

Seguridad de la información: La norma ISO/IEC 27001 define a la seguridad de la información como el conjunto de medidas preventivas y reactivas que toca como norma una Entidad, la cual permite el resguardo y protección la información, donde se tiene como base los siguientes principios:

- ✓ Confidencialidad. Asegura el acceso a la información a los funcionarios que cuenten con permisos mediante una autorización previa, en este caso está el manejo de permisos dentro de las entidades es muy importante y no puede ser tomado a ligera.
- ✓ Disponibilidad. La información dentro de las Entidades debe encontrarse a disposición de quienes deben acceder a ella en el momento que así lo requieran.
- ✓ Integridad. Busca mantener los datos libres de modificaciones no autorizadas, mantenerlos lo más completos posibles, tal como se obtienen de fuente.

La norma ISO/IEC 27001 define a un Sistema Gestión de Seguridad de la Información como un conjunto de políticas de administración de la información con el propósito de que las Entidades diseñen, implanten y mantengan los procesos para gestionar eficientemente el acceso a la información, con el fin de mantener la información siempre disponible, integra y confidencial.

De un tiempo para acá se ha visto un esfuerzo importante por parte de las entidades del sector público específicamente las del sector salud por proteger la distinta información que manejan, planteando resoluciones, normatividad legal vigente, como ejemplo la implementación del estándar ISO/IEC 27001, la Ley de Protección de Datos Personales, Ley de Transparencia, entre otros.

Marco teórico

Importancia de la gestión de riesgos en de seguridad informática en Organizaciones del sector público en salud en Colombia

Actualmente las entidades Públicas del orden nacional apoyadas por el MINTIC buscan enfatizar en una adecuada gestión de riesgos de la seguridad informática en los diferentes entes a nivel nacional, el MINTIC cuenta con el Marco de Seguridad del Modelo de Seguridad y Privacidad de la información, este es utilizado para la toma de decisiones (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021).

Se debe como punto importante resaltar que, para la evaluación de riesgos en seguridad de la información, un prerrequisito de alta importancia es la clasificación de activos de información, tomando esta como una buena práctica al momento de realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA tomando en cuenta criterios de clasificación como son: Confidencialidad, Integridad y Disponibilidad.

Según el (Departamento Nacional de Planeación, 2020) en su documento CONPES 3995 Política Nacional de Confianza y Seguridad Digital, en el plan de acción sugiere analizar la adopción de modelos, estándares y marcos de trabajo enfocados en la gestión de riesgos de seguridad digital y respuesta a incidentes del sector.

Teniendo en cuenta lo anterior, en el sector público se resguarda información sensible de los ciudadanos a nivel nacional, y el activo más importante de las Entidades del sector público y para todos los sectores es la información, la seguridad informática busca resguardarla a través de 5 pilares la disponibilidad, la integridad, la confidencialidad, la autenticidad y el no repudio.

En la actualidad aplicar estos cinco pilares de seguridad de información es conocida como actitud ciber-resiliente, la cual se puede definir como "la capacidad de una organización de gestionar el riesgo existente y superarlo con un mínimo impacto para la organización"

A lo largo del mundo se ha comprobado que la ciber-resiliencia ayuda a reducir las pérdidas financieras y los daños respecto a la reputación de las organizaciones. Tanto así que, si una organización recibe la certificación de resiliencia cibernética, puede infundir confianza en sus clientes y usuarios, a esto se le conoce como impacto positivo en cuanto a lo que tiene que ver con la reputación de las organizaciones, lo que puede aumentar la posibilidad de ganar licitaciones con clientes y obtener nuevos socios.

Para precisar la resiliencia de acuerdo con el (Departamento Nacional de Planeación, 2016) CONPES 3854 Política Nacional de Seguridad Digital, es la capacidad para recuperar la operación de los sistemas e infraestructura a sus estados iniciales, dando por terminada la perturbación a la que haya sido sometida.

Efectos negativos de no realizar gestión de riesgos en la Seguridad informática.

Cuando una entidad no tiene un manejo de gestión de riesgo de seguridad de la información está poniendo en riesgo la información sensible, en el caso de las entidades públicas la afluencia de la información es bastante alta, además que es la información de sus ciudadanos, sin irnos más lejos las entidades del sector salud, manejan información de las Eps, Arl, fondos de pensiones, las historias clínicas, las personas que cotizan al sistema nacional de país, sus beneficiaros, esta información es información de alta importancia, que si se llega a violar algunos de los pilares de la información, se pierde información vital para el funcionamiento de EPS, IPS y demás prestadores de salud, este sería el primer enfoque la perdida de la información.

Además, el aplicar el proceso sistemático de la gestión de riesgos de una manera adecuada en las organizaciones los hace cada vez menos propensos a sufrir ataques de tipo ramsomware, donde las entidades que carecen de sistemas de control interno donde se gestionen estos riesgos son más vulnerables y pueden ser víctimas de ataques por parte de estructuras organizadas de ciberdelincuentes.

Entrando un poco más en contexto, según el *estudio trimestral de ciberseguridad ataques a entidades del gobierno* (2022) existen diferentes tipos de ataques ransomware dentro de los cuales se encuentran los ataques “Lock and Leak” haciendo uso de criptografía para el cifrado de los datos con el objetivo de interrumpir las actividades de las organizaciones para posteriormente filtrarlos en comunidades de hacktivistas y cibercriminales con el fin adicional de llamar la atención con relación al ataque.

Este es un tema de especial cuidado, el manejo de la información y las salvaguardas para la gestión de los activos de información, dado que información de las personas podría ser divulgada para fines delictivos, fraudes, extorción y violación de la privacidad.

Si se perdiera información sensible de los ciudadanos por ataques, las personas que robaron esta información la podrían usar para realizar diferentes tipos de fraude, se debe recordar que las entidades públicas manejan do tipos de información la privada y la pública. La pública debe ser publicada en la página web de cada entidad, como por ejemplo procesos de contratación, resoluciones, entre otros, y la información privada debe ser salvaguardada como por ejemplos los datos personales de los ciudadanos.

A causa de un ciberataque se podrían perder información sensible de los ciudadanos, y vienen otro enfoque, la seguridad, la perdida de la credibilidad de los ciudadanos al estado, recuperar la confianza de los ciudadanos en las instituciones públicas es fundamental para que haya un crecimiento inclusivo y de mayor bienestar para todos, en resumen, sin seguridad de la información y sin gestión de riesgos se podría perder credibilidad, esto se vería traducido en pérdida de confianza en la entidad por la mala reputación, y de la misma manera significaría pérdidas económicas.

La gestión de riesgos en la seguridad informática y los 5 pilares de seguridad de información y salvaguardar la información.

Mediante una metodología para el análisis de riesgos en TI, es de precisar que los riesgos son el potencial de una vulnerabilidad de un activo o de un grupo de activos en una entidad pudiendo ser explotada por una amenaza, dentro del análisis de los riesgos el primer paso es realizar la identificación de activos de información de las entidades, los activos de TI son la información, el hardware, el software, instalaciones y las personas.

En la Guía de Gestión de Riesgos emanada por el (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016a) la cual está orientada a las entidades públicas, para seguir los procedimientos para la gestión de riesgos basado en la ISO 27005, se puede usar las

diferentes etapas de la gestión de riesgos como en la planificación, identificación, análisis, beneficiando a las entidades y manteniendo su información.

De acuerdo con fuente consultada en (*IBM*, s. f.) La gestión del riesgo se define como "el proceso de identificar, evaluar y controlar los riesgos financieros, legales, estratégicos y de seguridad para el capital y las ganancias de una organización."

La gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño de la organización; el enfoque integral de la gestión del riesgo depende esencialmente de la identificación y análisis del riesgo, concepción y aplicación de medidas de prevención y mitigación.

El riesgo es un resultado combinado de la amenaza y la vulnerabilidad, en el primer caso son procesos o fenómenos naturales con suficiente intensidad, en un espacio y tiempo específicos, para causar daños, en la segunda son condiciones resultantes de factores físicos, socioeconómicos y ambientales que aumentan la susceptibilidad de la comunidad a los impactos de amenazas.

Realizar una implementación adecuada de la gestión de riesgos le permite a la organización aumentar la probabilidad de alcanzar los objetivos, ser consciente de la necesidad de identificar y tratar los mismos, mejorar los controles, asignar y usar eficazmente los recursos, minimizar perdidas entre muchas otras.

Marco legal

A continuación, se define el marco legal relacionado a la presente investigación se hace necesario citar las leyes, decretos y normativas mediante las cuales se han regulado los temas de seguridad de la información en Colombia.

CONPES 3854 DE 2016 “POLÍTICA NACIONAL DE SEGURIDAD DIGITAL”. Este documento CONPES trata de una estrategia nacional y consideraciones relacionadas a la seguridad digital, incluyendo la gestión de riesgos como elemento principal.

LEY 1581 DE 2012 “PROTECCIÓN DE DATOS PERSONALES” Existen datos que pueden ser públicos y otros que no, esta ley define los datos que son considerados como sensibles, es decir que afectan la intimidad del ciudadano que su uso indebido puede generar discriminación, las entidades públicas están obligadas a proteger estos datos sensibles.

DECRETO 1008 DE 2018 “POLÍTICA DE GOBIERNO DIGITAL” Este decreto especifican los lineamientos generales de la política de gobierno digital, mediante lo cual se pretende el aprovechamiento de las tecnologías de la información y la Comunicación, tomando gran importancia porque se quiere facilitar el número de tramites que generan las entidades en un portal centrado para tal fin.

Decreto 767 del 2022 Nueva Política de Gobierno Digital en este decreto se establece los lineamientos generales de la Política de Gobierno Digital, esta va dirigida a las entidades públicas a nivel nacional, es obligatoria para las entidades que conforman la administración pública y los particulares que cumplen funciones administrativas.

Marco contextual

Actualmente en cuanto a seguridad de información se está implementando la política de gobierno digital 2018-2022 establecida por MINTIC, la cual se obliga por dos políticas:

En la Política de Gobierno Digital de la Presidencia de la república (2022) y emanada mediante decreto 767, se establecieron los lineamientos generales de la Política de Gobierno Digital, esta va dirigida a las entidades públicas, la academia, el sector privado, las

organizaciones de la sociedad civil, los ciudadanos y, en general, los habitantes del territorio nacional.

Esta política es obligatoria para las entidades que conforman la administración pública y los particulares que cumplen funciones administrativas, también se contara con un manual de gobierno digital el cual comprende lineamientos, guías y estándares para la implementación y desarrollo de la Política de Gobierno Digital los cuales estarán contenidos en un único instrumento, centralizado, estandarizado y de fácil uso, denominado Manual de Gobierno Digital.

En los lineamientos generales de la política de gobierno digital *Decreto 1008 de 2018 - Gestor Normativo - Función Pública* (2018), tiene como objeto establecer lineamientos generales de la Política de Gobierno Digital para Colombia, que se conocía antes estrategia de Gobierno en Línea, la cual desde debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

En este caso también son obligadas a aplicarlas las entidades públicas y las particulares que cumplan funciones administrativas dentro del estado Colombiano, nos habla específicamente de seguridad de la información donde como principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del estado, y de los servicios que prestan al ciudadano.

Teniendo en cuenta los componentes de la Política de Gobierno Digital, estos componentes permiten alcanzar con éxito la implementación de esta política:

TIC para el estado: su objetivo es mejorar el funcionamiento de las entidades y su relacionamiento con otras entidades.

TIC para la sociedad: Su objetivo es el fortalecimiento de la relación del estado con la sociedad en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de estos.

Habilitadores Transversales de la Política de Gobierno Digital: estos son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, permitiendo el logro de la política de gobierno digital.

Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los Entidades deberán cumplir con la finalidad de lograr el establecimiento de la Política de Gobierno Digital.

Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital.

Los propósitos de la Política de Gobierno Digital: Son los fines de la Política de Gobierno Digital, entre los cuales se encuentran:

Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.

Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información.

Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto

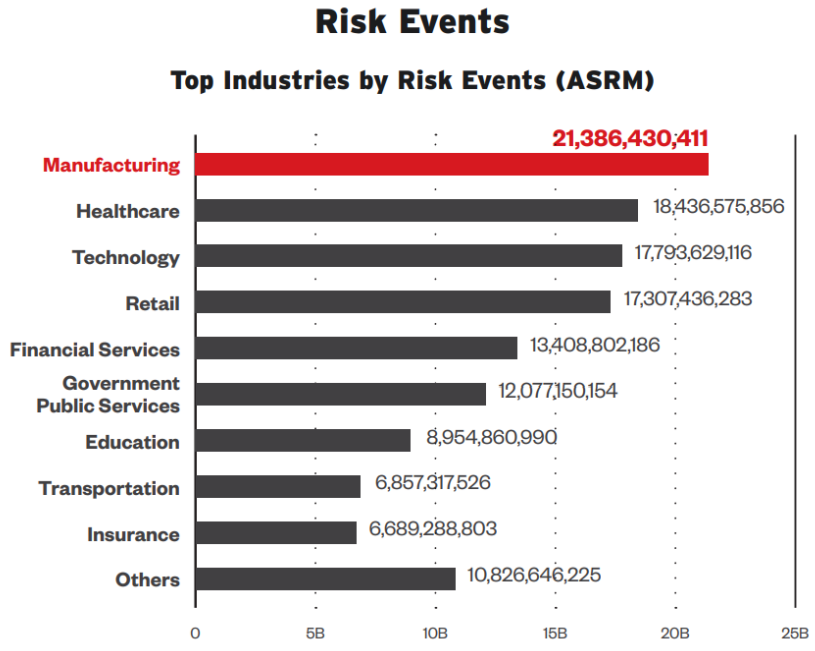
Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.

Trend Micro, esta organización dedicada a prestar servicios de ciberseguridad a empresas alrededor del mundo y que se posiciona como uno de los lideres y referentes en materia de ciberseguridad.

En su reporte anual sobre ciberseguridad (TrendMicro, 2023), la salud aparece en segundo lugar como uno de los sectores principales que se enfrentan a eventos de riesgo detectados a través de ASRM, esto sugiere que las organizaciones dedicadas al cuidado de la salud se encuentran entre las más atacadas por amenazas relacionadas con recursos en la nube, por lo que se detectaron más de 18 Billones de eventos de riesgo, como se muestra en la imagen a continuación, solamente superado por el sector de la manufacturación.

Figura 1

Industrias por Eventos de Riesgo

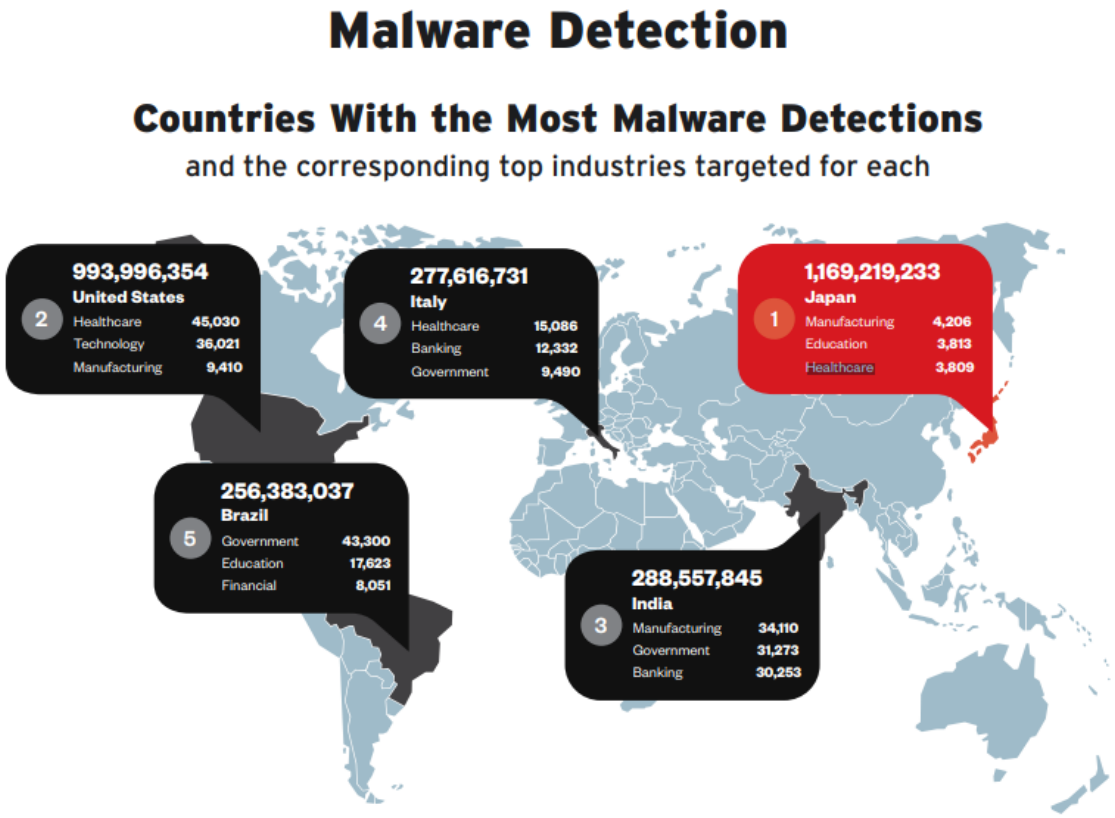


Nota. Industrias más afectadas por eventos de riesgo. Tomado de (TrendMicro, 2023).

