Panorama de la Respuesta a Incidentes de Seguridad de la Información en las Organizaciones del Sector Salud en Colombia

Ivonne Rocio Bernal Núñez

Directora

Yenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2024

Resumen

Dentro de este trabajo de grado se buscará abordar la gestión que las organizaciones del sector salud en Colombia dan a los incidentes de seguridad de la información y la respuesta ante su materialización, siendo esta un proceso crítico para estas, esto teniendo presente que de acuerdo con las cifras presentadas por el Centro Cibernético de la Policía Nacional se presentaron 54.121 denuncias relacionadas con ataques cibernéticos y Colombia se posiciona en el tercer lugar de los países más atacados en América Latina, los ataques han sido dirigidos a organizaciones de todo tipo, sin embargo, las que han tenido un mayor impacto son las entidades gubernamentales y las del sector de la salud, en los que estos ataques pusieron en riesgo la vida o el libre desarrollo de millones de ciudadanos.

Este trabajo abordara las siguientes temáticas, todas ellas dentro del contexto de las organizaciones del sector salud en Colombia:

Los principales vectores de ataque más explotados en las organizaciones, donde se identificarán las principales tendencias y su materialización en Colombia, para el entendimiento de estos en el contexto del país, identificar el estado actual la gestión de la seguridad de la información, así como identificar los factores que influyen en la respuesta a incidentes de seguridad de la información.

Palabras clave: incidentes de seguridad de la información, vectores de ataque, seguridad de la información.

Abstract

Within this degree work, we will seek to address the management that health sector organizations in Colombia give to information security incidents and the response to their materialization, this being a critical process for them, keeping in mind that according to The figures presented by the Cyber Center of the National Police, 54,121 complaints related to cyber attacks were presented and Colombia is positioned in third place of the most attacked countries in Latin America, the attacks have been directed at organizations of all types, however, Those that have had the greatest impact are government entities and those in the health sector, in which these attacks put the lives or free development of millions of citizens at risk.

This work will address the following topics, all of them within the context of health sector organizations in Colombia:

The main attack vectors most exploited in organizations, where the main trends and their materialization in Colombia will be identified, to understand them in the context of the country, identify the current state of information security management, as well as identify The factors that influence the response to information security incidents.

Keywords: information security incidents, attack vectors, information security.

Tabla de contenido

Introducción

Durante el desarrollo de este trabajo se analizará el panorama de la respuesta a incidentes de Seguridad de la información (SI) en las organizaciones del sector salud en Colombia, se podría decir que la gestión de los incidentes de seguridad de la información que da una organización puede presentar una gran radiografía de esta, ya que puede evidenciar brechas y vulnerabilidades no atendidas, así como la carencia de procesos que puedan dar respuesta a estos incidentes, mitigando el impacto y retornando a la operación, así como la estrategia de las organizaciones y el compromiso de la dirección.

Con el incremento del cibercrimen cobra mucha importancia que todas las organizaciones asuman una postura de seguridad robusta, sin importar su sector, que por supuesto incluye una gestión de seguridad de la información efectiva.

Planteamiento del Problema

La pandemia adelanto la llegada de la cuarta revolución industrial y con ella llego la hiper conectividad, no solo las organizaciones son objeto de ataques cibernéticos, también los ciudadanos y estos se han visto en aumento durante los últimos tres años, actualmente Colombia es el tercer país más atacado de Latinoamérica, por lo que es indispensable lograr identificar la gestión y respuesta a los incidentes de seguridad, así como la efectividad al momento de la materialización de estos.

De acuerdo con el CCIT y su programa de Seguridad Aplicada al Fortalecimiento Empresarial, una organización colombiana puede llegar a perder de $400 a $1.200 millones de pesos a raíz de un ciberataque. (Mesa, 2022)

De igual forma en su informe anual de ciberseguridad, en retrospectiva con las denuncias generadas en 2023 cuando iniciaron los ataques con *Ransomware* se conocieron 3.380 reportes, ahora con una década en transcurso se cuentan con 65.794 reportes, durante el 2022 se presentó un repunte en el incremento de casos, el mayor se presentó en el 2020. (TicTac, 2023)

Pregunta, ¿Cómo se da respuesta a los incidentes de seguridad de la información en Colombia?.

Justificación

El desarrollo de este trabajo de grado busca tener la comprensión del panorama de la respuesta a incidentes de seguridad de la información, donde se buscará identificar los principales vectores de ataque y vulnerabilidades explotadas y gestión a los incidentes de seguridad de la información en las organizaciones del sector salud en Colombia, esto con el fin de lograr evaluar las debilidades y fortalezas que se tengan frente a esta gestión, así como puntos de mejora clave.

Objetivos

Objetivo General

Analizar el estado actual de las organizaciones del sector salud en Colombia en cuanto a su capacidad de respuesta frente a incidentes de seguridad de la información, a través de una revisión sistemática de literatura e informes especializados para la identificación de brechas existentes y como base para el desarrollo de mecanismos y buenas prácticas de aseguramiento adaptados a las necesidades específicas de dicho sector

Objetivos Específicos

Realizar una revisión exhaustiva de la literatura y de informes especializados para obtener un panorama actual de la seguridad de la información en las organizaciones del sector salud en Colombia.

Examinar los vectores de ataque de los que ha sido víctima las infraestructuras TI de las organizaciones del sector salud.

Analizar los factores internos y externos que influyen en la capacidad de respuesta ante incidentes de seguridad de la información en las organizaciones del sector salud en Colombia, dentro de un contexto operativo y regulatorio.

Proponer mecanismos que contribuyan en el aseguramiento y la capacidad de gestión de incidentes en las organizaciones del sector salud.

Marco Referencial

Antecedentes o Estado Actual

De acuerdo con el estudio realizado riesgos cibernéticos en el sector financiero colombiano situación actual y tendencias, indica que, de acuerdo con el aumento de ciberataques, al igual que su complejidad y sofisticación, se identifica la necesidad de que las medidas de seguridad sean robustas y acordes para proteger los activos. (Nieto Rodríguez & Sanches Rojas, 2023b)

Marco Conceptual

La Triada de la Seguridad

La triada de la seguridad comprende la confidencialidad, integridad y disponibilidad, de acuerdo con incibe la confidencialidad garantiza que la información será accesible solo por las personas que lo requieran y estén autorizadas para su acceso, por su parte la integridad, asegura que los datos ya sea en su transporte o reposo no han sido alterados o destruidos y por último, la disponibilidad corresponde a la capacidad con la que cuenta la información y/o infraestructura tecnológica para que se pueda acceder y hacer uso de esta cuando sea requerido.

Los SGSI buscan generar políticas, practicas, controles, entre otros, para lograr la preservación de la triada de seguridad en todos los activos de la organización. (INCIBE, 2020)

Gestión de Incidentes de Seguridad de la Información

Con la llegada de la cuarta revolución industrial las organizaciones públicas y privadas debieron realizar esfuerzos muy significativos para enfrentar los retos que estas traían, para la gestión de incidentes de SI, a continuación, se abordaran los siguientes marcos de trabajo:

NIST SP 800-61, Guía para el Manejo de Incidentes. Esta guía contempla cuatro etapas las cuales son (National Institute of Standards and Technology (NIST), 2021):

Preparación: Busca establecer y capacitar a quienes serán responsables de la respuesta a incidentes de seguridad, de igual forma garantizar que se cuente con los recursos necesarios para su atención y el despliegue de controles para prevenir la materialización de los incidentes esto tomando como base la gestión de riesgos.

Detección y análisis: Esta fase es fundamental ya que en caso de que los controles fallen la organización debe poder identificar y generar las alertas necesarias.

Contención, Erradicación y Recuperación: De acuerdo con la criticidad del incidente la organización debe contemplar las herramientas y mecanismos necesarios para poder contenerlo y recuperarse de este, es decir volver a operar.

Actividades post incidentes: Por ultimo las organizaciones deben generar informes que permitan identificar de claramente lo ocurrido, lo costos de este y actividades que se deban desarrollar para prevenir escenarios como el presentado.

GTC-ISO/IEC 27035, Gestión de Incidentes de Seguridad de la Información. El alcance de este framework es el de brindar un enfoque planificado y estructurado para la detección, reporte y evaluación de incidentes, de igual forma se contemplan las siguientes fases (ISO (International Organization for Standardization), 2013):

Planificación y preparación: Dentro de esta fase se deben contemplar todos los recursos necesarios para la atención de los incidentes, dentro de ellos se encuentra contar con el respaldo de la alta dirección, la generación de la política para la gestión de incidentes de seguridad de la información y políticas específicas como gestión de riesgos, esquema o proceso para la atención de incidentes de SI, establecer el equipo responsable de los SI, capacitación hacia los diferentes actores en el proceso y pruebas para la respuesta a SI.

Detección y reporte: Dentro de esta fase se realizará la detección y recolección de los eventos de SI presentados, así como el reporte de estas, dentro de esta fase también se deberá realizar a la identificación de las vulnerabilidades.

Evaluación y decisión: En esta fase se deberán evaluar los eventos de SI y tomar una decisión sobre si este es un incidente o un evento de SI.

Respuesta: Respuesta y recuperación del incidente de SI, asegurando la preservación de las pruebas forenses.

Lecciones aprendidas: Ejecución de análisis forenses más exhaustivo, identificación de lecciones aprendidas y generación de planes de trabajo para la mejora continua y notificar a la alta dirección sobre el estado de la gestión de los incidentes de SI.

Para abordar cada una de estas fases las organizaciones deberán contemplar diversos procesos, prácticas y mecanismos para abordar estas diferentes fases y lograr dar una respuesta efectiva a los incidentes de seguridad de la información, actualmente los incidentes de SI presentados en Colombia son cubiertos en su mayoría por prensa, sin embargo, no se cuenta con un punto focal que logre dar el soporte necesario a las organizaciones, así como el seguimiento e identificación del impacto, este trabajo busca identificar por medio de estas múltiples fuentes cuales son las fortalezas y debilidades frente a estos.

NTC-ISO/IEC 27005, Gestión de Riesgos para la Seguridad de la Información. La norma NTC-ISO/IEC 27005 para la gestión de riesgos para la seguridad de la información comprende las siguientes fases ((ISO (International Organization for Standardization), 2020):

Contexto: Se establece el enfoque para la gestión de riesgos, criterios para la evaluación y aceptación, alcance y límites.

Evaluación de los riesgos: Durante esta fase se identificarán los activos de información y los riesgos que puedan generar una perdida potencial, se identificarán las amenazas y su origen, se realizara la validación de los controles asignados para la mitigación de estos riesgos y por último se realizara la valoración del riesgo.

Tratamiento del riesgo: De acuerdo con la valoración de los riesgos y los criterios establecidos se deben tomar las siguientes medidas, reducir, retener, evitar o compartir el riesgo.