Destaca, además, los países con la mayor detección de malware por industria, donde aparece la salud con los mayores niveles de detección de malware en países como Estados Unidos e Italia, tal cual como se evidencia en la figura a continuación donde se puede observar la cantidad de detección de malware.

Figura 2

Detección de Malware



Nota. Países con mayor detección de malware. Tomado de (TrendMicro, 2023).

Las amenazas dirigidas a las instituciones de atención médica pueden tener consecuencias graves más allá de las filtraciones de datos o las pérdidas financieras; las

interrupciones en las redes de atención médica pueden afectar potencialmente la atención al paciente, el acceso a los registros médicos e incluso poner vidas en riesgo en casos extremos.

Al final del informe provee un conjunto de recomendaciones con la finalidad de mitigar los riesgos, dentro de las que se encuentran:

Actualizar sistemas y aplicaciones: aplicar el último parche, actualizar el sistema operativo o la versión de la aplicación.

Fortalecer la seguridad con Trend Micro: aplicar reglas de prevención en los productos Trend Micro dedicados a proteger contra la explotación de vulnerabilidades.

Optimizar la configuración: Optimizar la configuración débil en el entorno actual.

Bloquear acceso a aplicaciones riesgosas: evitar acceder a aplicaciones reportadas como riesgosas o bloquear su uso.

Fortalecer la seguridad de las cuentas: desactivar cuentas con contraseñas débiles o restablecerlas con contraseñas fuertes. Habilitar la política de bloqueo de cuentas en el Active Directory.

Restringir el acceso y revisar dispositivos: restringir el uso de cuentas de usuario en dispositivos afectados, verificar y resolver eventos de alto riesgo.

Fortinet

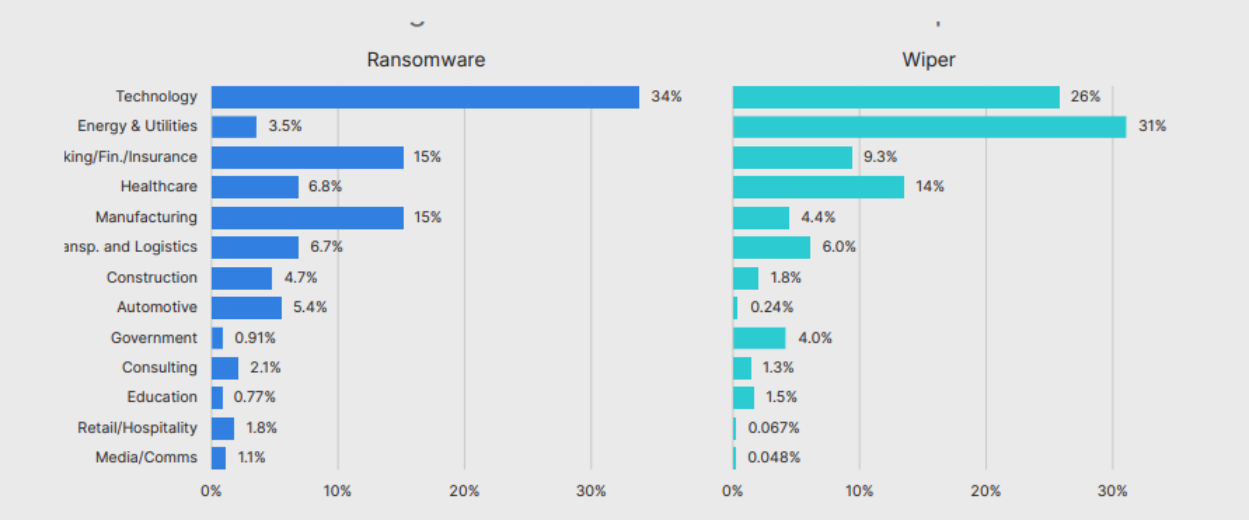
En el informe global del panorama de amenazas (Fortinet, 2023) menciona específicamente a la industria de la salud como uno de los sectores críticos que está cada vez más en la mira de los grupos de ransomware.

Pronostica que para el 2024 los adversarios que buscan pagos más grandes dirigirán su atención a industrias críticas como la atención médica, los servicios públicos, la fabricación y las finanzas.

De acuerdo con la imagen a continuación, aparecen discriminadas las muestras de ransomware y wiper que recogieron los sensores de Fortinet durante la segunda mitad de 2023.

Figura 3

Muestreo Ransomware vs Wiper 2023



Nota. Informe global del panorama de amenazas - Segundo semestre 2023. - gráfico comparativo ransomware vs wiper. Tomado de Fortinet. (2023).

El informe, dedica una sección para los grupos de APT que continúan siendo altamente adaptables y activos durante la segunda mitad del año 2023, a la vez que actúan de manera sigilosa a medida que planifican y ejecutan ataques. En esta sección, muestra un gráfico de los Grupos APT más activos durante el segundo semestre de 2023, según la inteligencia de FortiRecon, aparece el sector de la salud como afectado por el grupo APT OilRig de acuerdo con (*MITRE ATT&CK®*, s. f.) es un supuesto grupo Iraní de amenazas que ha atacado a víctimas de Oriente Medio y de todo el mundo desde al menos 2014. El grupo ha atacado a una variedad de sectores, llevando a cabo ataques a la cadena de suministro, aprovechando la relación de confianza entre las organizaciones para atacar a sus objetivos principales.

Dentro de las recomendaciones del informe, sugiere ajustar la estrategia de gestión de riesgos teniendo en cuenta las tendencias del último semestre de 2023 para priorizar e implementar medidas de seguridad acordes dentro del alcance de cada organización. Sugiere, además, que se tenga en cuenta la previsibilidad que el informe está presentando con el fin de asignar recursos para mitigar la zona roja de cada organización. También se recomienda un programa activo de parches y actualizaciones.

Al final del informe indica que la inteligencia compartida es una parte fundamental para asegurar respuestas precisas y oportunas cuando los ciber atacantes efectúan sus ataques.

Destacando la importancia de que entre más exista colaboración entre los sectores público y privado, más efectivas pueden ser las respuestas para interrumpir la persistencia dentro de los ambientes de negocio por parte del cibercrimen.

Respuesta a Incidentes Gobierno

CSIRT Gobierno

El propósito principal del CSIRT Gobierno de acuerdo con (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023) es brindar servicios de gestión de seguridad proactivos, reactivos y básicos a todas las agencias gubernamentales, generar alertas sobre amenazas y vulnerabilidades, manejar el procesamiento, análisis, respuesta a incidentes y se trata de realizar ajustes, fortalecer el conocimiento de seguridad, y fortalecer los conocimientos sobre seguridad.

El objetivo es poder establecer de manera clara una cultura de seguridad digital entre todos los funcionarios y responsables de la seguridad digital, una colaboración entre el CSIRT Gobierno y la entidad, con el CSIRT Gobierno apoyado en el equipo técnico y la experiencia de la entidad en caso de incidente.

Los CSIRT gubernamentales acompañan y apoyan a las entidades estatales a través de una cartera de servicios para mejorar los procesos de seguridad de la infraestructura tecnológica, gestionar incidentes cibernéticos y crear conciencia sobre la seguridad digital.

Está formado por un grupo de expertos técnicos que implementan y desarrollan medidas para prevenir y responder a incidentes cibernéticos.

Los servicios prestados por el CSIRT gobierno incluyen servicios proactivos, servicios reactivos y servicios de gestión de calidad de la seguridad.

Servicios Proactivos

El objetivo es mejorar los procesos de seguridad de su infraestructura tecnológica con el fin de prevenir incidentes de seguridad digital y reducir su impacto y magnitud cuando ocurren.

Alertas y Generación de Alertas: Difundir información sobre amenazas y vulnerabilidades digitales para que se tomen medidas de emergencia o ajustes en la infraestructura técnica para evitar que ocurra el riesgo.

Difusión de información relacionada con la seguridad: Difusión de información relevante sobre nuevas tecnologías, soluciones, concientización y temas generales relacionados con la seguridad digital.

Esto permite a los CISO y líderes de seguridad generar conocimientos, habilidades, capacidades y destrezas.

Análisis de vulnerabilidad web, escanea los portales web gubernamentales en busca de vulnerabilidades y realiza ajustes y mitigaciones para evitar la explotación.

Monitoreo de eventos de seguridad basados en la infraestructura TI empresarial: Revisión de alertas de seguridad digitales y alertas resultantes de la correlación de registro de eventos (logs) de la plataforma de seguridad para generar alertas.

Monitoreo del portal WEB en el dominio GOV.CO: Monitorea la disponibilidad del portal web e informa cualquier degradación del servicio al administrador del portal para que el administrador del portal pueda tomar las acciones necesarias para restaurar el servicio.

Servicios reactivos, que apoyan la gestión, procesamiento y disposición de evidencia de incidentes cibernéticos en infraestructura tecnológica.

Gestión de Incidentes, que permite soporte y asesoramiento en caso de un incidente de ciberseguridad en todas las etapas de la gestión de incidentes: detección, evaluación, análisis, notificación, contención, remediación y recuperación.

Coordinar tareas de respuesta entre entidades y sitios involucrados en ataques, partes que brindan soporte de TI, proveedores de servicios de Internet, otros CSIRT (colCERT CCOCI CECIP), administradores de redes y sistemas, y para: llevar a cabo las actividades que ha realizado.

Intercambio y análisis de información Análisis de malware: esto incluye conocer los indicadores de compromiso de una amenaza para identificar contramedidas apropiadas y permitir que los proveedores de herramientas de seguridad generen firmas para eliminar la amenaza.

Servicios de gestión de calidad de la seguridad, estos aumentarán la conciencia sobre la seguridad digital, particularmente la concienciación sobre el riesgo y las amenazas cibernéticas entre los funcionarios, y proporcionarán conocimientos, habilidades, capacidades y habilidades a los CIO y CISO empresariales para construir una cultura de notificación y gestión de incidentes.

Colcert

Según (ColCERT, s. f.) el Grupo de Respuesta a Ciberemergencias de Colombia – COLCERT por disposición del Mintic del Gobierno Nacional, Resolución N° 473 del 17 de

febrero de 2022 adiciona al artículo 1 de la Resolución 002108 de 2020 el Grupo Interno de Trabajo en Ciberemergencia en Colombia.

Colombia – COLCERT, bajo la jurisdicción del Viceministerio para la Transformación Digital, continuará aclarando y coordinando a nivel nacional los aspectos de ciberseguridad de todos los sectores públicos y privados del país.

El COLCERT en su página oficial publica boletines relacionados con alertas de seguridad o vulnerabilidades de manera semanal, advertencias de seguridad, así como también cuenta con enlaces para reportar incidentes de ciberseguridad por parte de las entidades del sector público y privado en Colombia. Cuenta con procedimientos a seguir en caso de un incidente de ciberseguridad dependiendo su nivel de severidad, los canales de atención y los criterios para activar el equipo de respuesta de incidentes CSIRT para la contención, erradicación y mitigación de los incidentes de ciberseguridad.

DESARROLLO DE LOS OBJETIVOS

Indagar sobre el uso de marcos de trabajo en la gestión de riesgos de ciberseguridad en organizaciones estatales colombianas del sector salud, mediante la identificación de sus principales componentes y la comparación con estándares internacionales.

¿Como se realiza la gestión de riesgos de seguridad de la información en entidades públicas?

El propósito de la gestión de riesgos es la creación y la protección del valor. en este caso el valor es la información de la Entidad, por medio de la gestión de riesgos y realizándola de una manera adecuada se mejora el desempeño, fomenta la innovación y contribuye al logro de objetivos de las Entidades.

Principios de la gestión de riesgos

La creación y protección de valor maneja principios los cuales se describen en la siguiente figura:

En la figura a continuación se puede apreciar los principios de la creación y protección del valor tomada de la norma ISO 31000, conformada por 8 componente que aportan de manera integral al desarrollo de esta.

Figura 4

Principios de Creación y Protección del Valor

Nota. Gestión del riesgo - Directrices. Organización Internacional de Normalización. Tomado de ISO 31000:2018.

Una gestión de riesgos efectiva debe cumplir con los principios:

- ✓ Integrada, la gestión de riesgos debe hacer parte de todos las actividades e la entidad.
- ✓ Estructurada y exhaustiva, una adecuada estructura en la gestión de riesgos permite resultados coherentes y comparables

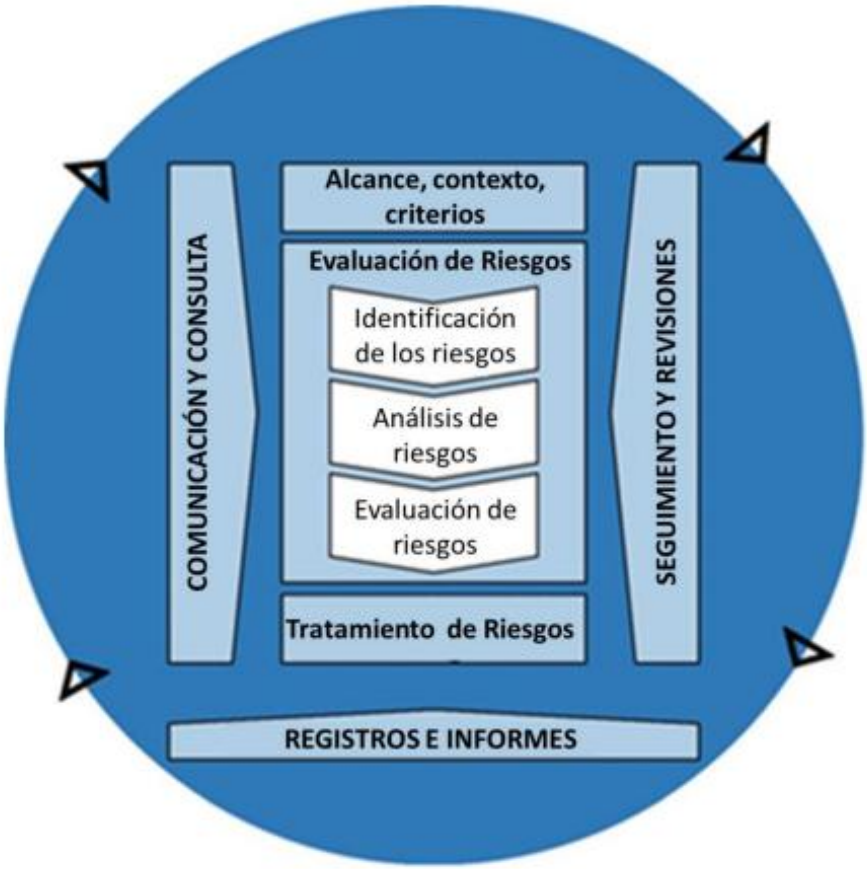
- ✓ Adaptada / Ajustada: la gestión de riesgos se adapta y son proporcionales a las Entidades.
- ✓ Inclusiva: La participación apropiada de todos los involucrados en los procesos. Permite puntos de vista y perspectivas diferentes.
- ✓ Dinámica: Los riesgos aparecen, cambian o desaparecer con los cambios de los contextos interno y externo de la organización. La administración/gestión de riesgos anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- ✓ Mejor información disponible. Se basan en información histórica y actualizada, la información debe ser clara y oportuna.
- ✓ Factores humanos: se refiere a la influencia de la parte humanan en la gestión de riesgos
- ✓ Mejora Continua: todo está en evolución, incluyendo la gestión de riesgos y con cada experiencia se puede mejorar más y más.