Aceptación de los riesgos: Conforme a los resultados de las fases anteriores los responsables y partes interesadas deberán tomar las decisiones que correspondan.

Vigilancia de los riesgos: Se deberá hacer seguimiento a las fuentes de riesgos, así como a la evaluación constante de estos y propender por la mejora continua de la gestión de riesgos de SI.

NIST SP 800-115, Guía Técnica para Pruebas y Evaluaciones de Seguridad de la Información. Este marco de gestión da una guía técnica para pruebas y evaluaciones de seguridad de la información para la correcta gestión de vulnerabilidades el cual cuenta con las siguientes fases (National Institute of Standards and Technology (NIST), 2021b):

Planificación: Durante esta fase se usará la metodología para la gestión de proyectos, se deberá recopilar la información necesaria para el desarrollo de las pruebas, se definiría el alcance, tipo de prueba, metodologías, metas objetivos, resultados esperados, roles y sus responsabilidades, recursos y los entregables.

Análisis de vulnerabilidades: A lo largo de esta fase se realizará la identificación y análisis de vulnerabilidades, estas pruebas pueden ser automatizadas por medio de herramientas o manuales

Ataque o prueba de penetración: Las pruebas de penetración tienen el objetivo de generar un escenario real y donde se explotarán las vulnerabilidades antes descubiertas.

Post-Ejecución: Finalmente se llevará a cabo el análisis de los resultados, generando los planes de remediación que allá lugar, así como la elaboración de los informes donde se identifique claramente todo el ejercicio.

Marco Teórico

De acuerdo con la información presentada en la XXI Encuesta Nacional de Seguridad Informática el 72% de las personas encuestadas tuvieron un incidente de SI en sus organizaciones, teniendo un aumento del 4% respecto al año anterior, adicionalmente se evidencia que los principales tipos de incidentes presentados fueron errores humanos, phishing, accesos no autorizados en la web, ingeniería social y por último la instalación de software no autorizado y solo el 28% de las empresas realiza el reporte de estos a las diferentes autoridades nacionales (Almanza J, 2021), dentro de la XXII Encuesta Nacional de Seguridad Informática se evidencia que el 3,67% de los encuestados no tienen conocimiento de la cantidad de incidentes de SI que se presentaron en sus organizaciones y el número de personas que estuvieron en contacto con un incidentes de SI disminuyo al 56% y una cifra bastante interesante es que el 17% de los encuestados han tenido más de 7 incidentes de SI, frente a los tipos de incidentes de SI se evidencia los siguientes cambios, frente a phishing aumento del 6%, la ingeniera social paso al tercer lugar con un aumento del 5% y entra dentro de los principales 5 tipos de incidentes el fraude electrónico (Almanza J, 2022).

Por otro lado, se encuentran las cifras presentadas por la Policía Nacional donde año a año se ha visto un incremento en el número de denuncias, esto sin contar con el hecho que con lo

evidenciado anteriormente para el 2022 solo el 28% de empresas realizaban el reporte formal a las autoridades competentes, esta cifra podría ser mucho mayor (CAI Virtual, s.f.).

Marco Legal

Ley 1273 de 2009, ley de delitos informáticos en Colombia, “de la protección de la información y los datos” esta ley modifico el código penal, creando un nuevo bien jurídico tutelado “de la protección de la información y de los datos”, tiene como propósito el de preservar los sistemas tecnológicos de la información y comunicaciones (LEY 1273 DE 2009, 2009).

Ley 1581 de 2012, ley de la protección de los datos personales, esta ley busca desarrollar el derecho que tienen las personas naturales o titulares a conocer, actualizar, rectificar y eliminar su información y las responsabilidades que tienen las organizaciones como encargados de su tratamiento, esta ley comprende las bases de datos físicas como las digitales (LEY_1581_2012, 2012).

CONPES 3854, política nacional de seguridad digital, busca dar gestión a los riesgos que pueden presentarse en el entorno digital, su objetivo es el de fortalecer las capacidades las partes interesadas dando gestión a los riesgos de seguridad digital de cara a las actividades socioeconómicas realizadas (CONPES 3854, 2016).

Marco Contextual

De acuerdo con el estudio de la evolución de los incidentes de la SI en Colombia de las décadas de 2010 a 2020, el 33% de las personas encuestadas indicaron que no conocían si se habían presentado incidentes de SI, por lo que queda en tela de juicio el correcto proceder para la identificación y respuesta ante los incidentes de SI, en las organizaciones, esto puede tener numerosas causas, desde el desconocimiento del proceso de gestión de incidentes de SI, por lo que pueden existir eventos de los que no se cuenta con reporte, otro motivo es que el proceso no

sea eficiente o este no se esté llevando a cabo por los colaborades de forma sistemática, también se podría evaluar que tan conectado se encuentra el equipo de respuesta a incidentes con el resto de la organización y por último, no se han dispuesto los recursos necesarios para monitorizar, identificar y reportar los incidentes.

Los sectores que cuentan con una mayor precisión sobre esta información y también materialización de incidentes son entes gubernamentales, el sector financiero, consultoría especializada y el sector de las telecomunicaciones, esto coincide en que estos sectores son los que han desarrollado mayores capacidades para la atención de incidentes de SI (Almanza J & Cano M, 2020).

Panorama Actual de la Seguridad de la Información en las Organizaciones del Sector Salud en Colombia

De acuerdo con la Organización Panamericana de la Salud en América Latina se cuenta con un marco normativo heterogéneo en materia de protección de datos personales, como es el caso de Colombia. Este marco normativo va muy de la mano con la seguridad de la información, ya que por medio de los controles y mecanismos dispuestos se logra dar una gestión y respuesta oportuna a la protección de los datos, sin embargo, es necesario generar estrategias nacionales que tengan equilibrio entre la privacidad y la accesibilidad, estas estrategias deben alinearse con normativas y estándares internacionales y ser complemento de la legislación y normativa actual (Organización Panamericana de la Salud, 2023).

Una de las brechas identificadas es la cadencia de políticas públicas que contemplen los planes de seguridad basado en perfiles de acceso, por lo que dificulta dar respuesta a un entorno que se encuentra en constante cambio para el aseguramiento de los datos, a esto se suma la falta de información sobre las tendencias y evolución de los ataques e incidentes de seguridad presentados, en el caso de Colombia sean generado números esfuerzos para articular esta información por medio del CAI virtual de la policía nacional donde se pueden identificar cifras sobre los casos presentados a nivel del cibercrimen, sin embargo, estas cifras no permiten generar estrategias o políticas para la seguridad de la información, por su parte el CSIRT presta asesoría a las organizaciones a las que se materialice un incidente de seguridad de la información y generan boletines informativos sobre alertas, vulnerabilidades y brechas de seguridad, no obstante y al igual que el CAI virtual, esta información no permite orientar las estrategias de ciberseguridad y seguridad de la información.

La tercera falencia identificada por Organización Panamericana de la Salud es la falta de planes y programas de capacitación en seguridad de la información y ciberseguridad, siendo los usuarios la primera línea de defensa ante un ataque cibernético este es un ítem fundamental para la prevención, preparación y reporte de incidentes de seguridad de la información, por lo que es imperativo que los usuarios puedan conocer los riesgos asociados a las actividades que desarrollan en el día a día y su responsabilidad con la protección de los datos personales, ya que como se evidencia en la XXIII Encuesta Nacional de Seguridad Informática (Almanza J, 2023), los profesionales de las áreas de seguridad y ciberseguridad reconocen la ausencia de una cultura de seguridad de la información como su principal obstáculo.

Adicionalmente, el sector salud no cuenta con el suficiente personal especializado para la atención y respuesta de incidentes de seguridad de la información, de acuerdo con la XXII Encuesta Nacional de Seguridad Informática (Almanza J, 2022), las áreas de ciberseguridad el sector de la salud en Colombia tiene una tendencia a la tercerización de los servicios de ciberseguridad y sus áreas internas están compuestas de uno a cinco colaboradores sin importar el tamaño de la organización, sin embargo, la información que genera una mayor preocupación es que no cuentan con roles dedicados a la gestión y mantenimiento de la seguridad de la información, lo que permite identificar que las funciones son compartidas con áreas de TI y la seguridad de la información puede pasar a un segundo plano. Dentro de las principales actividades realizadas resalta la definición de controles a nivel de TI y garantizar la protección de los datos personales.

Otra brecha identificada es la falta de mecanismos para la detección y respuesta a los incidentes de seguridad de la información, ya que no se cuenta con una estrategia a nivel gubernamental, como se indicó anteriormente el CSIRT dispuesto por el gobierno ofrece apoyo a

las organizaciones que lo requieran hasta el momento de la materialización, de acuerdo con la XXIII Encuesta Nacional de Seguridad Informática, los principales incidentes de seguridad de la información en el sector de la salud obedecen al error humano, el phishing, ataques a las aplicaciones web y de denegación de servicios, el costo de estos incidentes promedio en este sector alcanzo el costo de 750.000 USD.

Un factor fundamental para las organizaciones en materia de seguridad de la información es la de contar con una política de seguridad de la información implementada y comunicada a todos los colaborares, ya que con esta se puede establecer la postura de seguridad de la información y el apoyo de la alta dirección a su ejecución de acuerdo con la XXIII Encuesta Nacional de Seguridad Informática en el sector salud se cuenta con una política escrita, aprobada e informada, sin embargo, la seguridad de la información y ciberseguridad no es incluida en la estrategia organizacionales del sector salud y la alta dirección no se relaciona directamente con las decisiones que son necesarias tomar, esto también se refleja en que los profesionales del área indican como un factor que obstaculiza su labor la falta de tiempo por lo que la seguridad y ciberseguridad no es vista como un factor estratégico.

Otro pilar para la gestión de la seguridad de la información es la gestión de riesgos, la cual busca identificar, analizar y evaluar los riesgos y controles dispuestos por la organización para la mitigación de los riesgos, de acuerdo con lo presentado en la encuesta el sector salud desconoce esta gestión, lo cual genera una gran brecha ya que conforme con la norma ISO 27005:2022 para la orientación sobre la gestión de riesgos de seguridad de la información, donde se busca establecer el alcance para la gestión de riesgos, criterios para la evaluación y aceptación y límites, la identificación de los activos de información y los riesgos a los que estos puedan

verse expuestos, lo que puede permitir que las implementaciones e inversiones realizadas sean estratégicas y respondan a la necesidades de la organización.

Las mayores brechas percibidas por el sector salud es la seguridad en los dispositivos médicos, las amenazas persistentes avanzadas (APT), la fuga de información sensible, el aseguramiento de la infraestructura que se encuentra en la nube y sus infraestructuras críticas. De acuerdo con la revista Semana los avances sobre los equipos médicos como Software as a Medical Device (SaMD) y Internet of Medical Things (IoMT) abren una puerta para los ciber atacantes, incrementando el riesgo de que un incidente de seguridad de la información pueda materializarse, esto con el agravante que es uno de los sectores más deseados por los ciber delincuentes por la cantidad de información que almacenan (Semana, 2023), en Colombia por medio del Invima se cuenta con el programa institucional de Tecnovigilancia cuyo propósito es el de identificar eventos e incidentes asociados a dispositivos médicos y los riesgos asociados por su uso, sin embargo, dentro de este programa no se contempla un marco para la seguridad de la información y ciberseguridad en estos dispositivos (Invima, 2023).

Vectores de Ataque Más Explotados por los Ciberdelincuentes en las Organizaciones de Colombia y el Sector Salud

La pandemia llevo a las organizaciones colombianas a cambiar radicalmente su interacción con el mundo digital, en el país se veía lejana la incursión de nuevos métodos de trabajo como el teletrabajo o el trabajo hibrido, sin embargo, esto ya no fue una opción, si no el medio para dar continuidad a las operaciones ya que el 91% de las organizaciones se acogieron a estos métodos durante la emergencia, durante el 2020 se evidencio un incremento del 71% de colaboradores que pasaron a las modalidades antes dichas, lo que genero grande avances en la adopción digital.

Los crímenes cibernéticos también tuvieron numerosos incrementos, donde las denuncias por acceso abusivo a sistemas informáticos crecieron un 46%, en muchas organizaciones no se tomaron los controles de seguridad para hacer el cambio en la modalidad de teletrabajo esto fue rápidamente aprovechando por medio del protocolo RDP para el acceso a la infraestructura tecnológica (Castañeda Pérez, 2022).

De acuerdo con la revista perspectivas en inteligencia, se logran identificar tendencias presentadas en el año 2020 sobre el desarrollo del ciber crimen en Colombia, las organizaciones deben proyectar estas tendencias en el desarrollo de sus estrategias para la preservación de la integridad, confidencialidad y disponibilidad de los activos de información, dentro de ellos se destacan los ataques por medio de ingeniería social, amenazas persistentes avanzadas (APT), *ransomware* y sistemas sin parches (Mozo Rivera & Ardila Contreras, 2022), como lo identificamos anteriormente el sector salud no es ajeno a estas amenazas, de igual forma el estudio anual de ciberseguridad 2022-2023 de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) indica la relevancia que han tomado los ataques usando el spoofing

y el phishing (TicTac, 2023), a continuación, se detallan los ataques que se encuentran en tendencia.

Conforme al informe estrategia nacional digital de Colombia 2023-2026 del MinTIC (MinTIC, s.f.) donde al igual que los artículos explorados anteriormente se identifica el crecimiento de ataques en especial de malware, adicionalmente identifican las falencias en las organizaciones y ciudadanos frente a los hábitos de uso seguro de las tecnologías de información, donde se identifican brechas frente a lineamientos básicos que deben tener los ciudadanos como el uso de software antimalware e implementación de contraseñas seguras, estos dos factores sin duda permean las prácticas en el ámbito laboral de las organizaciones, en el estudio del Global Cibersecurity Index (GCI) Colombia obtuvo un puntaje de 6,67 sobre 20 puntos, lo que demarca el bajo desempeño organizacional de la ciberseguridad, de igual forma no se cuenta con un liderazgo a nivel gubernamental o de entes de control sobre los temas concernientes a la ciberseguridad y seguridad ya que actualmente, si bien los organismos actuales generan recomendaciones y lineamientos se encuentra descentralizado y no cuentan con los recursos y alcance para desarrollar las estrategias y liderazgo de la seguridad digital. Estos factores propician la materialización de los ataques descritos a continuación, ya que en su mayoría logran tener éxito al vulnerar la primera línea de defensa de las organizaciones, los usuarios y colaboradores, y las falencias organizaciones que frente al aseguramiento de su infraestructura y renovación tecnológica.

Vectores de Ataque

Amenazas Persistentes Avanzadas (APT)

Como lo indica el equipo de investigación de ESET a finales del 2022 se evidencio que fue orientada y desplegada una campaña de espionaje en Colombia dirigida a organizaciones de alto perfil como entidades gubernamentales, la cual fue nombrada operación absoluta.

Este ataque uso el malware AsyncRAT, este es un troyano que genera acceso remoto permitiendo la ejecución de actividades maliciosas, en este caso para el robo de información, este ataque se destaca por el uso de la técnica de ofuscación empleada, que facilita la evasión de controles de seguridad y dificulta el análisis de este (González, 2023).

Ransomware

La ingeniería social juega un papel fundamental en los ataques por medio de ransomware, de acuerdo con el artículo publicado por la Universidad de la Sabana, Colombia fue víctima de 4.4 billones de ataques durante el primer trimestre del 2020, estos tipos de ataque buscan manipular, influenciar y engañar a los usuarios para que realicen actividades maliciosas, esta técnica se basa en el error humano, estos son poco predecibles y de difícil detección, ya que las tecnologías para la protección del factor humano son limitadas son bastante vulnerables y adicionalmente el costo para llevarlo a cabo para el atacante es bajo, como se evidenciara más adelante con los siguientes tipos de ataques los ciber criminales no se limitan al uso de una técnica y la ingeniería social es usada con otros ataques como es el caso del phishing (Ingeniería social, la técnica de los delincuentes cibernéticos, s.f.).

De acuerdo con el estudio anual de ciberseguridad 2022-2023 de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), los ataques por medio de ransomware tuvo un aumento del 122% con respecto al 2021, aunque también se evidencio que los cibercriminales

hacen uso de un conjunto de técnicas que nos lleva a escenarios más difíciles de enfrentar. Los criminales llevaron a cabo múltiples ataques sobre las infraestructuras críticas de Colombia a lo largo del 2022, estos ataques tuvieron fuertes repercusiones por la información que se vio comprometida (TicTac, 2023).

Como lo indica *securelist*, los ataques por medio de ransomware siguen acaparando los titulares ya que no solo en Colombia, si no a nivel mundial los ataques son dirigidos a todas las industrias, llegando a poner la vida de los ciudadanos en juego, como ocurrió al momento de los ataques al sector salud, Kaspersky identifico un incrementó en la detección de ataques de este tipo del 20% respecto con el 2021, llegando a 74,2 millones esto a nivel mundial, en 2023 se ha tenido una disminución de estos pero los ataques generados han sido mejor dirigidos y más sofisticados que los que veíamos anteriormente.

Las herramientas que estos grupos emplean para sus ataques no han presentado cambios, ya que hacen uso de Mimikatz para escalar privilegios, para la recopilación de datos usan PowerShell y PsExec para la ejecución de comando de forma remota (Overview of ransomware trends in 2023, 2023).

En el caso del sector salud se vio gravemente afectada cuando uno de los principales proveedores de servicios de TI del estado sufrió un ataque de ransomware, en este ataque los servicios del Ministerio de Salud se vieron afectados, como lo fue el caso de la plataforma MIPRES y la Superintendencia Nacional de Salud (Supersalud), si bien este ataque afecto a múltiples entidades públicas y privadas, tuvo un gran impacto frente a la garantía de la prestación de servicios de salud para los ciudadanos, el ataque materializado corresponde a MarioLocker y comprometiendo el hipervisor de VMware, las máquinas virtuales de la empresa IFX fueron

secuestradas por medio del cifrado de la información afectando a 46 entidades públicas (ColCERT, 2023).

Como se expone en la revista hospitalaria este no fue el único ataque sufrido por el sector salud, ya que entre el 2022 y 2023 se presentaron ataques al Invima donde el ataque causo retrasos en la nacionalización de medicamentos y alimentos, esta entidad tuvo dos ataques en el mismo año, otra de las entidades que vio su infraestructura tecnológica crítica comprometida fue la EPS salud total impidiendo el acceso a la información, otra EPS que se vio impactada por este tipo de ataques fue la EPS Sanitas, este ataque afecto a más de 5 millones de usuarios presentando inconvenientes frente la atención de citas médicas, entrega de medicamentos, resultado de exámenes médicos y atención de los usuarios por los diferentes canales, entre las entidades de la salud que presentaron casos fue Audifarma y Cafam (Revista Hospitalaria, 2024).

Sistemas sin Parches

El caso no solo más reciente si no con gran repercusión fue el ataque realizado a IFX Networks el cual afecto a numerosas entidades del estado que ocasiono la interrupción de la prestación de servicios a la ciudadanía, este ataque tuvo lugar en septiembre del 2023, RansomHouse accedió a la infraestructura tecnológica por medio de la plataforma VMWare la cual no se encontraba actualizada y cuya versión contaba con una vulnerabilidad ya reportada y que fue explotada en este ataque, lo que es una gran omisión por parte de IFX como un proveedor de servicios de TI (García Rico, 2023), si bien el ataque inicio por ransomware como lo vimos anteriormente, las vulnerabilidades como en este caso facilitan a los atacantes su labor.

Conforme con el monitoreo y seguimiento realizado por el equipo de ESET en la región de Latinoamérica durante el 2022, lograron identificar las vulnerabilidades que tuvieron mayores intentos para ser aprovechadas, la identificación de estas tendencias ayudara a las organizaciones

a identificar los mecanismos de operación y establecer estrategias para la protección de estos, algo bastante particular es que se identificaron que dos de las vulnerabilidades fueron identificadas en el 2012 y 2017, lo que indica una gran brecha para la solución de estas por parte de las organizaciones ya sea por una política de instalación de parches débil o por el uso de tecnología obsoleta (Gutiérrez Amaya, 2022).

Phishing

Los atacantes han logrado mejorar los ataques basados en phishing, ya que la inteligencia artificial les permite mejorar los mensajes dirigidos a sus víctimas, disminuyendo los errores gramaticales y ortográficos, haciendo más eficiente la creación de páginas web suplantada y correos electrónicos, dentro de los avances por medio de estos ataques también se encuentra el deepfake, que permite suplantar personas de alta rango en las organizaciones en video, generando mayor credibilidad y sentido de urgencia. (TicTac, 2023)

Según Valora Analitik, Kaspersky registro 2.4 millones de intentos de ataques de phishing en Colombia durante el segundo semestre del 2022 y el primero de 2023, teniendo como resultado un promedio de 4 ataques por minuto, así como un incremento de 12.5% respecto al anterior periodo (Neira, 2023).

Spoofing

Si bien podremos encontrar similitudes entre este tipo de ataque y el phishing, el spoofing busca suplantar la identidad de un correo o página web en la que el usuario confié, recientemente se identificó un ataque dirigido a diferentes juzgados, donde el atacante quiso hacer creer a la víctima que el correo se trataba de juzgado segundo administrativo del circuito de Popayán y daba indicaciones para ingresar a un expediente, lo que resalta es que este corr

eo no indicaba un destinatario en particular ya que esto no era de conocimiento del atacante (Ataque masivo de suplantación de diferentes juzgados de Colombia, 2023).