Proceso de la gestión de riesgos

El proceso de gestión de riesgos ilustrado en en la siguiente figura, establece las diferentes etapas alcance, evaluación y tratamiento del riesgo, así como también actividades transversales como la comunicación y consulta, registros e informes y seguimiento y revisiones:

Figura 5

Proceso de Gestión de riesgos



Nota. Gestión del riesgo - Directrices. Organización Internacional de Normalización. Tomado de ISO 31000:2018.

Comunicación y consulta: Su finalidad es apoyar a las partes interesadas para que puedan comprender los riesgos, se basa en la comunicación para lograr concientización y la comprensión de los riesgos y la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

Para las entidades públicas es de gran importancia este punto debido a que son entidades grandes y la comunicación no siempre es la más asertiva, lo que se logra con este punto es lograr una sinergia en los equipos con el fin de, mejorar respecto a la comunicación y poder tomar la mejor decisión ante cualquier problema que se pueda presentar.

Este punto es transversal a todo el proceso de la gestión de riesgos ya que es necesario en cada uno de los pasos y es vital lograr alcanzar el objetivo de tener una comunicación asertiva y una consulta definida:

Donde se pretende:

- ✓ Reunir varias áreas experimentadas en cada una de las etapas del proceso.
- ✓ Asegurar que todas las opiniones sean tenidas en cuenta y analizadas.
- ✓ Proporcionar suficiente información que permita una toma acertada de decisiones.
- ✓ Construir sentido de inclusión y propiedad para los afectado por los riesgos.

Alcance, contexto y criterios: Es vital que las organizaciones definan el alcance de manera clara y objetiva teniendo en cuenta las siguientes consideraciones

- ✓ Objetivos y decisiones claras.
- ✓ Resultados esperados de cada una de las etapas.
- ✓ El tiempo, la ubicación, las inclusiones y las exclusiones.
- ✓ Las herramientas y las técnicas para la de evaluación de riesgos.
- ✓ Los recursos requeridos, responsabilidades y registros a conservar.
- ✓ las relaciones que se tienen con otros proyectos, procesos y actividades.

Los contextos interno y externo: El contexto del proceso de la gestión de riesgos se debe establecer a partir de la comprensión de los entornos interno y externo en las Entidades.

Un contexto bien establecido es de gran importancia porque dada la misión, visión, estructura organizacional, objetivos estratégicos de gobierno y gestión, las actividades asociadas a los diferentes procesos de las entidades, la gestión de riesgos esta interrelacionada con los objetivos de las entidades de acuerdo a los recursos destinados para tal fin.

La importancia de la comprensión de contexto:

- ✓ contexto de los objetivos y las actividades de la entidad hacen parte de la gestión de riesgos.
- ✓ los factores organizacionales pueden ser una fuente de riesgos.
- ✓ propósito y alcance del proceso están dentro de la gestión de riesgos ya que permiten alcanzar los objetivos de las entidades.

Definición de los criterios para riesgos: Las Entidades públicas a nivel nacional deben definir los riesgos que están o no dispuestas a tomar con relación a los objetivos, La definición de los criterios de los riesgos deben estar acordes a los objetivos y recursos de la organización, también deben ser coherentes con las políticas y declaraciones de la gestión de riesgos.

Para el establecimiento de los criterios se tiene las siguientes consideraciones:

- ✓ lo tangible y lo intangible que puede afectar los resultados y los objetivos.
- ✓ Definir y medir consecuencias positivas y negativas.
- ✓ Todo lo relacionado del tiempo que va a tomar el desarrollo de la gestión de los riesgos.
- ✓ El cómo determinar el nivel de los riesgos.
- ✓ La capacidad de cada una de las Entidades.

Evaluación de riesgos, es el proceso que comprende de identificación, análisis y evaluación.

Identificación de riesgos Su objetivo principal es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos, para esto se necesita contar con una información apropiada y actualizada.

Para Hacer una adecuada identificación de riesgos se deberían de considerar los siguientes factores:

- ✓ Los riesgos tangibles e intangibles.
- ✓ las causas y los eventos que los produjeron.
- ✓ las amenazas y las oportunidades a las que haya lugar.
- ✓ que vulnerabilidades y que capacidades puedan existir.
- ✓ los cambios en los contextos interno y externo.
- ✓ Indicadores de riesgos emergentes.
- ✓ la naturaleza y el valor de los activos y los recursos.
- ✓ las consecuencias y sus impactos sobre objetivos de la entidad.
- ✓ las limitaciones de conocimiento y la confiabilidad de la información.
- ✓ Para una Entidad no siempre es fácil la identificación de los riesgos, algunas veces debido a la falta de compromiso de los funcionarios de la entidad, o que simplemente no ven la importancia de identificar los riesgos a tiempo.

Análisis de riesgos: Los activos de TI de las entidades públicas pueden tener dentro de su infraestructura tecnológica vulnerabilidades conocidas potencialmente explotables, es por esto, que es necesario desarrollar estrategias que los identifiquen, con el fin de poder detectar los riesgos y vulnerabilidades que puedan afectar la triada de la seguridad de la información.

El análisis de riesgos se realiza dependiendo del grado de detalle y complejidad, dependiendo del propósito del análisis, la disponibilidad y la confiabilidad de la información y los recursos disponibles. Las técnicas de análisis pueden ser cualitativas, cuantitativas están dependen del momento en que toque usarlas.

Para resumir el análisis de riesgos es un proceso sistemático y metodológico, utilizado para atribuir o determinar el valor de las dimensiones de los riesgos a los que está expuesta una Entidad. El Análisis del riesgo debe lograr determinar cuáles son las principales actividades más apropiadas, rentables y eficientes para ejecutar el análisis de forma cuantitativa o cualitativa.

Enfoque cuantitativo: Este enfoque se basa en un enfoque o modelo matemático y estadístico para la toma de decisiones.

Ventajas del enfoque cuantitativo:

- ✓ Proporciona diferencias y semejanzas entre vulnerabilidades
- ✓ Soporta de forma numérica las opiniones fundamentadas por los empleados de la organización
- ✓ Permite justificar la aplicación de medidas de gestión de riesgos.

Desventajas del enfoque cuantitativo:

- ✓ Su metodología es estándar, para que proporcionen resultados producto de la aplicabilidad de cierto nivel metodológico y con datos corroborables.
- ✓ Este tipo de estudios debe ser realizado por profesionales especializados, el ejercicio de esta actividad requiere de experiencia y entrenamiento, el no contar con profesionales calificados se considera un aspecto desfavorable.

Como conclusión este tipo de enfoque es objetivo, y se basa en los resultados.

Enfoque cualitativo: Se fundamenta en el argumento del analista o del funcionario designado para calcular las pérdidas potenciales, sin la necesidad de manejar ningún método probabilístico.

El enfoque cualitativo es el más utilizado para realizar el análisis de riesgos, suele utilizarse cuando el nivel de riesgo no es elevado o cuando los datos numéricos no son adecuados para una correcta estimación del riesgo. (Chicano Tejada, 2014)

Ventajas del enfoque cualitativo

- ✓ Se orienta primordialmente en la identificación de los eventos que ya han sucedido.

Desventajas del enfoque cualitativo

- ✓ Está en manos de la calidad profesionalidad y habilidad de los participantes que están realizando el Análisis de riesgos.
- ✓ Demanda la opinión e intervención de un profesional.
- ✓ Según el nivel de conocimientos del profesional, es posible que se pasen por alto riesgos importantes desconocidos.
- ✓ Identifica los eventos con mayor claridad, pero no puede determinar la probabilidad real de ocurrencia, conocimiento, habilidad y su formación para valorar las probabilidades de riesgo en la organización.

En resumen, para realizar análisis de riesgos se requiere de profesionales altamente calificados, con el fin de que los resultados sean de alta calidad.

Los pasos siguientes son los pasos generales de un análisis de riesgo, pueden variar ligeramente dependiendo de la metodología que se aplique:

Paso 1: Identificar los activos y la valoración mediante la confidencialidad, integridad y disponibilidad.

Paso 2: Identificar las amenazas, cuando se reduce la integridad, confidencialidad y disponibilidad de un activo, con qué frecuencia o probabilidad puede suceder las amenazas.

Paso 3: Determinar las salvaguardas que posee la organización y su capacidad para producir el efecto deseado.

Paso 4: Identificar el impacto, al activo por la ejecución de una amenaza.

Paso 5: Determinar el riesgo, o la cantidad de daño que probablemente tenga el activo.

Tratamiento de los riesgos

El objetivo del tratamiento de los riesgos es seleccionar e implementar opciones para abordar los riesgos.

El siguiente es el proceso de tratamiento de los riesgos:

Opciones para el tratamiento de los riesgos:

- ✓ Evitar el riesgo.
- ✓ Aceptar o evitar este riesgo.
- ✓ Eliminar la fuente de riesgo.
- ✓ Modificar las probabilidades.
- ✓ Modificar las consecuencias.
- ✓ Transferir el riesgo.
- ✓ Retener el riesgo.

Planear e implementar el tratamiento de los riesgos:

El propósito de los planes para el tratamiento de los riesgos es especificar el cómo se implementarán las opciones elegidas para el tratamiento.

La información proporcionada en los planes de tratamiento debiera incluir:

La selección de las distintas posibilidades para el tratamiento de los riesgos, incluyendo los beneficios esperados, las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan, las acciones propuestas los recursos necesarios, las contingencias, las medidas de desempeño, las restricciones, los reportes y seguimientos requeridos y por último los plazos previstos para la realización y la finalización de las acciones.

Evaluar la efectividad de dicho tratamiento: En este paso y según los resultados se sabrá qué tan eficientes han sido los tratamientos sobre los riesgos de seguridad.

Decidir si los riesgos residuales son aceptables y si no son aceptables, efectuar algún tratamiento adicional: En este paso se decide si es factible seguir con los riesgos residuales o volver a tratarlos.

Registros e Informes:

La gestión realizada se debe documentar e informar a través de los mecanismos apropiados.

Los registros y reportes pretenden:

Informar de las diferentes actividades de la gestión de riesgos y sus resultados a los miembros que se requiera dentro de la Entidad

Brindar información para la toma de decisiones

Mejorar las actividades de la administración gestión de riesgos.

Apoyar en la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión de riesgos.

¿Qué dice MINTIC acerca de la gestión de riesgos de seguridad de la información?

La información que maneja una entidad pública es uno de los principales insumos para el desarrollo de sus operaciones, esencialmente en el sector público la transaccionalidad de esta

puede generar ganancias o perdida de recursos de acuerdo con el manejo oportuno o no que se le dé a esta, ya que la fuente de mucha información pública y privada proviene de los ciudadanos y los activos necesarios para la operación de actividades de diferentes sectores económicos a nivel nacional.

En el anexo técnico 4 Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021) se especifica las diferentes etapas para integrar el Modelo de privacidad y seguridad de la información procedente de la misma entidad, se designa una hoja de ruta para las organizaciones del sector público en Colombia, en este documento se resalta la importancia sobre la aprobación de estos lineamientos por parte del Comité Institucional de Coordinación de Control Interno.

En la Guía para la Gestión y Clasificación de Activos de Información del (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016b) se establece los criterios de clasificación para los activos de información, es de anotar que esta valoración queda a potestad de la entidad dado el nivel de importancia que maneje cada activo de información, ya que para una organización puede ser muy valioso un activo de información y para otra puede que no tenga el mismo valor, o después de un plan de tratamiento de riesgos se opte por prescindir de un activo de información.

De esta manera MINTIC relaciona los niveles de clasificación de los activos de información con relación a la triada de seguridad de la información, como se puede evidenciar en la imagen a continuación.

Figura 6

Clasificación de la Información

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Nota. Clasificación de la información basada en los niveles de confidencialidad, integridad y disponibilidad. Tomado de MINTIC.

Tal cual como aparece en la figura 6 relaciona la clasificación de la información de acuerdo con niveles de severidad.

En la figura a continuación se puede observar el nivel de criticidad de los activos de información (ALTA, MEDIA, BAJA) junto con sus respectivas definiciones previamente establecidas por parte de MINTIC.

Figura 7

Criticidad de los Activos de Información

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Nota. Niveles de clasificación para activos de información según confidencialidad, integridad y disponibilidad. Tomado de MINTIC.

Esta clasificación de los riesgos permite atacar primero los riesgos clasificados como altos, esto con el fin de dar solución a los que ponen más en peligro los activos de las entidades.

Etapas para la gestión de los riesgos en la seguridad de la información

- ✓ Compromiso de las alta y media dirección: Es importante que la alta gerencia este comprometida con el fin de garantizar en gran medida el éxito de cualquier proceso emprendido.
- ✓ Conformación de un Equipo MECI o de un grupo interdisciplinario, el objetivo es lograr una integridad en el tratamiento de riesgos, poder tener un aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el Modelo de seguridad y privacidad de la información, se hace supremamente importante incluir los riesgos de

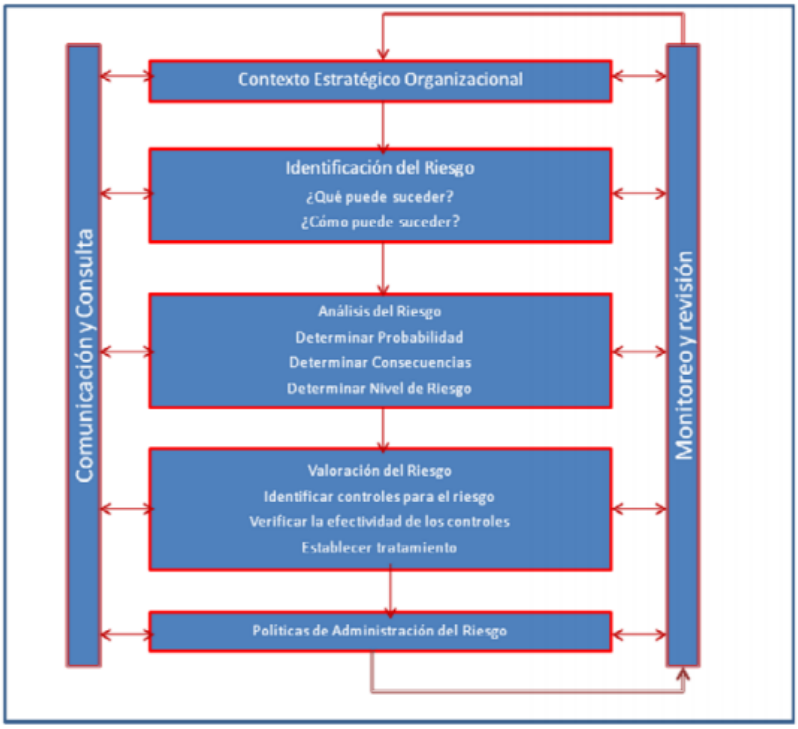
seguridad en el momento que se hace el análisis para el MECI, o para el modelo de Gestión de Calidad.

- ✓ Capacitación en la metodología: El equipo interdisciplinario debe estar capacitarse para poder analizar ahora los riesgos de seguridad, sin embargo, dicho equipo debe estar integrado por alguno de los integrantes del proyecto MSPI.

Administración del riesgo de seguridad de la información, el proceso de gestión de riesgo en la seguridad de la información está conformado por un enfoque organizacional con el fin de valorar el riesgo y su posterior tratamiento.