El sector salud fue víctima de un ataque de spoofing, los atacantes aprovechando la emergencia sanitaria generada por el COVID-19, suplantaron el dominio de @minsalud.gov.co, dirigiéndose a ciudadanos y empresas del sector público y privado, con el propósito de distribuir malware (CCIT, 2021).

Credential Stuffing

De acuerdo al estudio trimestral realizado por CCTI se identificó un incremento en los ataques que no hicieron uso un programa malicioso, donde se especializan en la explotación de vulnerabilidades en la infraestructura tecnológica y el uso de credenciales legitimas, este tipo de ataque dificulta su detección y busca evadir las defensas tradicionales, las credenciales son obtenidas en la Deep web y Dark web donde fruto de anteriores ataques son obtenidas y ya que muchos usuarios tienen la práctica de reciclar usuarios y contraseñas o usan contraseñas fáciles o comúnmente utilizadas facilitan estos ataques. (Jaimovich, 2021).

Ataques a la Cadena de uministros

Este tipo de ataques a cobrado gran relevancia, como lo pudimos ver anteriormente en el caso de IFX Networks, proveedor de servicios de TI, el ataque tuvo un impacto muy alto en Colombia, como se indica en el estudio trimestral de ciberseguridad, durante el 2022 se identificó que se han incrementado los ataques a proveedores o terceros que cuentan con acceso a la red o recursos compartidos con las organizaciones a quienes prestan sus servicios, comúnmente las organizaciones cuentan con múltiples terceros, por lo que es de vital importancia garantizar que todos los proveedores cuenten con controles que salvaguarden la información y accesos generados (Bautista García & Mesa Guzmán, 2022).

Recopilación de Información

La fase de reconocimiento es vital para los atacantes, ya que podrá conocer a su objetivo, esta recopilación de información incluye información propia de la organización que se encuentre en la web, escaneo de su infraestructura tecnológica no intrusivo, sus redes sociales y también las redes sociales de sus empleados, esta información le permitirá evaluar los métodos de ataque que usara, como identificar el dominio de correo en que desplegara una campaña de phishing (Las 7 fases de un ciberataque. ¿Las conoces?, 2020).

Dominios Malignos

De acuerdo interpol durante la pandemia del COVID-19 este vector de ataque tuvo una incidencia del 22%, se evidencio el incremento de sitio web con nombres llamativos y que hacían alusión a la pandemia, el propósito de estos sitios era la de difundir malware y phishing, es por esto que las organizaciones deben contemplar dentro sus capacitaciones este tipo de vectores (Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19, 2020).

Factores Internos y Externos que Influyen en la Capacidad de Respuesta Incidentes de Seguridad de la Información

Las amenazas cibernéticas hacen parte de las organizaciones de todos los sectores, de hecho, estos ataques se han comenzado a dar hacia los ciudadanos, estas amenazas han tenido un gran avance, el entorno y contexto cambian constantemente, por lo que es fundamental identificar cuáles son los factores que juegan un papel crucial para la respuesta a incidentes de seguridad de la información y ciberseguridad, a continuación, serán evaluados factores desde un punto de vista interno y externo.

Factores Internos

Se realizará la validación de los principales factores internos que juegan un papel fundamental para la respuesta a incidentes, esto permitirá identificar las áreas que requieren acciones urgentes, dentro de estos factores encontramos la falta de una cultura de seguridad de la información, falencias o ausencia de la gestión de riesgos y un plan de respuesta a incidentes y por último, la protección de equipos médicos.

Cultura de seguridad de la información: Los usuarios son la primera línea de defensa de las organizaciones, desde la identificación de un correo de phishing, no hacer préstamo de contraseñas, hasta la identificación de comportamientos anómalos en las plataformas o aplicativos de la organización, por lo que la adopción de la seguridad es imprescindible.

Los profesionales del sector salud manifestaron en la XXIII Encuesta Nacional de Seguridad Informática que la ausencia de una cultura de seguridad de la información y ciberseguridad es uno de sus principales obstáculos para lograr una postura de seguridad madura y estable en las organizaciones, esta falta de cultura de seguridad se puede evidenciar desde la alta dirección ya que este ítem no es contemplado desde la estrategia de la organización y una de

sus principales causas de incidentes de SI es el error humano. Esta es una gran brecha que debe afrontar el sector ya que los usuarios deben conocer y entender el tratamiento que deben darle a los activos de información de acuerdo con la clasificación establecida, los riesgos con los que deben convivir y prevenir su materialización.

Gestión de riesgos y plan de respuesta a incidentes: Según la revista hospitalaria el sector salud se demora más en identificar un evento de seguridad, en promedio pueden tardar 329 días desde el momento en que inicia el ataque hasta el momento en que la organización detecta que sus sistemas fueron comprometidos y no menos alarmante el 80% de la información comprometida corresponde a datos personales de los usuarios. En la XXIII Encuesta Nacional de Seguridad Informática en el sector de la salud mayoritariamente se presentó de 1 a 3 incidentes de seguridad de la información, este se encuentra estrechamente vinculado con la gestión de riesgos, ya que una correcta gestión de riesgos le permitirá a la organización identificar controles que deban ser modificados o implementados, teniendo presente que existe una gran probabilidad de materialización de un incidente es vital que la organización cuente con un plan de continuidad.

Protección de equipos médicos: El sector de la salud cuenta con múltiples avances tecnológicos entre ellos los dispositivos IoMT, el propósito de estos dispositivos es mejorar la calidad en la prestación de los servicios de salud y la calidad de vida de los pacientes, es por esto que es de vital importancia obtener capacitación oportuna y adecuada sobre estos en términos de seguridad, estos dispositivos se encuentran cada vez más interconectados con la infraestructura crítica ya que almacenan y transmiten información sensible constantemente, los equipos médicos deben ser contemplados dentro de la gestión de activos de información y la gestión de riesgos

esto para identificar claramente la información que procesan y los riesgos asociados a su uso (Rosero, 2024).

Factores Externos

A continuación, se evaluarán los factores externos que impactan al sector salud para dar una respuesta a los incidentes de seguridad de la información, inicialmente se establecerá el entorno regulatorio, el cual le brinda al sector los lineamientos para la definición de responsabilidades, obligaciones y procedimientos, con estos lineamientos se buscará la prevención, detección, respuesta y recuperación para todas las entidades públicas y privadas del estado colombiano, el crecimiento exponencial que el cibercrimen ha tenido en el país y el aseguramiento de la cadena de suministros, es decir la dependencia que se tiene hacia los proveedores.

Entorno regulatorio: De acuerdo con los avances de las TIC en el 2009 en Colombia se sanciono la ley 1341, esta ley da los principios generales y políticas públicas que gobernarán al sector de la TIC en Colombia. Estableciendo su régimen de competencia, protección de los derechos de los usuarios, criterios para la prestación de servicios de telecomunicaciones, creación de la Agencia Nacional del Espectro y fomenta el desarrollo tecnológico. Esta ley contempla la importancia de las TIC para la prestación de los servicios de salud, el uso de estas en caso de emergencia y el despliegue de la telesalud (Congreso de Colombia, 2009) y es durante este mismo año que se reconocen los delitos informáticos dentro del Código Penal, para esto fue sancionada la ley 1273 para la protección de la información, en el año 2011 el CONPES 3701 dio los lineamientos de política para ciberseguridad y ciberdefensa, en este se resalta el establecimiento de organismos para la respuesta a incidentes de ciberseguridad de la nación y la promoción de una cultura de seguridad, algunas de las organizaciones creadas a partir de este son

el ColCERT y el centro cibernético policial (Revista Hospitalaria, 2024). La ley 1581 de 2012 para la protección de los datos personales, cuyo propósito es desarrollar el derecho que tienen las personas naturales frente a su información y la responsabilidad que tienen las organizaciones como encargados de su tratamiento, si bien esta ley comprende las bases de datos físicas como las digitales, ha sido una de las leyes que más ha impulsado la implementación de controles de seguridad, ya que es responsabilidad de las organizaciones la protección de los datos personales de sus usuarios, de hecho como lo hemos visto en gran medida este es uno de los mayores factores por los que el sector salud es tan apetecido por los ciberdelincuentes (Ley 1581 de 2012, 2012). En el año 2016 se generó el CONPES 3854, estableciendo la política nacional de seguridad digital, su objetivo es el de fortalecer las capacidades las partes interesadas dando gestión a los riesgos de seguridad digital de cara a las actividades socioeconómicas realizadas en el entorno digital. (CONPES 3854, 2016).

Por medio de la resolución 866 del 2021 del ministerio de salud cuyo propósito es el de reglamentar los lineamientos de datos clínicos relevantes para la interoperabilidad de la historia clínica en el país, esta resolución cuenta con el artículo 19, seguridad de la información y seguridad digital en se indica que todos los actores que participen en la interoperabilidad de los datos y las historias clínicas deben (Ministerio de Salud y. Protección Social, 2021):

- Tener una estrategia de seguridad y privacidad de la información, ciberseguridad y para la continuidad de su operación.
- Implementar un sistema de administración de riesgos operativos, en la cual se haga un monitoreo al riesgo de seguridad digital y la implementación de la guía para la gestión de riesgos de seguridad de la información del MINTIC.

- Establecer políticas, normas, procedimientos, instructivos y demás documentación técnica y normativa para dar gestión a la seguridad de la información y la mitigación de los riesgos.
- Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual es una guía dispuesta por el MINTIC, en la cual hacen la recopilación de las mejores prácticas basadas en la norma ISO27000 y se encuentra compuesto por cinco fases que buscan brindar una gestión eficiente para la seguridad y privacidad y a su vez propone un modelo de madurez.
- Implementar el procedimiento para la gestión de los incidentes de seguridad digital, de acuerdo con la guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MINTIC y los lineamientos para la estrategia de seguridad digital emitidos por el MINTIC.

Crecimiento en las amenazas cibernéticas**:** De acuerdo con portafolio y el informe de IBM X-Force, (Diaz Rico, 2024). Colombia sigue siendo el segundo país más atacado de la región, solo por detrás de Brasil, sin embargo, Brasil tiene cuatro veces más habitantes que Colombia. El ransomware sigue siendo la actividad maliciosa más ejecutada por los criminales, constituyendo el 31% de los ataques, esta técnica fue seguida por el acceso abusivo a la infraestructura tecnología y uso de herramientas o aplicativos con un propósito malicioso, estas dos técnicas con un 23%.

En este informe también se resalta que la gran mayoría de los ataques pudieron prevenirse o mitigado su impacto por medio de controles de seguridad ampliamente conocidos como es el de mantener la infraestructura tecnología actualizada y establecer procesos para su aseguramiento, adoptar los principios de Zero trust para la asignación de permisos y privilegios y

el despliegue de soluciones de múltiple factor de autenticación, ya que la contraseña no brinda una protección suficiente.

Por su parte el MinTIC (MinTIC, 2023) informo que en el 2023 se presentaron 54.121 denuncias por ciberataques, esta cifra presenta un aumento del 79% frente a 2021, por lo cual el ministerio contempla que Colombia debe robustecer su ciberseguridad, uno de los factores más importantes es que actualmente se está discutiendo el proyecto de ley para la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales, sin embargo, este no ha tenido grandes avances ya que de acuerdo con la silla vacía, en este momento se están presentado dos proyectos diferentes, uno presentado por un equipo de senadores y otro por el gobierno actual, lo que está poniendo en riesgo la creación de esta agencia, la cual debería ser prioridad, la ciberseguridad del país requiere de medidas que se den en el corto plazo y que sean efectivas (Parra & Rodríguez, 2024).

Aseguramiento de la cadena de abastecimiento: Actualmente no hay una empresa que pueda operar por si sola, es decir todas deben adquirir servicios y/o productos con proveedores, en el ambiente de las tecnologías de la información esto no es la excepción, donde cada vez encontramos más servicios en la nube y servicios SaaS, que dentro de sus principales ventajas esta la disminución de costos. En el sector de la salud se muestra una gran tendencia por la tercerización de servicios de ciberseguridad, adicional a esto y con el ataque que impacto a la compañía IFX, proveedor de múltiples organizaciones en el país y que en el caso de los servicios del MinSalud estuvieron fuera de línea, muestra la gran importancia que tienen los proveedores y el impacto a las operaciones, de acuerdo con el portal red seguridad, el ataque a proveedores se ha convertido en un blanco para los ciberdelincuentes, como en el caso de IFX que el aprovechamiento de sus brechas de seguridad comprometió la operación de sus clientes. La

pandemia acelero la llegada de la cuarta revolución industrial por lo que las organizaciones no estaban preparadas para ello, en su interior aun no contaban con una estrategia de seguridad de la información madura, lo que nublaba su visión frente a los criterios para evaluar a sus proveedores, es por esto que las organizaciones deben establecer como requisitos para la contratación de proveedores los estándares más altos en seguridad y su constante monitoreo durante la prestación de los servicios, evaluando los riesgos que pueda generar el proveedor y su impacto hacia la operación (Ciberseguridad en la cadena de suministro: objetivo de los 'malos', 2023).

Mecanismos que Contribuyan en el Aseguramiento y la Capacidad de Gestión de Incidentes en las Organizaciones del Sector Salud.

Como se ha podido evidenciar el sector salud se encuentra enfocado en la implementación de controles técnicos, sin embargo, es de vital importancia desarrollar controles organizacionales para garantizar que los controles tecnológicos implementados respondan a las necesidades de la organización y protejan correctamente los activos de información. Por lo que a continuación se sugiere la implementación de los siguientes mecanismos:

- Plan estratégico de seguridad de la información, conforme con el articulo salud y transformación digital (Vidal Ledo & Delgado Ramos, 2022), el proceso de transformación digital es vital para el sector salud para la mejora de las prestación de los servicios, propender por la interoperabilidad y garantizar el acceso a la salud a todos los ciudadanos , sin embargo, es crucial que esta transformación se encuentre acompañada de un plan estratégico y organizado que permita el crecimiento y transformación y no solo la migración de servicios a la nube, adquisición de servicios o demás infraestructuras por lo que se debe cambiar la cultura organizacional, por lo que se tendrán que incluir los siguientes ítems: Conectividad, arquitectura digital, estrategias para hacer la salud inclusiva para todos los sectores de la población, interoperabilidad con diversas entidades, inteligencia artificial y todo esto teniendo presente a seguridad de la información desde el momento del diseño.

- Plan de concientización en seguridad de la información, en el artículo "Cybersecurity and use of ICT in the health sector" de National Library of Medicine (Cervera García & Goussens, 2024), contempla dentro del modelo ideal de ciberseguridad en salud se debe contemplar la educación y concientización como un pilar fundamental dentro de la estrategia de seguridad y ciberseguridad, ya que las herramientas, tecnología y mecanismos de

seguridad serán insuficientes si no se cuentan con una adecuada cultura de seguridad, es primordial contar con un plan de concientización que sea ejecutado periódicamente, adicional a esto deben ser prácticos y adaptables tanto al contexto del sector como a las amenazas del entorno frente a la exfiltración de datos, siendo los usuarios el eslabón más débil o la primera línea de defensa.

- Gestión de activos de información, tal y como lo indica incibe en su artículo "Inventario de activos y gestión de la seguridad en SCI" (INCIBE, 2016), el inventario y gestión de activos es una pieza fundamental en un sistema de seguridad de la información, ya que permite la identificación de los activos vitales de la organización y sobre los cuales se deberá priorizar la identificación de los riesgos, así como el de garantizar que los activos cuenten con los controles de seguridad adecuados a su clasificación.

- Gestión de riesgos de seguridad de la información. De acuerdo con la Pirani empresa líder en la gestión de riesgos una parte fundamental de la gestión de la seguridad de la información es la mitigación de riesgos (Jiménez, 2023), el sector salud cuenta con una gran cantidad de información con datos personales sensibles de los ciudadanos por lo que es imperativo garantizar la protección de la organización previendo los incidentes de SI y la materialización de los riesgos identificados, así como el desarrollo de los planes de mitigación.

- Integración de la inteligencia artificial y aprendizaje automático para la mejora de la respuesta incidentes de seguridad de la información, de acuerdo con el estudio "Inteligencia artificial en la gestión predictiva de incidentes de TI", (Amaya Jave, 2024) se identifican los grandes aportes a la identificación y respuestas a incidentes por parte de tecnologías como la inteligencia artificial y el machine learning, ya que mejoran su precisión, ya que no solo mejoran los tiempos de detección, logran anticiparse ante actividades sospechosas que son conocidas,

haciendo esta labor más rápida, precisa y eficiente, esto apoyara al sector salud no solo a detecta y responder ataques más rápido, si no que apoyara su adaptabilidad frente a las nuevas amenazas.

- Respuesta a incidentes de seguridad de la información y buenas prácticas, de acuerdo con el informe de Kaspersky sobre la respuesta a incidentes (Kaspersky, 2023), dentro de sus recomendaciones resaltan la importancia de contar con un plan de respuesta a incidentes, donde este se articule con los proveedores que cuente la organización y se orqueste una respuesta a los incidentes de forma ágil y precisa, así como la gran relevancia que tiene la ejecución de pruebas y evaluación de tiempos de respuesta a los incidentes de seguridad de la información, lo que le permitirá a las organizaciones del sector salud a contar con su equipo de respuestas calificado y a ejecutar los planes de acción que sean necesarios para mejorar la respuesta a incidentes.

Plan Estratégico de Seguridad de la Información

De acuerdo con la publicación realizada por el BID protegiendo la salud digital. Una guía de ciberseguridad en el sector de salud (Libedinsky et al., 2021) es de vital importancia ejecutar un plan estratégico de la seguridad de la información que permita articular controles técnicos, procedimentales y personas para el fortalecimiento de la seguridad de la información, para esto se deberán seguir los siguientes pasos:

1. Identificar los objetivos estratégicos de la organización: Se deberán identificar los objetivos estratégicos de la alta dirección y en caso de que no hallan objetivos orientados a la seguridad de la información y ciberseguridad realizar su inclusión.

2. Establecer la estructura organizacional para la seguridad: Ya que conocemos los objetivos que deben ser alcanzados, se debe evaluar si la estructura actual cumple con los requerimientos necesarios para alcanzar los objetivos trazados, en caso contrario de debe lograr

establecerla, es importante que esta estructura pueda contar con un responsable y un comité para la seguridad de la información y ciberseguridad.

3. Definir los objetivos del área: Una vez conocemos la estrategia de la organización, las partes involucradas en la seguridad de la información y ciberseguridad deben establecer los objetivos y metas que se deben cumplir todo esto alineado con la estrategia de la organización y teniendo en cuenta las partes interesadas, como lo es el entorno regulatorio. También es necesario establecer periodos de seguimiento y métricas que permitan a la organización identificar cuando se está en riesgo de no cumplir con uno de los objetivos trazados.

4. Ejecutar un diagnóstico de brechas: Ahora bien, es momento de que la organización identifique cuál es su estado actual, esto puede ser realizado por medio de un análisis de brechas que corresponde a identificar el grado de madurez de la organización frente a la implementación de los controles de uno o más estándares y buenas prácticas, adicional a este análisis es muy importante que este proceso se realice en conjunto con la gestión de riesgos con el propósito de realizar una correcta priorización.

5. Generar el plan estratégico de seguridad de la información y ciberseguridad: Los responsables de la seguridad de la información y ciberseguridad de la organización deben desarrollar este plan propendiendo por su alineación con la estrategia de la entidad y los objetivos propios del área, los proyectos o planes de acción a ejecutar deben responder a las brechas de seguridad identificadas por medio del análisis de brechas y a la mitigación de los riesgos, estos proyectos deberán integrar controles técnicos, procedimentales y personas, con el propósito de que estos puedan atender holísticamente las necesidades, se deberán establecer tiempos de implementación y los mecanismos para ejecutar su medición.

6. Ejecución del plan estratégico de seguridad de la información y ciberseguridad: Se deberá realizar un monitoreo oportuno a la ejecución de los proyectos o planes de acción para la identificación de limitaciones o desvíos. La medición y seguimiento a la ejecución del plan debe realizarse con los mecanismos de medición identificados.

7. Evaluación de los resultados: Una vez sea ejecutado el plan estratégico de seguridad de la información y ciberseguridad se deberá realizar la evaluación de los resultados, se deberá realizar la evaluación de los riesgos identificando si su mitigación cumple con los resultados esperados, adicionalmente se podría realizar un análisis de brechas dando prioridad a los aspectos en lo que se identificaron falencias previamente.

Plan de Concientización de Seguridad de la Información

Como se ha logrado evidenciar el factor humano es una de las brechas que más sobre salen en el sector salud es por esto, que se recomienda la implementación de un programa de concientización (Martínez, 2020), este debe contemplar, sin limitarse a ellos:

Garantizar el conocimiento y aplicación de la política de seguridad de la información.

Asegurar el conocimiento de los roles y responsabilidades en seguridad de la información y ciberseguridad de todos los colaboradores, incluyendo procesos sancionatorios en caso de incumplimiento.

Establecer las temáticas abordar a lo largo del año y su mecanismo de comunicación (correo, infografías, capacitaciones en línea, ente otras). Dentro de las temáticas a abordar deben ser incluidos los incidentes generados por errores humanos, la identificación de ataques de ingeniería social, tratamiento de los activos de información y las rutas para el reporte de incidentes y eventos de SI.