Figura 8

Proceso Para la Administración de Riesgos de la ISO 31000



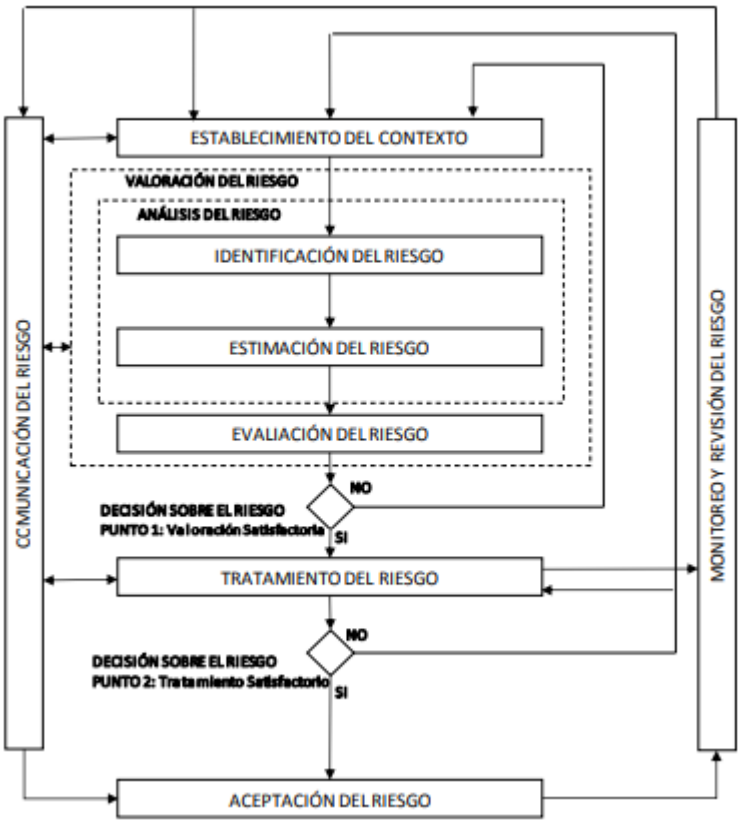
Nota. Diagrama proceso marco para la administración y gestión del riesgo, incluyendo sus fases clave y elementos de apoyo. Tomado de la Cartilla de Administración de Riesgos del DAFP.

La Figura 5 plasma el flujo del proceso para la gestión de riesgos, donde se tiene el paso a paso y los involucrados para poder llegar a una adecuada gestión de riesgos, también se encuentra este mismo proceso en la norma ISO/IEC 31000, explicada en el desarrollo del objetivo uno de este documento.

En el modelo de seguridad y privacidad de la información, también se menciona los lineamientos de la ISO 31000 y entre otras como la metodología Margerit.

Figura 9

Gestión de riesgos de la ISO 27005



Nota. *Gestión de riesgos* - Diagrama de Flujo de actividades en la gestión de riesgos. Tomado de Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Guía 7.*

En la Guía 7: Gestión de riesgos del (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016a) se indican los procesos para realizar la gestión de riesgos de seguridad de la información, donde gracias a su enfoque se valora el riesgo a profundidad, como primer paso es primordial definir el contexto, luego se realiza la valoración del riesgo y sigue el tratamiento del riesgo.

Si este proceso llegara a no ser suficiente, se llevará a cabo otra iteración de la valoración del riego con un contexto con el fin de mitigar al máximo los riesgos residuales, la eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo.

En la siguiente tabla se observan las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI:

Tabla 1

Actividades de Gestión de Riesgos MSPI

Etapas del MSPI	Proceso de gestión de riesgo en seguridad de la información
Planear	Establecer el contexto, valoración del riesgo, planificación del tratamiento del riesgo y aceptación del riesgo.
Implementar	Implementación del plan de tratamiento del riesgo
Gestionar	Monitoreo y revisión continua de riesgos.
Mejora Continua	Mantener y mejorar el proceso de gestión de riesgos en seguridad de la información.

Nota. Adaptado de Ministerio de Tecnologías de la Información y las Comunicaciones, (2021b). Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas. - etapas del MSPI.

Marcos y Referentes Internacionales

Requisitos de ciberseguridad Compuestos

En la publicación de la revista académica Advances in Multidisciplinary and scientific Research Journal (Yamcharoen et al., 2023) dice que el sector de la salud se enfrenta a desafíos cada vez mayores en materia de ciberseguridad debido a la rápida digitalización de los sistemas de atención de la salud y a la creciente dependencia de las tecnologías conectadas, y que entre los principales desafíos se encuentran:

- ✓ Aumento de las amenazas cibernéticas como ransomware, phishing y robo de datos.
- ✓ Complejidad de los sistemas de atención de la salud con muchos dispositivos, redes y aplicaciones interconectados.
- ✓ Falta de concienciación y formación en ciberseguridad entre los profesionales sanitarios.
- ✓ Medidas de ciberseguridad inadecuadas debido a limitaciones presupuestarias y prioridades en competencia.
- ✓ Desafíos del cumplimiento normativo en la gestión de riesgos de ciberseguridad.

Plantea una revisión con el fin de:

Identificar y analizar los requisitos, estándares, marcos, regulaciones y pautas de ciberseguridad existentes para la atención médica.

Evaluar las lagunas, limitaciones e incoherencia en los enfoques actuales de la ciberseguridad en la atención de la salud.

Proponer el desarrollo de un conjunto compuesto de requisitos de ciberseguridad adaptados a las organizaciones de atención médica.

Destacar los beneficios de un enfoque conjunto de la ciberseguridad en la atención de la salud.

Describir la metodología y el enfoque para desarrollar el marco de requisitos de ciberseguridad compuesto.

La revisión proporciona una descripción general de los estándares y marcos de ciberseguridad relevantes para la atención médica, incluidos HIPAA, NIST system, NIST SP 800-53, ISO 27001/27002, CIS Controls y HITRUST CSF.

El concepto de un marco de "requisitos de ciberseguridad compuestos", integra elementos de diferentes normas y directrices en un marco coherente y adaptable diseñado específicamente para las organizaciones de atención de la salud, este enfoque tiene como objetivo:

- ✓ Aprovechar las fortalezas de múltiples estándares y marcos.
- ✓ Simplificar la gestión del cumplimiento normativo.
- ✓ Permitir un enfoque más sistemático y ponderado en función del riesgo para la ciberseguridad.
- ✓ Fomentar la coherencia y la interoperabilidad entre los sistemas de atención de la salud y las partes interesadas.

La metodología propuesta para desarrollar el marco de requisitos compuestos de ciberseguridad implica:

- ✓ Revisión exhaustiva de la literatura de fuentes relevantes.
- ✓ Identificar y evaluar los estándares, marcos y mejores prácticas de ciberseguridad existentes.

- ✓ Interactuar con partes interesadas clave (expertos en ciberseguridad, profesionales de la salud, formuladores de políticas, líderes de la industria) para obtener aportes y perspectivas.

La revisión realiza la descripción de la implementación de los requisitos compuestos de ciberseguridad en la atención médica, incluidos:

- ✓ Realizar una evaluación de riesgos principalmente utilizando el proceso de gestión de riesgos del NIST.
- ✓ Hacer cumplir las normas de seguridad de HIPAA y otros requisitos reglamentarios
- ✓ Implementar controles de seguridad como gestión de acceso, cumplimiento del flujo de información, registro de auditoría, monitoreo continuo y capacitación en concientización sobre ciberseguridad.

La revisión concluye recomendando que las organizaciones de atención médica desarrollen un proceso fundamentalmente de evaluación de ciberseguridad, mantengan una plantilla de control actualizada e inviertan en un programa eficaz de concientización sobre ciberseguridad para garantizar la implementación exitosa del marco compuesto de ciberseguridad.

CIS Controls

De acuerdo con CIS Center for Internet Security (*CIS Critical Security Controls FAQ*, s. f.), CIS controls son un conjunto de acciones recomendadas para la ciberdefensa que proporcionan formas específicas y viables de frustrar los ataques más generalizados. Los controles del CIS son una lista relativamente corta de acciones defensivas de alta prioridad y altamente efectivas que proporcionan un punto de partida “imprescindible y que hay que hacer primero” para todas las empresas que buscan mejorar su ciberdefensa.

En (Gros, 2021) el artículo "Una visión crítica de los controles CIS", se describe de manera general los controles del CIS que son un conjunto de controles que se dividen en tres grupos: básicos, fundamentales y organizativos, que a su vez se subdividen en subcontroles, con el objetivo de proporcionar un conjunto priorizado de acciones para protegerse contra los ataques de ciberseguridad más comunes y dañinos.

Este marco de trabajo ofrece múltiples beneficios en ciberseguridad cuando se implementa correctamente estos Controles de Seguridad de Internet (CIS Controls).

Aborda 18 controles y 153 subcontroles con el objetivo de gobernar desde el ámbito de la ciberseguridad el conjunto de medidas de seguridad que debería de tener una organización, todo esto en diferentes grados de implementación.

Los grupos de implementación en CIS son una línea sobre la cual se puede priorizar los diferentes controles de seguridad críticos de este framework.

Grupo de Implementación 1: Según información de la página oficial de CIS, (*CIS Critical Security Controls Implementation Group 1*, s. f.), los controles CIS v8 y v8.1 definen el grupo de implementación 1 (IG1) como higiene cibernética esencial y representan un estándar mínimo emergente de seguridad de la información para todas las empresas. IG1 es la vía de acceso a los controles CIS y consta de un conjunto básico de 56 salvaguardas de defensa cibernética. Las salvaguardas incluidas en IG1 son las que todas las empresas deberían aplicar para defenderse de los ataques más comunes.

La higiene cibernética esencial se refiere a las prácticas de seguridad básicas que todas las organizaciones deben implementar para proteger su infraestructura y datos de TI de amenazas comunes y evitar vulnerabilidades fácilmente explotables.

Así como la higiene personal básica previene problemas de salud, la ciberhigiene puede ayudar a prevenir riesgos de seguridad mediante la implementación de medidas de seguridad.

Grupo de Implementación 2: basado en (*CIS Controls Implementation Group 2*, s. f.) Los grupos de implementación (IG) son la guía recomendada para priorizar la implementación de los controles críticos de seguridad del CIS (controles CIS).

La IG2 consta de 74 salvaguardas adicionales y se basa en las 56 salvaguardas identificadas en el IG1.

Las 74 protecciones seleccionadas para IG2 pueden ayudar a los equipos de seguridad a hacer frente a una mayor complejidad operativa. Algunas protecciones dependerán de tecnología de nivel empresarial y de conocimientos especializados para su correcta instalación y configuración.

Grupo de Implementación 3: teniendo en cuenta (*CIS Controls Implementation Group 3*, s. f.) Los grupos de implementación (IG) son la guía recomendada para priorizar la implementación de los controles críticos de seguridad del CIS (controles CIS).

El IG3 está compuesto por 23 salvaguardas adicionales. Se basa en las salvaguardas identificadas en el IG1 (56) y el IG2 (74), lo que suma un total de 153 salvaguardas en los controles CIS v8 y v8.1.

Alineamiento con los Marcos de trabajo y normas más utilizadas en ciberseguridad.

Cis controls permite realizar el mapeo de los controles de seguridad frente a los marcos de trabajo y normas de ciberseguridad, permitiendo seleccionar y comparar las prácticas de seguridad de los CIS controls con relación a los diferentes estándares.

Health Information Trust Alliance (CSF HITRUST)

Según el sitio web oficial de Microsoft (Microsoft Compliance, 2023) HITRUST creado y mantenido por Common Security System (CSF), un marco certificable para ayudar a las organizaciones del sector de la salud y sus proveedores a demostrar su seguridad y cumplimiento de forma coherente y simplificada.

El CSF de HITRUST (NIST, s. f.) es un marco de seguridad integral y certificable diseñado para ayudar a las organizaciones a gestionar eficazmente el riesgo y cumplir con los requisitos de cumplimiento al manejar datos confidenciales.

Se integra y se adapta a múltiples regulaciones y estándares existentes como HIPAA, GDPR, NIST, ISO 27001, PCI DSS en diversas industrias como atención médica, finanzas, tecnología, comercio minorista, etc.

El marco proporciona un conjunto estructurado de 14 categorías de control con 49 objetivos de control y 156 especificaciones de control que cubren áreas como gestión de riesgos, control de acceso, respuesta a incidentes y entre otros.

Las organizaciones de atención médica son un foco importante debido a la HIPAA y la protección de la información médica protegida (PHI), pero el marco beneficia a cualquier organización que maneje datos confidenciales.

Los beneficios clave incluyen la estandarización para múltiples necesidades de cumplimiento, escalabilidad, gestión de riesgos de terceros, creación de confianza y credibilidad y ventaja competitiva.

Para la atención médica, proporciona una protección sólida de los datos de los pacientes, alineación regulatoria con HIPAA, aceptación de la industria, reducción del riesgo financiero y un camino hacia la mejora continua.

El CSF de HITRUST es un valioso marco de riesgo y cumplimiento, especialmente para el sector de la salud, que integra las mejores prácticas de seguridad y se adapta a las regulaciones clave en un enfoque integral y certificable.

Cyber Security Framework (CSF)

Según el artículo de (Udroiu et al., 2022), se busca mejorar la ciberseguridad de los sistemas médicos mediante la aplicación del marco de trabajo para la ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

En este documento, se propone utilizar el marco trabajo para la ciberseguridad del NIST como una guía, especialmente para gestionar los riesgos de ciberseguridad en entornos médicos.

Brinda recomendaciones sobre cómo realizar la adaptación del marco NIST a las necesidades específicas de los sistemas médicos, abogando por adoptar estos estándares y aplicar mejores prácticas reconocidas internacionalmente, como el marco de trabajo para la ciberseguridad NIST, para fortalecer la postura de ciberseguridad de la infraestructura crítica en la atención de servicios de salud.

En la publicación del Cybersecurity Framework (CSF) 2.0 del (National Institute of Standards and Technology, 2024) brinda información actualizada de este marco de trabajo.

Descripción General: el CSF ofrece una guía a las organizaciones sobre la gestión de los riesgos de ciberseguridad y brinda una taxonomía de resultados de ciberseguridad de alto nivel que puede utilizar cualquier organización.

El CSF no es una ley universal sobre cómo deben de lograrse los resultados, sin embargo, ofrece enlaces a recursos en línea que ofrecen orientación sobre prácticas y controles.

El CSF se puede utilizar para comprender, evaluar, priorizar y comunicar los esfuerzos en materia de ciberseguridad.

Núcleo: el núcleo consta de funciones (gobernar, identificar, proteger, detectar, responder, recuperar), categorías y subcategorías que detallan los resultados de la ciberseguridad.

Los resultados son neutrales en cuanto a sector, país y tecnología para brindar flexibilidad a las organizaciones.

Las funciones están interrelacionadas y deben abordarse simultáneamente.

Perfiles y niveles del CSF: los perfiles organizacionales describen la postura de ciberseguridad actual y futura de una organización utilizando los resultados principales.

Dando alcance a la forma en que una organización podría crear un Perfil Organizacional en el marco del NIST CSF 2.0 se resumen los pasos claves:

Delimitar el perfil organizacional: definir el alcance del perfil, documentando hechos y supuestos, puede enfocarse en toda la organización o en áreas específicas, como sistemas financieros o respuesta a ransomware.

Recopilar información: reunir datos relevantes como políticas, recursos, prioridades de gestión de riesgos, análisis de impacto, y estándares de ciberseguridad seguidos por la organización.

Crear el perfil organizacional: determinar la información a incluir, basándose en los resultados del CSF, considerar los riesgos actuales y un perfil comunitario como referencia para el perfil objetivo.

Analizar las brechas y crear un plan de acción: identificar diferencias entre el perfil actual y el objetivo (futuro), y desarrollar un plan de acción priorizado para cerrar esas brechas.

Implementar el plan y actualizar el perfil: ejecutar el plan para mejorar las deficiencias y avanzar hacia el perfil objetivo (futuro); se puede repetir este ciclo continuamente para asegurar mejoras continuas.

Los perfiles también pueden ser útiles para comunicar capacidades y expectativas de ciberseguridad a partes externas como socios y proveedores.

Los niveles se caracterizan por la rigurosidad con que se abordan las prácticas de gestión y gobernanza de riesgos de ciberseguridad de una organización, desde Parcial (Nivel 1) hasta Adaptativo (Nivel 4); es decir el nivel de implementación del CSF en una organización.

Figura 10

Niveles de Implementación de CSF 2.0

Nota. Niveles de madurez de implementación del CSF 2.0. Tomado de (National Institute of Standards and Technology, 2024).

La figura 10 permite identificar los niveles del CSF aplicables a los perfiles organizacionales, para caracterizar el rigor de las prácticas de gobierno y gestión de riesgos de seguridad cibernética de una organización.

Nivel 1 Parcial: la gestión de riesgos de ciberseguridad es casual y reactiva, las actividades de ciberseguridad no están bien coordinadas ni integradas en las operaciones organizacionales, la organización tiene una baja concienciación del riesgo y dependencia de procesos ad-hoc.

Nivel 2 Riesgos Informados: la organización gestiona los riesgos de ciberseguridad, pero no de manera holística, existen políticas y procedimientos formales para algunas áreas de ciberseguridad, pero no en toda la organización, se utilizan procesos para priorizar riesgos, aunque la integración completa de la ciberseguridad con los procesos de gestión de riesgos aún no se ha logrado.

Nivel 3 Repetible: las prácticas de ciberseguridad están formalmente documentadas, y la gestión de riesgos está integrada en las operaciones, se realizan mejoras continuas basadas en revisiones periódicas, la organización tiene procesos establecidos para abordar riesgos y manejar amenazas cibernéticas de manera repetitiva y coherente.

Nivel 4 Versátil: la organización no solo gestiona los riesgos de ciberseguridad de forma integrada y proactiva, sino que también adapta su postura de seguridad según el entorno de amenazas cambiante, la ciberseguridad es una parte clave de la cultura organizacional, con una gestión de riesgos dinámica y una respuesta continua a incidentes, se implementa un enfoque basado en el aprendizaje continuo y en la previsión de amenazas futuras.

Estos niveles permiten que una organización evalúe su madurez en la gestión de ciberseguridad y establezca objetivos claros para mejorar.

Recursos complementarios en línea: el NIST y otras organizaciones ofrecen una variedad de recursos en línea para ayudar a las organizaciones a adoptar y utilizar (CSF).

Entre los principales recursos se encuentran:

Referencias informativas: estas muestran las relaciones entre el núcleo del CSF y estándares, pautas, regulaciones y otros contenidos, ayudan a las organizaciones a cumplir con los resultados del CSF y pueden ser específicas de un sector o tecnología, algunas referencias se

enfocan en subcategorías particulares, mientras que otras cubren múltiples subcategorías a nivel de políticas.

Ejemplos de implementación: proporcionan pasos teóricos y orientados a la acción para alcanzar los resultados del CSF, aunque no son una lista exhaustiva, sugieren acciones como compartir, documentar, desarrollar, monitorear, evaluar y probar, estos ejemplos no representan una línea base, sino una guía sobre posibles acciones a tomar.

Guías de inicio rápido: son documentos breves y específicos, diseñados para audiencias particulares, que desglosan partes del CSF en "primeros pasos" prácticos, ayudan a las organizaciones a mejorar su postura de ciberseguridad y gestionar los riesgos, las guías se revisan periódicamente y se agregan nuevas según sea necesario.

Integración con otros sistemas de gestión de riesgos: el CSF se puede integrar con la gestión de riesgos empresariales (ERM) y otros programas de gestión de riesgos (por ejemplo, privacidad, cadena de suministro, tecnologías emergentes), lo cual permite gestionar los riesgos de ciberseguridad junto con otros riesgos organizacionales.

CSF proporciona un marco adaptable e integral para que las organizaciones comprendan, evalúen, prioricen y comuniquen sus esfuerzos en materia de ciberseguridad en el contexto de su misión, sus riesgos y las expectativas de las partes interesadas.

Health Insurance Portability and Accountability Act (HIPAA)

De acuerdo con (Edemekong et al., 2024) en la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) se estableció para proteger la privacidad y seguridad de la información médica protegida (PHI) y la información médica electrónica protegida (ePHI).

HIPAA cubre a proveedores de atención médica, planes de salud, centros de intercambio de información sobre atención médica y sus socios comerciales.

Norma de privacidad de HIPAA: regula el uso y la divulgación de PHI por parte de entidades cubiertas.

Requiere que las entidades cubiertas obtengan la autorización del paciente para la mayoría de las divulgaciones de PHI.

Otorga a las personas el derecho a acceder a su PHI y solicitar correcciones.

Norma de seguridad HIPAA:

Establece estándares para la seguridad de la ePHI, incluidas las salvaguardas administrativas, físicas y técnicas.

Requiere que las entidades cubiertas realicen evaluaciones de riesgos e implementen medidas de seguridad adecuadas.

Cumplimiento y sanciones de la HIPAA: establece sanciones civiles y penales por violaciones a la HIPAA.

El Departamento de Salud y Servicios Humanos investiga las quejas de HIPAA y hace cumplir su cumplimiento.

Las infracciones pueden dar lugar a multas que van desde 100 a 50.000 dólares por infracción, con máximos anuales de hasta 1,5 millones de dólares.

Importancia clínica y repercusiones:

La HIPAA ha tenido un impacto significativo en las operaciones, la investigación y los costos de la atención médica.

Los proveedores de atención médica deben recibir capacitación sobre los requisitos de HIPAA para evitar posibles violaciones.

Las restricciones de HIPAA han afectado la capacidad de realizar ciertos tipos de investigación médica.

Ejemplos de violaciones de HIPAA:

Acceso o divulgación no autorizados de PHI por parte de empleados de atención médica.

No implementar medidas de seguridad apropiadas para proteger la ePHI.

Eliminación inadecuada de PHI o dejarla sin supervisión en áreas públicas.

En conslusión, la HIPAA establece estándares integrales para la protección de la PHI y la ePHI, con importantes consecuencias legales y financieras en caso de incumplimiento, las organizaciones y los profesionales de la atención médica deben comprender y cumplir con los requisitos de la HIPAA para garantizar la privacidad y la seguridad de la información de los pacientes.

Essentials of Cybersecurity in Healthcare Organizations (ECHO)

De acuerdo con (O'Brien et al., 2021) estudio que destaca la creciente importancia de la ciberseguridad en el sector de la salud, debido al uso de tecnologías de la información y de las comunicaciones durante la pandemia de COVID-19 y el consiguiente aumento de los ciberataques dirigidos a organizaciones del sector salud, dado todos estos incidentes de ciberseguridad seguridad y las amenazas para la seguridad de los pacientes, la ciberseguridad en el campo de la salud esta atrasada en comparación con otras industrias.

Para abordar esta brecha, los investigadores llevaron a cabo el estudio Delphi en línea con 42 expertos en ciberseguridad tanto en informática y en Tecnologías de la Información y de las Comunicaciones de la salud de diferentes partes del mundo, con la finalidad de desarrollar un marco de preparación para la ciberseguridad aplicable globalmente y relevante para el sector salud.

Después de dos rondas, se llegó a un consenso sobre el marco en mención, que consta de 51 componentes agrupados en 6 categorías, así mismo, determinaron que este marco es una

herramienta de planificación aceptable para guiar la ciberseguridad en el sector de la salud a nivel mundial.

El aspecto fuerte de este estudio radica en la metodología Delphi utilizada para sacar provecho de los conocimientos del colectivo de expertos internacionales y desarrollar un marco adaptado a las necesidades únicas del sector de la salud a nivel mundial; el marco ECHO resultante puede ayudar a los formuladores de políticas y organizaciones de salud a fortalecer su postura de ciberseguridad y brindar una atención segura a la par con la efectividad de los servicios prestados.

Además (O'Brien et al., 2024) en su artículo evaluación de la viabilidad y usabilidad de un recurso de ciberseguridad en línea y fuera de línea para organizaciones de atención médica (recurso del marco de referencia Los aspectos esenciales de la ciberseguridad en las organizaciones de atención médica): estudio de métodos mixtos, y que tiene en cuenta a (ECHO) dentro de este, destaca aspectos claves como los relacionados a continuación:

La ciberseguridad es un desafío creciente para los sistemas de salud en todo el mundo, ya que la rápida adopción de tecnologías digitales ha generado mayores vulnerabilidades cibernéticas con implicaciones para los pacientes y los proveedores de salud.

Recalca que el marco de recursos Fundamentos de la ciberseguridad en las organizaciones de atención de la salud (ECHO) se desarrolló para brindar orientación a las organizaciones de atención de la salud sobre los elementos clave de la ciberseguridad, incluyendo sus seis dimensiones:

La figura a continuación muestra las seis etapas del marco que son: Contexto, gobernanza, estrategia organizacional, gestión de riesgos, concienciación, educación y capacitación, y capacidades técnicas.

Figura 11

Etapas ECHO

Nota. Diagrama circular sobre los seis elementos esenciales de la ciberseguridad según ECHO. Tomado de (O'Brien et al., 2024).

Gobernanza: se refiere a la estructura organizativa y los procesos necesarios para gestionar la ciberseguridad de manera efectiva.

Capacidades técnicas: incluye las herramientas y tecnologías necesarias para proteger la infraestructura de TI y los datos.

Estrategia organizacional: implica el desarrollo de políticas y estrategias que alineen la ciberseguridad con los objetivos generales de la organización.

Conciencia, educación y formación: se centra en la capacitación del individual y la creación de una cultura de ciberseguridad dentro de la organización.

Gestión de riesgos: trata sobre la identificación, evaluación y mitigación de riesgos relacionados con la ciberseguridad.

Colaboración y comunicación: enfatiza la importancia de la comunicación efectiva y la colaboración entre diferentes partes interesadas para mejorar la ciberseguridad.

Se realizó un estudio de métodos mixtos para evaluar la usabilidad y viabilidad del recurso del marco (ECHO) en el cual participaron 16 organizaciones de salud.

Conclusiones del estudio:

El recurso del marco (ECHO) fue bien aceptado y resultó útil para las organizaciones de salud, mejorando su comprensión de la ciberseguridad como área prioritaria, reduciendo amenazas y permitiendo la planificación organizacional.

No todos los participantes pudieron implementar completamente el recurso debido a desafíos como costos, limitaciones de recursos humanos, apoyo del liderazgo, participación de las partes interesadas y tiempo limitado.

Quienes implementaron el recurso lo consideraron útil para generar conciencia y fácil de usar debido a su familiaridad con otras normas y directrices.

Los participantes señalaron que varias secciones eran difíciles de poner en práctica, especialmente en torno a la gobernanza, la estrategia organizacional y la concientización, la educación y la capacitación.

El análisis de subgrupos mostró una tendencia hacia una menor percepción de utilidad del componente de concientización, educación y capacitación a lo largo del tiempo entre los participantes de países de ingresos bajos y medios.

La investigación identificó la aceptabilidad y utilidad del recurso del marco (ECHO) como un recurso de ciberseguridad centrado en la salud, se necesitan investigaciones futuras para

explorar cómo se puede actualizar e implementar en la práctica, y cómo se podrían desarrollar materiales educativos sobre diferentes aspectos.

Para resumir, el recurso del marco (ECHO) fue generalmente bien recibido, pero se identificaron desafíos de implementación relacionados con costos, recursos y factores organizacionales, particularmente para ciertos componentes como concientización y capacitación.

ISO 27001/27002

De acuerdo con (*ISO/IEC 27002*, s. f.) ISO/IEC 27002 es un estándar internacional que proporciona orientación para las organizaciones que buscan establecer, implementar y mejorar un sistema de gestión de seguridad de la información (SGSI) con un enfoque en la ciberseguridad.

Mientras que ISO/IEC 27001 describe los requisitos aplicables al SGSI, ISO/IEC 27002 proporciona mejores prácticas y se especifican directrices relacionadas con aspectos clave de la ciberseguridad, como el control de acceso, el cifrado, la seguridad del personal y la respuesta a incidentes.

Este estándar sirve como modelo práctico para las organizaciones que desean proteger eficazmente sus activos de información contra las amenazas cibernéticas.

Siguiendo las directrices ISO/IEC 27002, las organizaciones pueden adoptar un enfoque proactivo para la gestión de riesgos de ciberseguridad y proteger la información crítica contra el acceso no autorizado o su pérdida.

Comparativo de los Marcos de Trabajo

Estos marcos de trabajo conocidos por la comunidad en la industria son comúnmente adoptados por organizaciones alrededor del mundo, todo depende de las necesidades de cada

empresa y los recursos, compromiso con que cuente cada compañía. A continuación, se relaciona un comparativo entre los marcos de trabajo más utilizados, plasmando para cada uno de estos sus ventajas y desventajas, así:

Tabla 2

Comparativo Marcos de Trabajo y Estándares

Nombre	Ventajas	Desventajas
CSF NIST	Es flexible y escalable, puesto que se adapta a organizaciones de todos los tamaños e industrias, siendo de gran utilidad para pequeñas y grandes organizaciones. Propone un enfoque orientado a la gestión de riesgos lo cual permite a las diferentes organizaciones optar por priorizar los recursos destinados a la ciberseguridad en función de las amenazas y las vulnerabilidades específicas. También se caracteriza por ser un marco de trabajo claro y fácil de usar. Es compatible con otros marcos de trabajo como la ISO 27001 y Controles CIS, lo cual brinda facilidades entorno a la integración de iniciativas de cumplimiento. Es una guía considerada como de las mejores prácticas para la identificación, evaluación y mitigación de los riesgos para mejorar la postura general de seguridad.	No es un marco de trabajo certificable lo cual puede que sea una desventaja para las organizaciones este respaldo por temas de cumplimiento. Requiere recursos considerables para su implementación como tiempo, inversión presupuestal y personas capacitadas, lo cual para organizaciones pequeñas puede ser dispendioso. Pueden requerir de adaptaciones de acuerdo con las normas de privacidad de otros países diferentes a otros países diferentes a Estados Unidos país de procedencia del Marco de Trabajo.
CSF HITRUST	Fue diseñado específicamente para el sector de la salud y es ideal para organizaciones de este sector que requieran proteger la información médica y cumplir con regulaciones estrictas como HIPAA. Integra múltiples estándares y regulaciones como HIPAA, NIST, ISO, PCI-DSS y GDPR para crear un enfoque unificado de ciberseguridad y cumplimiento normativo. Esto reduce la carga de trabajo para las organizaciones que deben de cumplir con	Las organizaciones que quieran obtener esta certificación y el acceso a las herramientas y consultoría del CSF pueden requerir inversiones considerables que podrían no estar dentro del alcance de las pequeñas empresas. La posible redundancia de controles puede representar una lista de controles muy complicados de implementar

Nombre	Ventajas	Desventajas
	diversos estándares de cumplimiento. Los controles de seguridad son específicos para ayudar a las organizaciones a implementar medidas de seguridad detalladas, ideal para organizaciones que requieren pautas especificas en lugar de recomendaciones generales. Proporciona, además, un proceso de certificación que permite a las organizaciones evaluar de forma independiente su postura de seguridad, esta certificación sirve como prueba de diligencia ante clientes, reguladores y partes interesadas. Combina la gestión de riesgo con el cumplimiento normativo ofreciendo una metodología estándar para estos dos pilares del GRC.	convirtiéndose en controles interminables de implementar y auditar. Su enfoque al sector de la salud limita su campo de acción en otros sectores.
CIS Controls	Los controles CIS son de acceso gratuito accesibles para organizaciones de todos los tamaños. Son fáciles de interpretar, siendo los controles más comunes para mitigar amenazas. Se divide en diferentes grupos de implementación lo cual permite hacer evaluaciones de manera gradual comenzando por una serie de controlas básicos hasta terminar con controles más avanzados dependiendo del nivel de madurez en ciberseguridad de la organización. Se pueden alinear con diferentes marcos de trabajos y estándares lo cual provee de una estrategia de seguridad integral orientada al cumplimiento.	Puede no cumplir con salvaguardas contra amenazas avanzadas. A pesar de que son de fácil acceso para diferentes organizaciones, la implementación de los controles puede representar inversión de recursos y personal a una escala que organizaciones pequeñas no estén dispuestas a costear.