Establecer los mecanismos de evaluación de los conocimientos por parte de los colaboradores, así como las métricas e indicadores para evaluar la ejecución del plan de concientización.

Gestión de Activos de Información

Comúnmente los equipos de TI tienen una visión parcial de los activos, por lo que es imperativo que se realice una correcta gestión de activos, donde toda la organización tenga participación, esta gestión también ayudara a mitigar los activos o aplicativos que el departamento de TI desconoce, ya que como sabemos muchas áreas realizan contrataciones por su cuenta por lo que TI pierde visibilidad, la gestión de activos de información permitirá identificar donde están las joyas de la corona de la organización.

Conforme a la guía para la gestión y clasificación de activos de información del MINTIC que da directrices básicas para las organizaciones públicas y privadas puedan desarrollar esta gestión, esta guía se encuentra basada en la norma ISO/IEC 27001:2013, anexo A. donde establecen los siguientes controles (MINTIC, 2016):

Inventario de activos: El propósito de este es identificar de forma clara y precisa todos los activos de información que tenga la entidad u organización, para el levantamiento de este inventario se debe establecer el tipo de activos que serán documentados, este debe contemplar sin limitarse a estos el nombre del activo, descripción, proceso al que pertenece, tipo de activo. responsable y custodio, clasificación, criticidad para la organización, ubicación y controles de seguridad dispuestos.

Se deben establecer un proceso y periodicidades para la revisión de los activos, mínimo se debe contemplar una revisión al año, sin embargo, son los dueños de proceso y dueños de los

activos quienes deben tener la responsabilidad de reportar cualquier novedad frente a sus activos en el momento en que se presente la novedad.

Clasificación de la información: La clasificación es sumamente importante, ya que por medio de esta la organización establecerá los controles de seguridad normativos y lógicos de acuerdo con la criticidad del activo, de igual forma el tratamiento que este debe recibir por los colaboradores al momento de interactuar con estos, para la clasificación de la información tendremos como referente la confidencialidad, integridad y disponibilidad del activo de información.

Etiquetado y tratamiento de la información: Por último, se deberá realizar el etiquetado de los activos de información, esto es vital, ya que los colaboradores podrán identificar rápidamente los criterios con que debe ser tratada el activo, sin embargo, esto no sustituye la sensibilización que debe ser realizada.

Por su parte la norma ISO/IEC 27002:2022 contempla de igual forma el inventario de activos de información, clasificación de la información y etiquetado de la información. Adicionalmente contempla en su numeral 5.10 el uso aceptable de los activos de información donde se recomienda la implementación de una política para este fin, esta política debe establecer una guía clara de cómo los colaboradores deben usar e interactuar con los activos, acciones o actividades que están prohibidas, en el marco del cumplimiento de la protección de los datos personales se debe contemplar la generación de un flujo donde se establezca todo el ciclo de vida del activo y controles dispuestos por la organización acordes a la clasificación del activo (ISO (International Organization for Standardization), 2022a).

Gestión de Riesgos de Seguridad de la Información

Dentro de las guías de buenas prácticas dispuestas en la familia de la ISO 27000, se cuenta con la norma ISO/IEC 27005:2022 seguridad de la información, ciberseguridad y protección de la privacidad. Guías para la gestión de los riesgos de seguridad de la información, esta contempla ((ISO (International Organization for Standardization), 2020):

Contexto: Inicialmente contempla el establecimiento del contexto de la organización para la gestión de riesgos y establecer el apetito del riesgo, es decir cuál es ese nivel de riesgo que la organización está dispuesta asumir, se deben contemplar las necesidades de las partes interesadas como el cumplimiento normativo que se debe tener en cuenta.

Una parte fundamental en esta fase es establecer los criterios para la evaluación del riesgo, determinar el nivel del riesgo y aceptación del riesgo, es decir como la organización identificara que tan importante es un riesgo, así como escoger el método que sea más adecuado para la organización.

Evaluación del riesgo: En esta fase del proceso, se deberá identificar los riesgos y sus propietarios, para esto se identificarán los eventos que puedan impactar negativamente a la organización y que se estén asociados a la perdida de la confidencialidad, integridad y disponibilidad, teniendo como referencia los activos de información previamente identificados, para la identificación de los riesgos se puede contemplar bajo dos enfoques, basado en la vulnerabilidades y amenazas y con un enfoque basado en eventos.

Una vez contemos con los riesgos identificados, se deberá hacer la evaluación de los riesgos en términos de impacto es decir cuáles son las causas que puede tener la materialización del riesgo identificado y en términos de la probabilidad de la ocurrencia, estos sin tener en cuenta los controles dispuestos para la protección de los activos. Con estos dos factores identificados

podremos seguir con la determinación del nivel de riesgo, esto comúnmente realizado por medio de un matriz de calor, este será nuestro riesgo inherente.

Por último, se deberán identificar los controles técnicos y normativos con los que cuenta la organización para mitigar los riesgos establecidos, estos controles podrán ser evaluados en términos de su tipo, si es preventivo, correctivo o detectivo, grado de madurez, histórico de fallas, complejidad para su ejecución, entre otros. Una vez se cuente con esta evaluación de controles frente al riesgo inherente, podremos obtener el riesgo residual, es decir el nivel del riesgo teniendo en cuenta los controles dispuestos por la organización para su protección.

Plan de tratamiento: Con el riesgo residual identificado y basado en los criterios de aceptación establecidos, se deberán generar los planes de tratamiento requeridos para los riesgos, las opciones de tratamiento que puede contemplar las organizaciones son evitar, eliminar la fuente del riesgo; modificar, establecer controles para modificar el impacto o la probabilidad; aceptar, mantener los controles actuales o compartir, transfiriendo o dividiendo las responsabilidades con una o más partes interesadas.

Como se indica anteriormente la gestión de riesgos permitirá tener un enfoque estratégico, ya que se podrá establecer si los controles actuales cubren las necesidades de la organización y en caso de requerir la implementación de controles adicionales se podrán justificar plenamente su necesidad y función en la organización, de igual forma que como la gestión de activos se deben establecer una periodicidad para la revisión de los riesgos, sin embargo, los cambios en el contexto, activos o la materialización de un riesgos deberán ser disparadores para activar nuevamente el ciclo de evaluación de los riesgos.

Integración de la Inteligencia Artificial y Aprendizaje Automático para la Respuesta a Incidentes de Seguridad de la Información

El aprendizaje automático o machine learning y la inteligencia artificial (IA) juegan un papel fundamental en la era actual y no es diferente en el caso de la respuesta a incidentes de seguridad de la información y ciberseguridad, de acuerdo con el articulo “El SOC “autónomo”: inteligencia artificial para la nueva ciberseguridad” (Serna Navarro & González Guerrero, 2022) las organizaciones sin importar su tamaña y sector económico, cuentan con números indeterminados de activos y que con los cambios generados por la pandemia no se encuentran centralizados, adicional a esto se cuenta con un gran número de herramientas de ciberseguridad que en el peor de los casos no estarán integradas, por lo que hace inmanejable la gran cantidad de alertas y eventos presentados, con la ayuda de la IA y el machine learning se identifican cuatro propósitos. Primero, la gestión de datos a nivel masivo, identificando y priorizando los eventos que deben ser evaluados y con el aprendizaje continuo su identificación será más precisa minimizando los falsos positivos; Segundo, llegar a tener una respuesta en tiempo real, como lo hemos visto anteriormente de acuerdo con su rápido procesamiento se podrá identificar y anticiparse a escenarios de riesgo, así como identificando actividades anómalas en el comportamiento de los usuarios apalancando la rápida detección; Tercero, de acuerdo con el aprendizaje que puede tener y los tareas preconcebidas como el aislamiento de un equipo con actividad sospecha, podrá mejorar la detección y contención de ataques informáticos; Y por último la predicción, una mejora constante en la defensa cibernética, ya que no solo identifica y aprende patrones presentados en la infraestructura tecnológica, si no que puede tener ingesta de información desde las fuentes que considere el fabricante por lo que la solución permitirá tener

una mayor adaptabilidad al contexto de los ciberataques, así como la identificación de indicadores de compromiso (IoC).

Ahora bien, para su implementación la organización deberá contemplar:

- Establecer un modelo de gobernanza y una estrategia para el despliegue de estas nuevas tecnologías donde continuamente se evalúen los riesgos y su uso ético.
- La identificación de proveedores y socios estratégicos, propendiendo la adquisición de servicios con organizaciones expertas que con su experiencia permita la mejora de la postura de la ciberseguridad y donde se busque unificar herramientas y su compatibilidad entre sí.
- Establecer el data lake o plataforma de datos donde se recolectará y almacenará la información generada por las diversas fuentes.
- Formación y capacitación para los analistas de ciberseguridad y demás roles que realizaran el uso de estas nuevas tecnologías.
- Establecer un plan de pruebas o monitoreo para los sistemas, esto para garantizar la calidad de los reportes y eventos generados e identificar problemas de sesgo.

Adicionalmente estas nuevas tecnologías no solo apoyan la respuesta a incidentes de seguridad de la información y ciberseguridad, las organizaciones las podrán usar para la administración de identidades, administración de puntos de conexión y seguridad de la red, seguridad en nube, protección de la información e investigación ante eventos e incidentes. (Microsoft, s.f.)

Buenas Prácticas para la Gestión De Incidentes

Conforme con la XXII Encuesta Nacional de Seguridad Informática se ha evidenciado una disminución de las organizaciones que no usan ningún marco de seguridad para el control de

su operación, los marcos más implementados son la norma ISO 27001 con un 69%, NIST con 37% e ITIL con 26%, las cuales abordaremos a continuación (Almanza J, 2022).

La implementación y adopción de normativas, frameworks y buenas prácticas en el ámbito de la seguridad de la información es de vital importancia, ya que estos han sido generados por grupos de expertos y son transversales a cualquier organización sin importar su tamaño o sector, como lo validaremos más adelante estas buenas prácticas son compatibles entre sí, por lo que su adopción por parte de las organizaciones fortalecerá la postura de seguridad de la información.

ISO 27001:2022.

Acorde con la cifra anteriormente indicada la norma ISO 27001:2022 para la seguridad de la información, ciberseguridad y protección de la privacidad. Sistema de gestión de la seguridad de la información, tiene un 69% de adopción por parte de las organizaciones, esta norma establece los requisitos para el establecimiento del sistema de gestión, todo esto en el marco del ciclo PHVA que garantiza la mejora continua, si evaluamos esta norma encontraremos que sus numerales responden a cada una de estas fases asegurando la mejora continua.

Ahora bien en la norma ISO 27001:2022 se encuentran los requerimientos para establecer el contexto de la organización, entender las necesidades de las partes interesadas y por su puesto establecer el alcance que tendrá el sistema de gestión dentro de la organización, esto es un punto importante ya que si bien una organización puede estar alineada con esta norma no necesariamente tendrá un cubrimiento hacia toda la organización; también genera directrices que demuestren el liderazgo y compromiso de la dirección con el sistema de gestión, la implementación de la política, el establecimiento de roles, responsabilidad y autoridad; en el numeral de planeación nos hablan sobre la gestión de riesgos, el establecimiento de objetivos de

SI y la planificación de cambios organizacionales; ahora en el numeral de soporte nos hablara sobre las directrices para proveer los recursos necesarios para el establecimiento, mantenimiento y mejora del sistema, la información documentada del sistema, las competencias requeridas por el personal para la gestión del sistema, su capacitación y toma de conciencia en SI; en el apartado de operación se encuentran los lineamientos para la planificación y control operacional, así como la importación de la evaluación de los riesgos de la seguridad de la información; en los últimos dos apartados contamos con las directrices para llevar acabo el seguimiento, análisis, medición y evaluación del sistema de gestión, la generación de auditorías internas, el seguimiento por la alta dirección y por ultimo los aspectos relacionados con la mejora continua (ISO (International Organization for Standardization), 2022).

Esta norma cuenta con el anexo A o ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad: Controles de seguridad de la información en esta encontraremos lineamientos del orden organizacional, ha personas, físicos y por supuesto tecnológicos, en esta norma encontraremos los lineamientos que nos hablan de una forma más precisa sobre la gestión de incidentes de la información que abarcaremos ahora (ISO (International Organization for Standardization), 2022a).

Control 5.24, planificación y preparación: Este control tiene como propósito asegurar una respuesta coherente, eficaz y ordenada a los eventos e incidentes de SI, nos indica que la organización debe planificar y prepararse para dar una correcta gestión a los incidentes de SI, por medio de procesos, responsabilidades y funciones que deben ser definidos y comunicados, la organización puede seguir estos lineamientos:

Generar un mecanismo conocido por los colaboradores para facilitar el reporte de incidentes y eventos de SI;

Documentar y establecer un procedimiento para la gestión de incidentes de SI;

Generar el procedimiento para la respuesta a incidentes de SI para la evaluación, respuesta y aprendizaje de estos;

Garantizar la capacitación y certificación continua del personal a cargo de la gestión de incidentes de SI;

Control 5.25, evaluación y decisión sobre eventos de SI: Su propósito es el de garantizar que la categorización y priorización de los eventos de SI sea realizada de forma efectiva, por lo que las organizaciones deben evaluar los eventos y decidir si deben ser clasificados como un incidente de SI, por lo que se deberá establecer un esquema para la categorización y priorización.

Control 5.26, respuesta a los incidentes de SI: Este control busca asegurar que la respuesta los incidentes de SI es dada de una forma eficaz, para dar cumplimiento a este numeral la organización debería incluir en sus procedimientos la documentación de:

Los sistemas que fueron afectados;

Evidencias del incidente de SI, así como salvaguardarlas;

Escalamientos requeridos;

Comunicación y coordinación del incidente de SI a las partes interesadas;

Análisis post-incidente.

Control 5.27, aprendizaje de los incidentes de SI: Este control tiene como propósito el de reducir la probabilidad de que vuelvan a presentarse incidentes o mitigar su impacto, por lo que los conocimientos generados a partir de los incidentes de SI deben usarse para fortalecer los controles implementados, de igual forma se debería documentar los tipos de incidentes y sus costos para la organización.

NIST V 1.1

El Instituto Nacional de Estándares y Tecnología (NIST) pertenece del gobierno de EE. UU., esta guía fue desarrollada para para la protección de las Infraestructuras Críticas de dicho país, no obstante, este ha sido adoptado a nivel mundial, ya que es ampliamente aplicable a organizaciones de todos los sectores y tamaños, este framework ha sido desarrollado sobre otros estándares reconocidos en la industria como:

NIST SP 800-53, guía de cumplimiento.

ISO/IEC 27001:2013, sistema de gestión de seguridad de la información;

CIS CSC, controles críticos de seguridad CIS;

Cobit 5, framework para el gobierno y gestión de TI;

ISA 62443-2-1:2009 4 e ISA 62443-3-3:2013, sistema de control de seguridad para sistemas automatizados y control industrial;

Este framework busca brindar una guía frente la administración de la ciberseguridad, tal vez esta sea la principal diferencia respecto con el estándar antes visto, teniendo como foco la correcta gestión de los riesgos, es una guía más técnica y cuenta con cinco funciones principales, las cuales son (National Institute of Standards and Technology (NIST), s.f.):

Identificar: Dentro de esta función la organización debe establecer los roles y responsabilidades para ciberseguridad, identificar los procesos críticos de negocio, así como establecer las políticas y procedimientos requeridos, establecer la gestión de activos críticos, gestión del riesgo de ciberseguridad y gestión de los proveedores críticos.

Proteger: Esta función contempla la gestión de accesos físicos y lógicos desde su alta, baja y modificación, diseñar y establecer la política de respaldo y garantizar su cumplimiento, política de parchado y cronograma para la aplicación a la infraestructura tecnológica, la gestión

de incidentes de ciberseguridad y plan el capacitación y concientización para colaboradores internos y proveedores.

Detectar: Esta función permitirá identificar y categorizar con el apoyo de herramientas de seguridad a nivel endpoint y de seguridad perimetral los eventos e incidentes de ciberseguridad.

Responder: Las pruebas a los planes de respuesta de incidentes de SI son vitales para las organizaciones ya que garantizaran que estos sean vigentes y coherentes a la operación, a su vez el personal podrá ser entrenado correctamente para dar una respuesta eficaz, se deben establecer los mecanismos de comunicación al momento de ser necesarios, como puede ser la comunicación a la mesa de crisis.

Recuperar: Los planes para la recuperación de la operación de igual forma requieren pruebas periódicas, esta permitirá garantizar que todos conozcan su rol y función y que los documentos generados responden a las necesidades y se encuentran actualizados y adquirir de seguros para ciberseguridad.

Al igual que la norma ISO27001:2022 esta guía cuenta con la NIST SP 800-61 que da un zoom hacia el manejo de incidentes, esta guía contempla cuatro etapas (National Institute of Standards and Technology (NIST), 2021):

Preparación: Esta etapa busca no solo establecer la capacidad para dar respuesta a los incidentes de SI, también busca la prevención de estos asegurando la infraestructura tecnológica y aplicaciones de forma robusta, esta guía contempla las siguientes recomendaciones en estas dos áreas:

Matriz de contactos con las personas de la organización, organismos y equipos externos para la respuesta a incidentes;

Comunicación de mecanismos para la notificación de incidentes;

Mecanismos para el seguimiento a los incidentes y problemas;

Establecer la sala de crisis;

Mecanismos para la protección de información confidencial y evidencias de los incidentes;

Estrategias de respaldo y recuperación de los sistemas;

Herramientas para hacer análisis de tráfico, analizar protocolos y rastrear paquetes;

Documentación extensa sobre la infraestructura tecnológica;

Simulación de incidentes para la preparación del personal ante un incidente real;

Llevar a cabo la gestión de riesgos de forma juiciosa y exhaustiva;

Reforzar los lineamientos y controles de seguridad de la infraestructura tecnológica;

Implementación de mecanismos para la detectar y detener ataques de malware;

Plan de capacitación y concientización a los colaboradores.

Detección y análisis: Como ya sabemos los incidentes pueden materializarse en cualquier momento, a pesar de las medidas tomadas, esta fase contempla: Identificar los vectores de ataque de la organización, mecanismos y herramientas para la detección de incidentes de SI, es importante que estos funcionen de forma conjunta para una mejor analítica, entrenar a los responsables para la identificación de incidentes de SI, garantizar la correcta documentación, priorización y notificación de los incidentes de SI.

Contención, Erradicación y Recuperación: Esta fase es fundamental para la mitigación del impacto del incidente a la organización, se deben contemplar herramientas y mecanismos necesarios para poder contenerlo y recuperarse de este, esta guía indica: Establecer una estrategia para la contención, esto puede tener como resultado un documento por cada tipo de incidente identificado, generar mecanismos para la recopilación y manejo de pruebas, en la medida de lo

posible identificar el host atacante, identificar los equipos afectados, acciones para la erradicación como eliminar el malware, mitigar vulnerabilidades explotadas o bloqueo de cuentas y restauración de la operación de acuerdo con las estrategias requeridas, de ser necesario la activación del DRP, esta decisión debe ser tomada antes de una afectación irremediable a la organización.

Actividades post incidentes: Por ultimo las organizaciones deben aprender de lo ocurrido por medio de la generación de reportes que permitan identificar claramente el proceso dado al incidente, los costos generados y desarrollar actividades que permitan prevenir nuevos incidentes de SI. Se pueden generar reuniones para hacer retroalimentación a nivel de equipo, planes de acción a partir de la información recopilada y las pruebas de los incidentes de SI deben ser contempladas en las políticas de retención documental.

ITIL V4

En su nueva versión ITIL diseña una práctica para la gestión de la seguridad de la información con el propósito de proteger la información; entender y dar gestión a los riesgos que impacten la integridad, disponibilidad y confidencialidad; asegurar la autenticación y el no repudio, lo anterior haciendo uso de políticas, procesos, controles y la gestión del riesgo, buscando prevenir, detectar y corregir.

Para el proceso de gestión de incidentes de seguridad de la información nos plantea las siguientes fases (InvGate, 2021):

Preparación: Contar con mecanismo que permitan dar respuesta a un incidente SI, como lo es la política de SI aprobada y comunicada, activos críticos del negocio o plan de respuesta, sin limitarse a estos.

Detección y escalamiento: Monitorear activamente la infraestructura tecnológica, contar con un procedimiento que permita hacer un correcto escalamiento y garantizar que la identificación y respuesta a los eventos de seguridad sea rápida, oportuna y eficaz.

Triage y análisis: En esta fase se realizará la recopilación de la información necesario para evaluar el incidente de SI;

Contención y recuperación: En esta fase se deberán llevar a cabo las acciones que permitan la contención del incidente y de ser necesario la recuperación de los activos de información;

Actividad posterior al incidente: Esta fase busca identificar las lecciones aprendidas, como realizar un análisis causa raíz y la generación del informe respectivo.

Guía para la Gestión de Incidentes de Seguridad en el Tratamiento de Datos Personales de la SIC

En el marco de la ley 1581 de 2012 para el tratamiento de datos personales, la Superintendencia de Industria y Comercio en adelante SIC emitió una guía para la gestión de incidentes de seguridad de la información en los que se vean impactados datos personales, esto teniendo como base que en ausencia de seguridad no abra un tratamiento de los datos personales adecuado.