Nombre	Ventajas	Desventajas
HIPAA	Se pueden alinear con diferentes marcos de trabajos y estándares lo cual provee de una estrategia de seguridad integral orientada al cumplimiento.	Se pueden alinear con diferentes marcos de trabajos y estándares lo cual provee de una estrategia de seguridad integral orientada al cumplimiento.
ECHO	Se pueden alinear con diferentes marcos de trabajos y estándares lo cual provee de una estrategia de seguridad integral orientada al cumplimiento.	Es un marco de trabajo que fue implementado en unas pocas instituciones de salud, a pesar de que fue aceptado por varias organizaciones de salud, desde el ámbito de gobernanza muchas organizaciones no se alinearon con la ciberseguridad lo que impidió su implementación.

Analizar los casos de ciberataques presentados en el sector salud de Colombia con el fin de Identificar posibles vectores de ataque.

Casos de Ciberataques al sector salud en Colombia

Supersalud y Minsalud

El 19 de septiembre la (Super Intendencia Nacional de Salud, 2023), mediante circular externa 2023100000000014 informa, que tiene contratado con la firma IFX NETWORKS COLOMBIA S.A.S. el servicio de nube privada, de conformidad con el acuerdo marco vigente establecido entre dicha empresa y Colombia Compra Eficiente. También informa, que el 12 de septiembre de 2023, el proveedor de servicios IFX NETWORKS COLOMBIA S.A.S. quien prestaba los servicios de telecomunicaciones a la superintendencia de salud, emitió un

comunicado el cual decía de manera sucinta, que: "…el día de hoy a las 5:50 a.m. (GMT-5), la nube del proveedor multinacional para servicios de telecomunicaciones, IFX NETWORKS, con operaciones en 17 países de la región, sufrió un ataque de ciberseguridad externo tipo Ramsonware, afectando a algunos de sus máquinas virtuales." Este incidente denota la magnitud del ataque cibernético incluyendo organizaciones de carácter internacional; en el caso específico de la Supersalud se vieron afectados los servicios tecnológicos, causando indisponibilidad de los aplicativos webs de uso externo e interno, incluyendo su portal web. Por consiguiente, se instaló un Puesto de Mando Unificado adelantado entre el Equipo de Respuesta a Incidentes de Seguridad - CSIRT de la Presidencia de la República, Ministerio de Salud y Protección Social, el grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT del Departamento Administrativo de la Presidencia de la República y otras entidades afectadas con el ataque cibernético. El 22 de septiembre de 2023 la Superintendencia de salud informa sobre el restablecimiento de los servicios y aplicativos tecnológicos.

El Ministerio de Salud, el 13 septiembre el (Ministerio de Salud y Protección Social, 2023) comunica que, desde el día de martes 12 de septiembre de 2023, debido a un incidente de ciberseguridad en el Datacenter de su proveedor de servicios tecnológicos, donde se encuentran alojadas las aplicaciones misionales asociadas a la prestación de servicios derivados de la atención a nivel nacional, presentan fallas y no es posible acceder a ellas; indicando además, que las aplicaciones se encuentran alojadas en la infraestructura contratada con IFX Networks Colombia S.A.S, compañía que está adelantando el análisis y evaluación para determinar el tiempo de restablecimiento de los servicios y de la información que allí se encuentra. El 25 de septiembre de 2023, el Ministerio de Salud y Protección Social informa, que fueron restablecidos

en su totalidad los servicios y aplicativos tecnológicos y digitales a nivel interno y externo que resultaron afectados tras el ataque cibernético a la empresa IFX Networks el 12 de septiembre.

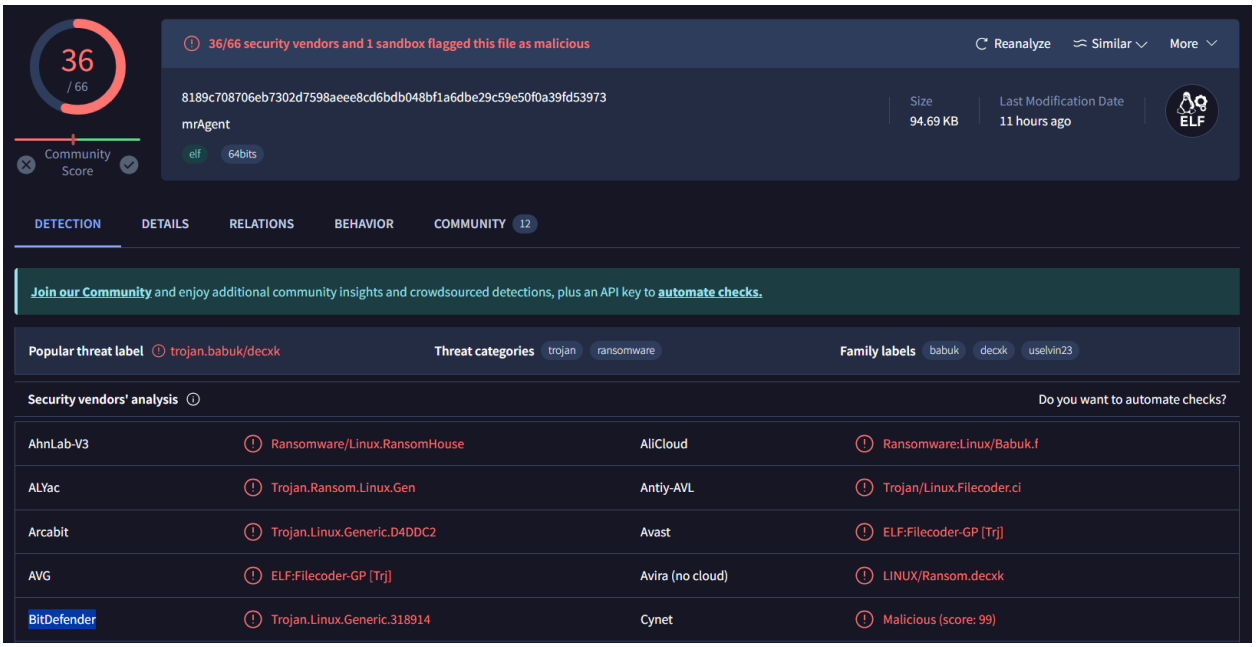
De acuerdo con (CSIRT, Coordinación Nacional de Ciberseguridad, Ministerio del Interior y Seguridad Pública, Gobierno de Chile, 2023), se describe de manera detallada los hallazgos realizados en el ramsomware en IFX teniendo en cuenta IoCs y contexto, Comandos C2, Rutinas ejecutadas y recomendaciones, el eje principal de todo este ataque giró en torno a un archivo malicioso denominado mrAgent el cual fue detectado por primera vez el 21 de septiembre del año 2023 a las 13:37:59 hora de Santiago de Chile según se relaciona en el informe.

Este archivo malicioso en la plataforma Hybrid Analysis tiene 6 indicadores que fueron asignados a 5 técnicas de ataque y 3 tácticas; y en la plataforma de virus total se evidencia que aplicaciones de antivirus consideran el archivo como malicioso.

En la figura a continuación se puede evidenciar el puntaje de la comunidad le da al archivo malicioso, el análisis de los diferentes proveedores de seguridad, etiquetado como de tipo trojano y ransomware y que es utilizado por lo general en sistemas operativos que están basados en Linux.

Figura 12

Captura Virus Total



Nota. Consulta de archivo malicioso en la plataforma Virus Total. Tomado de Virus Total.

El tiempo transcurrido de indisponibilidad de los servicios y aplicativos de las dos entidades fue de aproximadamente 10 días, esto impactó negativamente la prestación de los servicios de salud de los colombianos, ya que según describe (Rico, 2023) el Ministerio de Salud: le secuestraron la plataforma misional del Sistema Integrado de Información de la Protección Social (Sispro) y su aplicativo Mipres, donde los médicos ordenan medicamentos, tratamientos, cirugías, todo; por ello, el plan de contingencia ordenado por el ministro de Salud fue pedir a todas las EPS, hospitales, IPS y demás instituciones que volvieran al papel y lápiz para funcionar.

Según noticia de El Tiempo (*Ciberataque: el hombre detrás de IFX, la empresa que Colombia amenaza con demandar*, s. f.) Mauricio Lizcano, ministro de las TIC, reveló que ya habría datos de entidades colombianas en la Dark Web, a pesar de que IFX ha venido asegurando

que la información no ha sido saqueada de las plataformas. Por lo que la confidencialidad de la información también se estaría viendo afectada.

Riesgos asociados a los ciberataques teniendo en cuenta las amenazas y vulnerabilidades:

Ataque de ransomware: el ataque de ransomware a IFX Networks, un importante proveedor de servicios de telecomunicaciones, tuvo un impacto significativo en las operaciones de la Superintendencia Nacional de Salud y el Ministerio de Salud y Protección Social.

El ataque afectó a máquinas virtuales y provocó la indisponibilidad de aplicaciones web, servicios internos y externos y sitios web durante aproximadamente 10 días.

Esta interrupción afectó negativamente la prestación de servicios de salud a los ciudadanos colombianos, ya que las instituciones médicas tuvieron que volver a procesos manuales.

Confidencialidad y violación de datos: Según el ministro de las TIC, Mauricio Lizcano, hay indicios de que datos de entidades colombianas podrían haber sido filtrados a la Dark Web, pese a que IFX Networks asegura que la información no ha sido comprometida.

Esto genera preocupación por la posible violación de información confidencial, incluidos datos sensibles de la salud.

Vulnerabilidad a malware y ciberataques: el ataque de ransomware explotó vulnerabilidades en los sistemas de IFX Networks, permitiendo la implementación del archivo malicioso "mrAgent".

Este archivo fue detectado por virus total y plataformas de seguridad, lo que indica su naturaleza maliciosa y potencial para causar daño.

El ataque resalta la susceptibilidad de los proveedores de servicios e infraestructuras críticas a las ciber amenazas sofisticadas.

Dependencia de proveedores de servicios externos: tanto la Superintendencia Nacional de Salud como el Ministerio de Salud y Protección Social confiaron en IFX Networks para alojar sus aplicaciones y servicios.

Esta dependencia de un proveedor externo introdujo un único punto de falla, ya que el ataque de ransomware a IFX Systems afectó directamente las operaciones de estas entidades gubernamentales.

Respuesta a incidentes y planificación de contingencias: la respuesta al incidente involucró un Puesto de Mando Unificado establecido entre varias agencias gubernamentales, incluido el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y el Grupo de Respuesta a Emergencias (COLCERT).

Sanitas

De acuerdo a información suministrada por (Benito, 2023) en su artículo , informa sobre los últimos avances de un ataque de tipo ransomware en curso contra una importante empresa del sector salud Sanitas, donde se revela que se han filtrado más datos robados después de no recibir el pago del rescate.

El artículo proporciona antecedentes sobre el ataque inicial de noviembre de 2022, la respuesta de Sanitas y la participación de las autoridades de salud colombianas en la investigación del incidente, indicando, además, que el grupo de hackers RansomHouse, que violó el sistema de alojamiento de datos de Sanitas, Keralty, en noviembre de 2022, ha publicado más información clasificada de Sanitas.

También manifiesta que, RansomHouse publicó la mitad de los datos que robaron a Sanitas porque la empresa no ha pagado las exigencias de rescate y que RansomHouse anunció

esta última filtración a través de su canal de Telegram, además de que Sanitas no se ha pronunciado oficialmente sobre esta nueva filtración.

En el ataque de noviembre de 2022, RansomHouse robó datos confidenciales, incluidos registros de pacientes, información de empleados, registros de pagos e historias clínicas de Sanitas, los datos filtrados incluyen números de identificación, números de teléfono, direcciones, detalles de pago e información médica de pacientes y empleados de Sanitas.

Las investigaciones adelantadas por la propia EPS confirmaron que 241.589 usuarios de Sanitas vieron comprometida su información personal en la filtración, se sospecha que el ataque es un ataque de tipo ransomware.

Salud Total

Según la noticia o comunicado de prensa de Salud Total EPS (Diaz, 2024), informa sobre un ataque cibernético ocurrido el 27 de enero de 2024, proporciona detalles sobre el ataque, su impacto en las operaciones de la empresa y las medidas que se están tomando para enfrentar la situación.

Salud Total EPS sufrió un ciberataque externo el 27 de enero de 2024, lo que provocó la indisponibilidad de cierta información operativa.

La empresa siguió los protocolos establecidos, aislando los servicios de TI y las conexiones a servidores físicos y virtuales para salvaguardar la información y evaluar el estado actual de los activos de TI.

Manifiesta que, se están tomando acciones preventivas y reactivas para restaurar las aplicaciones relacionadas con las operaciones lo antes posible, también que, se ha implementado un plan de contingencia que incluye atención al cliente las 24 horas, los 7 días de la semana a

través de líneas telefónicas, horario extendido para asistencia en persona y desactivación temporal de canales virtuales como el portal en línea, la aplicación móvil y el asistente virtual.

Audifarma

El diario (S.A.S, 2023), proporciona una noticia o nota de prensa sobre Audifarma empresa farmacéutica, informando sobre un ciberataque que han sufrido y las medidas que están tomando para abordar la situación y restablecer sus servicios, sobre el ciberataque que sufrió Audifarma el 22 de enero de 2023.

Se menciona que Audifarma deshabilitó sus servidores físicos y virtuales para proteger la información de la organización y sus usuarios e indica que el sitio web y la aplicación de Audifarma se encuentran fuera de servicio debido al ataque.

También se informa que, la empresa ha implementado un plan de contingencia para continuar dispensando medicamentos en sus centros de servicio y que Audifarma está trabajando con empresas multinacionales de ciberseguridad para analizar sus sistemas y encontrar una solución para restablecer el servicio normal.

Se indica que la empresa destaca que cuentan con mecanismos de seguridad y respaldos para salvaguardar la integridad de la información y que han emprendido acciones legales contra el ciberataque, ya que condena este tipo de ataques a empresas del sector salud.

Invima

Según la información proporcionada por (Vásquez, 2022), en un artículo o noticia sobre un ciberataque de tipo ransomware al sitio web del Invima (Instituto Nacional de Vigilancia de Medicamentos y Alimentos), indica que delincuentes informáticos han cifrado sus sistemas y exigen un rescate multimillonario para restaurar el acceso.

Hackers han atacado el sitio web y los sistemas de Invima, cifrando sus datos y código, dejando inoperativas muchas de sus plataformas, exigen un rescate de 5 millones de dólares en criptomonedas para restaurar el acceso a los sistemas y datos del Invima.

No es la primera vez que el Invima enfrenta un ataque de este tipo. se precisa que, en el pasado, es decir en febrero de 2022, sufrieron un importante incidente de hackeo que los obligó a realizar procedimientos manuales y provocó retrasos en el registro de exportaciones e importaciones.

Francisco Rossi, director del Invima, aclaró que los hackers no robaron datos, sino que cifraron todo el código de programación y documentación del Invima, haciéndolo inaccesible para el instituto.

Rossi especuló que los piratas informáticos atacan instituciones como Invima para obtener publicidad, ya que estos ataques suelen aparecer en los titulares y algunas empresas privadas pagan los rescates exigidos, informa además sobre el incidente cibernético y la respuesta del Invima.

Vectores de Ataque

Los vectores de ataque asociados a cada uno de estos incidentes de ciberseguridad se encuentran asociados a los grupos Ransomhouse y Ra World.

Tabla 3

Vectores de Ataque Sector Salud

Entidad	Vector de Ataque
Supersalud y Minsalud	correo electrónico de tipo phishing.
	Explotación de vulnerabilidades conocidas.
	Uso de Malware.
	Escalada de Privilegios.
	Movimiento lateral.
	Ejecución.
	Exfiltración.
Sanitas	correo electrónico de tipo phishing.
	Explotación de vulnerabilidades conocidas.
	Uso de Malware.
	Escalada de Privilegios.
	Movimiento lateral.
	Ejecución.
	Exfiltración.
Salud Total	Correo electrónico de tipo phishing.
	Explotación de vulnerabilidades conocidas.
Audifarma	No se ha atribuido ataque a ningún grupo.

Entidad	Vector de Ataque
Invima	Explotación de vulnerabilidades conocidas: CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 presentes en el servidor de Microsoft Exchange del cliente. Una vez ejecutado, BlackByte elimina el Administrador de tareas (taskmgr) y el Monitor de recursos (resmon), posteriormente emite un comando ofuscado de PowerShell para detener el servicio de Windows Defender (WinDefend) A continuación, BlackByte realiza el reconocimiento de la red y la preparación del sistema antes del movimiento lateral dentro del entorno. Antes de realizar el cifrado, BlackByte emite varios comandos: El primer comando vssadmin resize shadowstorage, cambia el tamaño de almacenamiento de instantáneas. El segundo comando busca eliminar instantáneas directamente a través de objetos Usando WinRAR, BlackByte comprimió los datos locales de los puntos finales comprometidos y cargó los archivos en los sitios anónimos de intercambio de archivos anonymfiles[.]com y file[.]io Luego, los atacantes intentan extorsionar aún más al cliente amenazando con divulgar estos datos públicamente a través del sitio de fugas BlackByte Tor. El ejecutable BlackByte deja una nota de rescate en todos los directorios donde se produce el cifrado. La nota de rescate

Entidad	Vector de Ataque
	incluye el sitio. onion que contiene instrucciones para pagar el rescate y recibir una clave de descifrado.

Proponer recomendaciones teniendo como base un marco de trabajo de ciberseguridad y el análisis de los casos de ciberataques que sirvan como contribución para la mejora y la resiliencia del entorno digital del sector salud público en Colombia.

Varias organizaciones de diferentes industrias optan por establecer dentro de sus organizaciones marcos cruzados que comprenden marcos de ciberseguridad, relacionados con Gestión de riesgos, gobernanza de la ciberseguridad y cumplimiento normativo, enfocados en un entorno GRC de Governance, Risk Management y Compliance.

También dependiendo del tamaño de la organización, el sector al que pertenece y los requisitos reglamentarios que deben de cumplir de acuerdo con exigencias de organismos estatales.

Los casos de ciber ataques que sucedieron durante los últimos años en contra de las entidades del sector de la salud en Colombia, denotan la importancia de contar con la debida implementación de los marcos de trabajo relacionados con la seguridad de la información, la protección de la privacidad de la información y la gestión de riesgos teniendo en cuenta el panorama de amenazas que está en constante evolución.

El marco de trabajo de ciberseguridad CSF del NIST es aplicable a diferentes sectores e industrias incluyendo la Salud.

A continuación, se relacionan algunos de los aspectos importantes que hace del CSF 2.0 del NIST un marco de trabajo integral y actualizado acorde con las amenazas emergentes y buenas prácticas de ciberseguridad.

Integración Mejorada de la Gobernanza

El marco de trabajo del NIST CSF 2.0 lanzado en febrero de 2024, incluye un nuevo componente de gobernanza, («NIST Releases Version 2.0 of Landmark Cybersecurity Framework», 2024) tiene un alcance ampliado que va más allá de la protección de infraestructuras críticas, como hospitales y plantas de energía, y abarca a todas las organizaciones de cualquier sector. También tiene un nuevo enfoque en la gobernanza, que abarca la forma en que las organizaciones toman y llevan a cabo decisiones informadas sobre la estrategia de ciberseguridad.

La integración de la gestión de riesgos de ciberseguridad en la gestión estratégica es esencial para las organizaciones, según (Nist, 2024b) la función de gobernanza apoya la comunicación de los riesgos organizativos con los directivos. Las discusiones de los directivos tienen que ver con la estrategia, en particular con la forma en que las incertidumbres relacionadas con la seguridad cibernética podrían afectar al cumplimiento de los objetivos de la organización.

A medida que los directivos establecen prioridades y objetivos de seguridad cibernética basados en esas necesidades, comunican las expectativas sobre el apetito de riesgo, la responsabilidad y los recursos. Los directivos también son responsables de integrar la gestión de riesgos de seguridad cibernética con los programas de ERM (Enterprise Risk Management) y los programas de gestión de riesgos.

La colaboración entre diferentes departamentos, la asignación de recursos de manera transparente, una comunicación efectiva y el cumplimiento proactivo a nivel normativo, son

estrategias principales que pueden fomentar la integración exitosa del gobierno corporativo con el gobierno de la ciberseguridad, cultivando de esta manera la cultura de la ciberseguridad donde todos los niveles comparten responsabilidad desde diferentes aristas.

Todas las consideraciones de ciberseguridad deben de estar integradas en todos los procesos de la organización y en los planes, estrategias, así como también en la toma de decisiones.

Gestión Avanzada de Riesgos en la Cadena de Suministro

(Nist, 2024b) dice que una organización puede utilizar el CSF para fomentar la supervisión de los riesgos de seguridad cibernética y las comunicaciones con las partes interesadas a lo largo de las cadenas de suministro. Todos los tipos de tecnología dependen de un ecosistema de cadena de suministro complejo, distribuido a escala mundial, extenso e interconectado, con rutas geográficamente diversas y diversos niveles de subcontratación. Este ecosistema está compuesto por entidades de los sectores público y privado (p. ej., compradores, proveedores, desarrolladores, integradores de sistemas, proveedores de servicios de sistemas externos y otros proveedores de servicios relacionados con la tecnología) que interactúan para investigar, desarrollar, diseñar, fabricar, adquirir, entregar, integrar, operar, mantener, eliminar y utilizar o gestionar de otro modo productos y servicios tecnológicos Estas interacciones están determinadas e influidas por tecnologías, leyes, políticas, procedimientos y prácticas. Los ataques dirigidos a la cadena de suministro con el paso de los años se han venido convirtiendo en una vulnerabilidad crítica para las organizaciones de todo el mundo.

De acuerdo con El CSF ayuda a gestionar riesgos en cadenas de suministro mediante CSCRM (gestión de riesgos de la cadena de suministro de ciberseguridad), como se detalla en SP 800-161r1.

CSF 2.0 aborda esta creciente amenaza centrándose en la seguridad de la cadena de suministro, incluyendo:

Gestión de riesgos de terceros: el marco actualizado incluye la gestión de riesgos de terceros, sugiriendo en (Nist, 2024a) que se evalúe los riesgos de seguridad cibernética que plantean los proveedores y otros terceros antes de entablar relaciones formales.

Integración Mejorada de CTI

A medida que las ciber amenazas evolucionan de manera muy acelerada, la capacidad de compartir eficazmente inteligencia sobre amenazas es cada vez más importante.

(«NIST Releases Version 2.0 of Landmark Cybersecurity Framework», 2024) destaca la importancia de integrar la inteligencia sobre amenazas como parte del perfil objetivo el cual especifica los resultados deseados que una organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión de riesgos de seguridad cibernética. Un Perfil Objetivo considera cambios anticipados a la postura de seguridad cibernética de la organización, tales como nuevos requerimientos, adopción de nuevas tecnologías, y tendencias de inteligencia de amenazas.

Dentro de la función detectar se analizan anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos para caracterizarlos y detectar incidentes de seguridad cibernética. Dentro de los controles que aportan a esta función, menciona la inteligencia de amenazas DE.AE-07: La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis.

Estrategias de defensa colaborativa: este marco alienta a las organizaciones a participar en redes de intercambio de información sobre amenazas en el control de la evaluación del riesgo

ID.RA-02: se recibe información sobre amenazas cibernéticas de foros y fuentes de intercambio de información.

Mecanismos mejorados para compartir información: para respaldar el intercambio efectivo de información, esta actualización proporciona orientación para evaluar la identificación y registro de amenazas internas y externas como lo indica el control ID.RA-03.

Gestión de Identidades

CSF 2.0 dentro de la función proteger incluye la gestión de identidades, autenticación y control de acceso.

Relacionado con la gestión de identidades aparecen los controles relacionados a continuación:

PR.AA-01: La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados.

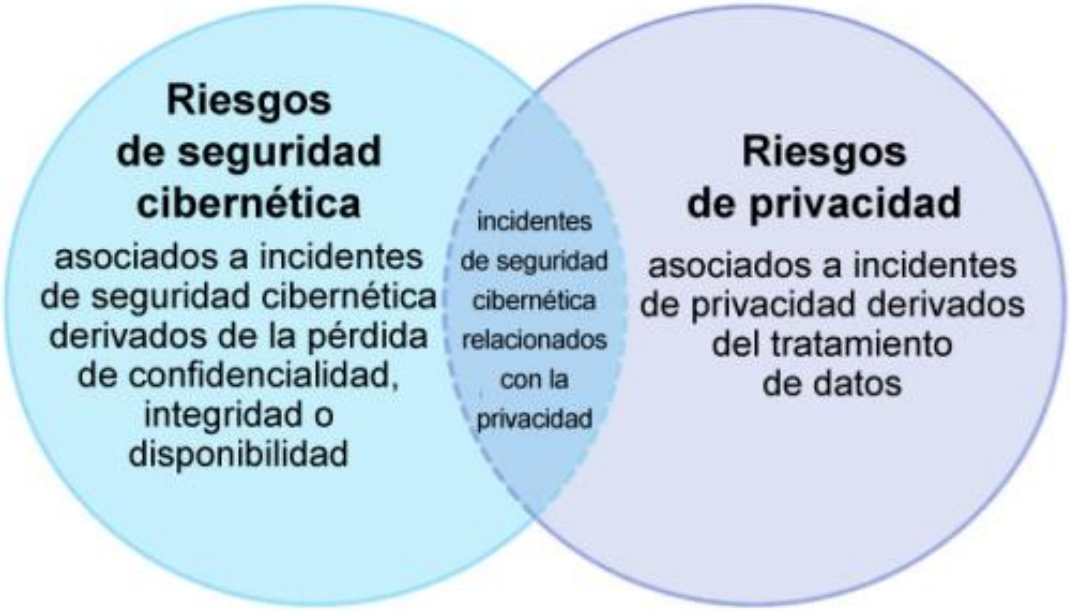
PR.AA-02: Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones.

Seguridad cibernética y la privacidad

CSF 2.0 integra la seguridad cibernética y los riesgos de privacidad como aparece en la figura a continuación, donde dependiendo de las circunstancias estos pueden resultar en incidentes de seguridad cibernética que tienen que ver con la privacidad.

Figura 13

Incidentes de Seguridad Cibernética y de Privacidad



Nota. Diagrama de Venn sobre los tipos de incidentes de seguridad cibernética y privacidad e intersección entre estos. Tomado de («NIST Releases Version 2.0 of Landmark Cybersecurity Framework», 2024).

Reconociendo el vínculo intrínseco entre la privacidad y la ciberseguridad, este marco expande sus directrices de privacidad para asegurar que las organizaciones puedan gestionar y proteger mejor la información personal.

¿Por qué es importante proteger la información pública?

Las entidades del sector público deben proteger la información, basándose en directivas y normas legales vigentes referentes al tema y como ejemplo la implementación del estándar ISO/IEC 27001, la Ley de Protección de Datos Personales, y entre otras, como por ejemplo la ISO 27701 o también conocida por el Sistema de Gestión de Privacidad de la Información.

Proteger la información de los ciudadanos sean personas naturales y jurídicas, lograra que la confiabilidad en las entidades aumente, ya que si no se protege la información de manera adecuada el sistema puede colapsar y puede haber perdida de la información vital para el Estado colombiano.

¿Cómo se puede proteger la información pública?

Esta tarea es difícil y tal vez se encuentren varias formas de protegerla, pero es posible definir los aspectos generales que determinen cómo se puede llevar a cabo la tarea:

Se debe definir el cómo y cuándo, que se realiza con las diferentes guías aportadas por el MINTIC como con la normatividad vigente, además que este ente está actualizando continuamente su documentación, además lidera los procesos de innovación tecnológica y de transformación digital del Estado y que tiene entre sus funciones elaborar los planes, políticas, normativas y directivas en el marco de las necesidades.

La implementación de las normas, estándares, políticas, decretos; tiene un plazo para que las entidades las puedan establecer, en el caso del Sistema de Gestión de Seguridad de la Información existen fechas que cada una de las entidades debe cumplir, su incumplimiento podrá generar multas o sanciones.

Seguimiento y control; no es solamente cumplir con las fechas establecidas para implementar las normas, estándar, entre otros, se debe seguir un control y un seguimiento a su cumplimiento según la normatividad vigente, sino que es necesario evaluar cómo se está desarrollando la protección. Se debe verificar la eficiencia de las protecciones a la información de modo que, de acuerdo a las necesidades, se ajuste a la seguridad de la información

¿Cuáles son las recomendaciones a nivel de seguridad informática para salvaguardar la información pública?

La seguridad de la información a lo largo de los últimos años se ha convertido en un punto muy importante, las siguientes son algunas de las recomendaciones:

Gestionar los riesgos, toda organización debería de administrar y gestionar los riesgos de seguridad de la información, estableciendo equipos de trabajo donde se involucren diferentes áreas, además de esto tener un equipo calificado, que permita una identificación de riesgos de calidad que mitigue la materialización de los riesgos.

Realizar una gestión de riesgos con el fin de encontrar las mayores vulnerabilidades

Realizar pruebas de caja blanca, negra y gris sobre los sistemas informáticos de la Entidad, pero cuales son estas pruebas a continuación su descripción:

Auditoría caja negra: Denominada test de intrusión, es en la que el auditor no posee conocimientos de la infraestructura tecnológica a auditar, esta revisión es excelente ya que sirve para simular ataques realizados por parte de personal externo a la Entidad y conocer el nivel de exposición a un ataque.

Auditoría caja blanca: Es más minuciosa ya que en esta facilita información técnica sobre los activos de la entidad a auditar incluyendo, donde se obtiene o es entregada información tal como usuarios, contraseñas y mecanismos de seguridad existentes, gracias a esto el auditor se puede concentrar en lo que verdaderamente interesa. El objetivo de las auditorias de caja blanca es colocar un obstáculo frente a ataques más sofisticados y entregar más recursos para evitar posibles ataques.

Todos los equipos deben de estar protegidos con antivirus, firewalls, sistemas de autenticación, VPN para el acceso remoto.

Generación de contraseñas seguras (Políticas de gestión de contraseñas)

Control de dispositivos extraíbles en los puertos USB.

Capacitaciones para poder detectar los diferentes ataques, tanto los que son enviados vía correo electrónico como por mensaje de texto.

Es importante comprometer a los responsables de los activos de TI la puesta en marcha de las medidas establecidas en cada uno de los activos para poder minimizar las amenazas que atentan a los diferentes activos de TI, de esta manera tendrá cambios significativos la institución.

El análisis y gestión de riesgos debe ser actualizado constantemente con el fin de poder lograr una adecuada mitigación de estos

Todas las entidades públicas deben contar un plan de mitigación de riesgos para evitar cualquier amenaza que atente contra los activos de la entidad

Compartir y capacitar a los funcionarios en el plan de mitigación de riesgo con el fin que sepan que acciones realizar en caso de materializarse una amenaza en los de TI.

Soluciones de seguridad orientadas a la defensa en profundidad que actualmente son muy utilizadas a nivel mundial como la gestión de identidades como se puede ver en la figura a continuación, donde aparecen la administración de los recursos, los permisos que se pueden conceder a que usuarios, si están autorizados a acceder a los recursos y a que recursos pueden acceder.

Figura 14

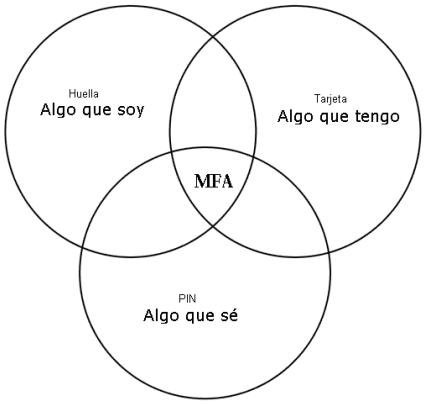
IAM – Gestión de identidades y accesos

Nota. Diagrama sobre aplicación granular de permisos a recursos y servicios en AWS. Tomado de AWS - Introducción a AWS Identity and Access Management (IAM).

En la siguiente figura, destaca aspectos esenciales de la autenticación multifactor, que está conformada por algo que soy, algo que tengo y algo que sé, lo cual genera una capa adicional de seguridad para los recursos.

Figura 15

MFA – Autenticación Multi Factor

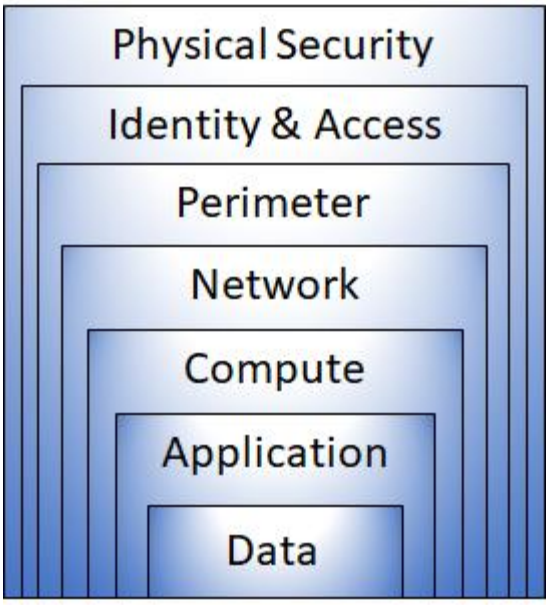


Nota. Elaboración propia - Diagrama de Venn sobre los tres factores de autenticación.

Actualizaciones y parches de seguridad, mantener los sistemas operativos, el software y las aplicaciones actualizados con los últimos parches de seguridad, esto con el fin de evitar que versiones desactualizadas o no parchadas y con vulnerabilidades conocidas que sean potencialmente explotable.

Las anteriores, fueron una de las tantas medidas a adoptar y mantener, lo ideal es propender por un enfoque orientado a la defensa en profundidad que está conformada por capas, como se puede observar en la figura a continuación.

Figura 16 *Defensa en Profundidad*



Nota. Seguridad por capas. Tomado de "What is defense in depth?" por AzureGuru, 2021, AzureGuru Community.

Aspectos claves de seguridad relacionados con los datos, aplicación, computo, Red, perímetro, identidades y accesos, como también seguridad Física.

Conclusiones

Durante el desarrollo de este trabajo de grado en la modalidad de monografía, se realizó la exploración de manera profunda sobre la importancia de los marcos de trabajo relacionados con la gestión de riesgos de ciberseguridad en las organizaciones de salud del orden estatal en Colombia; con el objetivo primordial de comprender como todos estos marcos de trabajo de una u otra manera desde su alcance aportan a la gestión de riesgos de ciberseguridad en entidades de salud a nivel global y también los estándares, políticas y procedimientos que desde MINTIC se direccionan a las entidades estatales incluyendo las de la salud.

A lo largo de la consulta documental, se descubrió que las organizaciones de salud de carácter estatal cuentan con directrices emanadas por parte de MINTIC relacionadas con la gestión de riesgos y todo lo que implica este proceso. Mediante la consulta de diferentes fuentes de información se logró identificar los conceptos clave de marcos de trabajos y estándares sobre los cuales se basa MINTIC y otros referentes internacionales, por lo cual se requiere la adopción de un marco de trabajo flexible, como por ejemplo CSF 2.0 del NIST del año 2024, aplicable a todo tipo de organizaciones y de acuerdo con las necesidades específicas de cada una de estas.

En el Análisis de casos de ciberataques al sector salud en Colombia dio lugar a realizar algunas observaciones respecto a la aplicabilidad del CyberSecurity Framework 2.0 del NIST, el cual es fundamental para realizar la mitigación del riesgo cibernéticos, así como también aspectos relacionados con la recuperación ante incidentes de ciberseguridad. La tendencia de las organizaciones Federales de estados unidos y otras organizaciones a nivel mundial está en tener en cuenta este FrameWork junto con otros documentos y guías de la serie 800 del NIST principalmente NIST SP 800-161 Rev. 1 Prácticas de gestión de riesgos de la cadena de suministro de ciberseguridad para sistemas y organizaciones, NIST SP 800-61 Rev. 3 Guía de

manejo de incidentes de seguridad informática. NIST SP 800-53 Rev. 5 Controles de seguridad y privacidad para sistemas de información y organizaciones.

Un marco de trabajo de ciberseguridad cruzado puede ser un buen punto de partida, que comprenda temas normativos como la Ley Estatutaria 1581 de 2012, elementos adicionales como cumplimiento con estándares de HIPAA, un análisis de brechas de los Controles CIS dentro de sus diferentes grupos de implementación para comparar los implementado a nivel de TI en las entidades de salud estatales contra lo que indican las salvaguardas, implementación de CSF 2.0 del NIST sumando los marcos de trabajo y estándares existentes como el mapeo de los controles de la ISO 27001/27002 de 2022.

La aplicación de marcos de trabajos en las organizaciones y gestionar los riesgos de manera adecuada puede resultar en un gran desafío dados los recursos que se requieren para su implementación, seguimiento, administración y gestión en pro de mejora continua, puesto que no existe un nivel de riesgo cero y que constantemente aparecen nuevas vulnerabilidades que en algunos casos son un poco dispendiosas de remediar por cuestiones de tiempo, recursos o porque simplemente existe una vulnerabilidad Zero Day que no es posible remediar hasta que el parche o actualización sean suministrados por el fabricante de software, también puede suceder que a nivel de negocio no se autorice la implementación de una salvaguarda que puede afectar la continuidad operativa del negocio.

Los desafíos importantes en materia de seguridad y la implementación de estos FrameWorks son la resistencia al cambio y los recursos limitados, sin embargo, esto también puede representar oportunidad de mejora, ya que al proponer planes de sensibilización y concienciación esta resistencia al cambio va mejorando de manera gradual por medio de indicadores de gobierno de la ciberseguridad que es uno de los pilares importantes incorporados

en la versión 2.0 del CSF además que el factor humano es el eslabón más importante dentro de un esquema de ciberseguridad. También, la oportunidad de mejora que puede resultar de los recursos limitados es la opción de realizar comités de ciberseguridad donde se puede evaluar y priorizar los riesgos y la implementación de controles de seguridad de los diferentes marcos de trabajo y estándares.

Referencias

Benito, P. L. (2023, marzo 14). *Ciberataque a Sanitas: Hackers revelaron más información clasificada de la EPS*. infobae. https://www.infobae.com/colombia/2023/03/14/ciberataque-a-sanitas-hackers-revelaron-mas-informacion-clasificada-de-la-eps/

Ciberataque: El hombre detrás de IFX, la empresa que Colombia amenaza con demandar. (s. f.). Recuperado 2 de junio de 2024, de https://www.eltiempo.com/unidad-investigativa/ciberataque-el-hombre-detras-de-ifx-la-empresa-que-colombia-amenaza-con-demandar-807437

CIS Controls Implementation Group 2. (s. f.). CIS. Recuperado 26 de octubre de 2024, de https://www.cisecurity.org/controls/implementation-groups/ig2/

CIS Controls Implementation Group 3. (s. f.). CIS. Recuperado 26 de octubre de 2024, de https://www.cisecurity.org/controls/implementation-groups/ig3/

CIS Critical Security Controls FAQ. (s. f.). CIS. Recuperado 23 de septiembre de 2024, de https://www.cisecurity.org/controls/cis-controls-faq/

CIS Critical Security Controls Implementation Group 1. (s. f.). CIS. Recuperado 26 de octubre de 2024, de https://www.cisecurity.org/controls/implementation-groups/ig1/

ColCERT. (s. f.). *Inicio—ColCERT*. Recuperado 14 de octubre de 2024, de https://www.colcert.gov.co/800/w3-channel.html

Conozca más de la Superintendencia Nacional de Salud. (s. f.). Recuperado 8 de agosto de 2024, de https://www.supersalud.gov.co/es-co/Paginas/Oficina%20de%20Comunicaciones/campa%C3%B1as/que-es-la-supersalud/index.html

CSIRT Académico UNAD. (2024). *Febrero: Tendencias de amenazas de ciberseguridad previstas para el año 2030* (20). Universidad Nacional Abierta y a Distancia. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Boletin_N_20_-_Febrero_2024_-_F.pdf

CSIRT, Coordinación Nacional de Ciberseguridad, Ministerio del Interior y Seguridad Pública, Gobierno de Chile. (2023). *14TCA23-00013-01 Ransomware en IFX*. https://csirt.gob.cl/documentos/14tca23-00013-01/

Decreto 1008 de 2018—Gestor Normativo—Función Pública. (2018). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86902

Departamento de Seguridad Informática. (2014). *Amenazas a la Seguridad de la Información*. Universidad Nacional de Luján. https://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Departamento Nacional de Planeación. (2016). *CONPES 3854 Política Nacional de Seguridad Digital*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2020). *CONPES 3995 Política Nacional de Confianza y Seguridad Digital*. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Diaz, J. D. R. (2024, enero 29). Salud Total EPS-S presentó un ataque informático externo. *Salud Total EPS-S*. https://saludtotal.com.co/plan-de-beneficios-en-salud/salud-total-eps-s-esta-siendo-objeto-de-ataque-informatico-externo-2/

Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2024). Health Insurance Portability and Accountability Act. En *StatPearls*. StatPearls Publishing. http://www.ncbi.nlm.nih.gov/books/NBK500019/

El Tiempo, C. E. E. (2017, septiembre 27). *A diario se registran 542.465 ataques informáticos en Colombia*. El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Escrivá Gascó, G., Romero Serrano, R. M., Ramada, D. J., & Onrubia Pérez, R. (2013). *Seguridad informática*. Ra-Ma Editorial.

Estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf. (2022). https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf

Fortinet. (2023). *Informe global del panorama de amenazas*. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2h-2023.pdf

Función Pública. (s. f.). *Decreto 338 de 2022—Gestor Normativo*. Recuperado 8 de agosto de 2024, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Función Pública. (2005). *Decreto 1599 de 2005—Gestor Normativo—Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=16547

Gómez Vieites, Á. (2014). *Enciclopedia de la seguridad informática (2a. Ed.)*. RA-MA Editorial.

Gros, S. (2021). A Critical View on CIS Controls. *2021 16th International Conference on Telecommunications (ConTEL)*, 122-128. 2021 16th International Conference on Telecommunications (ConTEL). https://doi.org/10.23919/ConTEL52528.2021.9495982

ISO/IEC 27002:2022. (s. f.). ISO. Recuperado 4 de noviembre de 2024, de https://www.iso.org/es/contents/data/standard/07/56/75652.html

Microsoft Compliance. (2023, marzo 17). *Marco de seguridad común (CSF) de Health Information Trust Alliance (HITRUST)*. https://learn.microsoft.com/es-es/compliance/regulatory/offering-hitrust

Ministerio de Salud y Protección Social. (2023). *Incidente de ciberseguridad en los servicios digitales de Ministerio de Salud y Protección Social*. https://www.minsalud.gov.co/Paginas/Incidente-ciberseguridad-en-servicios-digitales-Ministerio-Salud-y-Proteccion-Social.aspx

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016a). *Guía de gestión de riesgos*. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016b). *Guía para la Gestión y Clasificación de Activos de Información.* https://gobiernodigital.mintic.gov.co/692/articles-5482_G5_Gestion_Clasificacion.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas*. https://gobiernodigital.mintic.gov.co/692/articles-237907_maestro_mspi.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023). *CSIRT Gobierno*. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno

MITRE ATT&CK®. (s. f.). Recuperado 14 de octubre de 2024, de https://attack.mitre.org/groups/G0049/

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

NIST. (s. f.). *Framework for Reducing Cyber Risks to Critical Infrastructure*. Recuperado 23 de septiembre de 2024, de https://www.nist.gov/system/files/documents/2017/06/01/040913_hitrust.pdf

Nist, G. M. (2024a). *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide (Spanish translation)* (NIST SP 1300 spa; p. NIST SP 1300 spa). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1300.spa

Nist, G. M. (2024b). *Spanish Translation of the NIST Cybersecurity Framework 2.0* (NIST CSWP 29 spa; p. NIST CSWP 29 spa). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29.spa

NIST Releases Version 2.0 of Landmark Cybersecurity Framework. (2024). *NIST*. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

O'Brien, N., Crespo, R., O'Driscoll, F., Prendergast, M., Chana, D., Darzi, A., & Ghafur, S. (2024). Usability and Feasibility Evaluation of a Web-Based and Offline Cybersecurity Resource for Health Care Organizations (The Essentials of Cybersecurity in Health Care Organizations Framework Resource): Mixed Methods Study. *JMIR Formative Research*, *8*, e50968. https://doi.org/10.2196/50968

O'Brien, N., Grass, E., Martin, G., Durkin, M., Darzi, A., & Ghafur, S. (2021). Developing a globally applicable cybersecurity framework for healthcare: A Delphi consensus study. *BMJ Innovations*, *7*(1), 199-207. https://doi.org/10.1136/bmjinnov-2020-000572

Presidencia de la república. (2022). *Decreto 767 de 2022 Nivel Nacional*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=123541

¿Qué es gestión de riesgos? | IBM. (s. f.). https://www.ibm.com/mx-es/topics/risk-management

Rico, J. C. G. (2023, septiembre 16). *Así enfrenta Colombia su primer caso de 'megasecuestro digital'; ¿qué está pasando?* El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-detalles-del-ataque-a-ifx-networks-806778

Riveros, A. (2020, junio 25). ISO 31000 y la Gestión de Riesgos: Para qué sirve. *EALDE Business School*. https://www.ealde.es/iso-31000-para-que-sirve/

Salazar, J. S. (2019). *Estrategia para la preservación de documentos digitales en el archivo de la Secretaría de la Junta Directiva del Banco de la República de Colombia*.

S.A.S, E. L. R. (2023, enero 23). *Audifarma sufrió ataque cibernético y se suma a otras empresas que han sido víctimas*. Diario La República. https://www.larepublica.co/empresas/audifarma-sufrio-ataque-cibernetico-y-se-suma-a-otras-empresas-que-han-sido-victimas-3528413

Sector salud afectado en ciberataque a entidades del Estado. (2023, septiembre 14). https://consultorsalud.com/ciberataques-entidades-del-estado/

SonicWall. (2022). *2022 SonicWall Cyber Threat Report*. https://www.sonicwall.com/resources/white-papers/2022-sonicwall-cyber-threat-report/gated/thank-you/asset

SonicWall. (2023). *2023 SonicWall Cyber Threat Report*. https://www.sonicwall.com/2023-sonicwall-cyber-threat-report

SonicWall. (2024). *2024 SonicWall Cyber Threat Report*. https://www.sonicwall.com/resources/white-papers/2024-sonicwall-cyber-threat-report

Super Intendencia Nacional de Salud. (2023, septiembre 19). *Circular externa 2023100000000014*.

https://docs.supersalud.gov.co/PortalWeb/Juridica/CircularesExterna/Circular%20Externa%20No.%202023100000000014-5%20de%202023.pdf

TrendMicro. (2023). *Calibrating Expansion: 2023 Annual Cybersecurity Report*. https://documents.trendmicro.com/images/TEx/articles/Calibrating-Expansion_2023-Annual-Cybersecurity-Report.pdf

Udroiu, A.-M., Dumitrache, M., & Sandu, I. (2022). Improving the cybersecurity of medical systems by applying the NIST framework. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1-7. https://doi.org/10.1109/ECAI54874.2022.9847498

Vásquez, G. B. (2022, noviembre 22). *Invima: 'Hackers' piden US$ 5 millones en criptomonedas para restablecer página*. El Tiempo. https://www.eltiempo.com/economia/sectores/invima-hackers-piden-5-millones-de-dolares-para-restablecer-la-pagina-web-719600

Vásquez Ojeda, A. W. (2020). Diseño de un Sistema de Gestión de Seguridad de Información para la empresa Neointel SAC basado en la norma ISO/IEC 27001:2013. *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://doi.org/10.19083/tesis/652123

Yamcharoen, P., Folorunsho, O. S., Bayewu, A., & Fatoye, O. E. (2023). Advancing healthcare security: Developing a composite set of cybersecurity requirements for the healthcare industry. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *14*(1), 9-20. https://doi.org/10.22624/AIMS/CISDI/V14N1P2