La guía desarrollada por la SIC (Superintendencia de Industria y. Comercio, 2020) tiene como objetivo brindar recomendaciones a los responsables y encargados del tratamiento de los datos personales gestionados y custodiados por las organizaciones, ya que al igual que otras normas y/o frameworks las organizaciones deberán adaptarlo a su contexto y necesidades, estas deberán definir los controles y mecanismos necesarios para la respuesta ante un incidente de seguridad de la información.

De acuerdo con el marco normativo de la ley 1581 de 2012 todos los incidentes de SI deberán ser reportados a la SIC en un término de 15 días hábiles a partir de la identificación del incidente y que los responsables del tratamiento sean puestos en conocimiento, esto aplicara a todas las organizaciones tanto las que deben registrar sus bases de datos en el RNBD como las que no están obligadas hacerlo, los incidentes deberán ser reportados sin excepción.

Dentro de esta guía también se resalta la importancia del control hacia terceros en especial cuando se cuenta con servicios como cloud computing la exigencia del cumplimiento de la política de protección de datos legales estipulada por las organizaciones y los requerimientos legales, ya que si bien se realiza la tercerización de servicio no exime a la organización de las responsabilidades con los titulares de los datos, por lo que es de vital importancia la creación de acuerdos vinculantes y que en este se estipulen los siguientes requerimientos:

- Proceso para la respuesta de incidentes de SI;
- Estipulación de roles y responsabilidades, así como la matriz de contactos;
- Procedimiento para tramitar consultas por parte de los titulares;
- Reporte de incidentes de SI por parte de otros terceros o sub encargados;
- Alinearse y dar cumplimiento a la política de tratamiento de la organización;

En la guía se establecen los registros necesarios para evitar la recurrencia de incidentes de SI y adicionalmente lograr brindar los soportes necesarios al momento de una investigación, la información que se relaciona a continuación debe ser exhaustiva y debe tener los detalles requeridos para lograr establecer el correcto proceder de la organización y deben conservarse con los controles de salvaguarden la confidencialidad, integridad y disponibilidad.

- Descripción de las circunstancias en las que se presentó incidente de SI, incluyendo las bases de datos y datos personales impactados;

- Fecha y hora en la que se presenta el incidente, así como su fecha de descubrimiento de este;
- Responsables dentro de la organización del tratamiento de los incidentes de SI;
- Identificar la categoría a la que pertenecen los titulares afectados;
- La investigación realizada por la organización;
- Planes de acción y medidas correctivas llevadas a cabo;
- Pruebas de los reportes realizados a la SIC y titulares informados de la materialización del incidente, este último en caso de que fuese necesario;
- La evaluación de riesgos llevaba a cabo a raíz del incidente de SI presentado;

A continuación, se relacionan los pasos para la atención de un incidente de seguridad de la información:

Contención el incidente de seguridad: Al momento de que se identifique un incidente de SI se deben tomar acciones de forma inmediata para mitigar el impacto, la organización debe asegurarse de no eliminar evidencias del incidente. Se deberá iniciar la investigación inicial del incidente, esto con el objetivo de dar respuesta a los interrogantes:

- ¿Cómo se originó, cuándo y dónde ocurrió?
- ¿Cuál fue su raíz y quién lo identifico?
- ¿Aún se presenta fuga de información?
- ¿Cuenta con acceso a los datos?
- ¿Cuáles son los controles necesarios para salvaguardar la información o reducir el impacto?
- ¿Se debe notificar a los titulares de la información sobre la ocurrencia del incidente inmediatamente?

Evaluar los riesgos e impactos asociados a los incidentes: Se deberá realizar una exhaustiva gestión de los riesgos para la identificación y evaluación de estos, frente a la probabilidad de afectación a los titulares de la información, así como el nivel de riesgo para sus libertades y derechos, se deberá identificar el tratamiento hacer hacia estos.

La calificación del riesgo dependerá de la metodología de la organización estos pueden ser categorizados como bajo, medio, alto y grave, la evaluación de estos riesgos debe tener en cuenta la clasificación de los riesgos y el contexto en que se da el incidente, dentro de esta fase se podrá dar respuesta a las siguientes preguntas:

- ¿Cuántas personas fueron afectadas y en que categoría se encontraban?
- ¿Por cuánto tiempo se vieron comprometidos los datos?
- ¿Qué tipo de información personal se vio afectada, es sensible?
- ¿Los datos comprometidos estaban cifrados y anonimizados?
- ¿Qué uso le podría dar el atacante a esta información?
- ¿La información robada ha sido expuesta en internet?
- ¿La información objeto del ataque fue recuperada?
- ¿Cuáles son las causas y el alcance del incidente?
- ¿El incidente es recurrente?
- ¿Cuáles mecanismos se han tomado para mitigar el impacto?

Identificación de daños: En esta fase se deberán evaluar los daños que se pudieron generar a la organización, personas y al público, estos podrían ser a nivel organizacional afectación de la reputación, pérdida de clientes, pérdida de confianza, perdida de activos o sanciones; a nivel de personas pueden haber riesgos a nivel de la seguridad e integridad de la persona, extorción, suplantación o discriminación; por ultimo a nivel la ciudadanía o el público

se pueden generar riesgos a la seguridad y salud pública, alteración del orden o pánico económico.

Notificación a la SIC: Como lo indicamos anteriormente todas las organizaciones con domicilio en Colombia deben hacer el reporte de la materialización de un incidente de SI dentro de los siguientes quince días hábiles.

Comunicar a los titulares afectados: Esta notificación es necesaria para que los titulares de los datos puedan tomar medidas para su protección, también se deberán brindar herramientas para que estos puedan minimizar el daño. Por lo que es de gran importancia que la organización documente claramente dentro de sus procesos, cuándo, cómo, a quién y que se debe comunicar.

Prevenir futuros incidentes: La organización deberá desarrollar un plan de prevención con el fin de prevenir la ocurrencia de este tipo de eventos, dentro de estas actividades pueden estar la ejecución de auditorías, robustecer los diferentes controles y creación de planes de trabajo.

Conclusiones

Desde el inicio de la pandemia los ciberataques han ido en aumento, como hemos logrado evidenciar dentro de los vectores de ataque más representativos en Colombia y el sector salud se encuentran los ataques por medio de ramsomware, sin embargo, estos son cada vez más sofisticados, generando importantes retos en materia de capacitación y adopción de la ciberseguridad por parte de los colaboradores, ya que estos ataques siguen teniendo un alto impacto y de fácil ejecución, adicionalmente, se logró evidenciar que las vulnerabilidades más explotadas en el país en promedio tienen 7 años desde su descubrimiento, lo que muestra la gran brecha que tienen las organizaciones para llevar a cabo una correcta gestión de la capacidad o renovación tecnológica y una gestión de parchado, adicional a esto el sector salud presenta brechas frente a la articulación de los controles técnicos con controles normativos y estos a su vez orientados con la estrategia de la organización.

Actualmente se cuenta con numerosos marcos para la gestión de la seguridad de la información si bien mayoritariamente estos son internacionales, el gobierno nacional se ha comenzado a apropiar de este ámbito generando resoluciones como es el caso del MinSalud para que las organizaciones que se encuentran inmersas en la gestión de datos e historias clínicas fortalezcan su postura de seguridad, por su parte el MinTIC ha generado guías para una correcta gestión de los incidentes de información, por lo que se puede evidenciar que el gobierno entiende las necesidades e importancia del sector.

Las organizaciones en Colombia han incrementado la adopción de estas buenas prácticas durante la última década, sin embargo, las brechas a tratar aún son extensas en materia de ciberseguridad, como una adopción del proceso de gestión de activos, gestión de riesgos y gestión de incidentes de seguridad de la información, siendo el sector salud uno de los más

atacados los avances deben realizarse en el corto y mediano plazo, así como obtener el compromiso de la dirección y sumar a la agenda estratégica la seguridad y ciberseguridad.

Referencias Bibliográficas

Almanza J, A. R. (2021, 9 de julio). Vista de XXI Encuesta Nacional de Seguridad Informática. Revista Sistemas. https://sistemas.acis.org.co/index.php/sistemas/article/view/150/115

Almanza J, A. R. (2022, 1 de julio). Vista de XXII Encuesta Nacional de Seguridad Informática. Revista Sistemas. https://sistemas.acis.org.co/index.php/sistemas/article/view/186/146

Almanza J, A. R. (2023, 14 de diciembre). Vista de XXIII Encuesta Nacional de Seguridad Informática. Revista Sistemas. https://sistemas.acis.org.co/index.php/sistemas/article/view/Investigación%20169/199

Almanza J, A. R., & Cano M, J. J. (2020, 8 de octubre). Estudio de la Evolución de los Incidentes de Seguridad Informática en Colombia: 2010-2020. Association for Information Systems (AIS) eLibrary. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1010&context=isla2020

Amaya Jave, L. J. (2024, 30 de septiembre). Inteligencia artificial en la gestión predictiva de incidentes de TI. Revistas Universidad La Salle. https://revistas.ulasalle.edu.pe/innosoft/article/view/177/250

Ataque masivo de suplantación de diferentes juzgados de Colombia | Quiero ser UNAB. (2023, 18 de septiembre). Quiero ser UNAB. https://unab.edu.co/ataque-masivo-de-suplantacion-de-diferentes-juzgados-de-colombia

Bautista García, F., & Mesa Guzmán, L. (2022). Estudio trimestral de ciberseguridad Ataques a entidades de gobierno. CCIT. https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf

CAI Virtual. (s.f.). BALANCES ANUALES DEL CIBERCRIMEN | CAI Virtual. CAI Virtual. https://caivirtual.policia.gov.co/observatorio/analisis-cibercrimen

Castañeda Pérez, M. S. (2022, 17 de noviembre). Panorama de Ciberataques Más Recurrentes en Colombia 2021 y 2022. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12279/Artículo_IEEE_Coterminal.pdf?sequence=1&isAllowed=n#:~:text=Se%20puede%20concluir%20que%20los,le%20representan%20a%20los%20atacantes

CCIT. (2021, 2 de enero). Así están robando sus datos con información falsa del ministerio de salud sobre el coronavirus. CCIT - Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/en_los_medios/asi-estan-robando-sus-datos-con-informacion-falsa-del-ministerio-de-salud-sobre-el-coronavirus/

Cervera García, A., & Goussens, A. (2024, 13 de enero). Cybersecurity and use of ICT in the health sector. PubMed Central (PMC). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10823061/

Ciberseguridad en la cadena de suministro: objetivo de los 'malos'. (2023, 8 de junio). Red Seguridad. https://www.redseguridad.com/actualidad/ciberseguridad/la-cadena-de-suministro-se-ha-convertido-en-el-principal-objetivo-de-los-ciberdelincuentes_20230608.html

ColCERT. (2023, 23 de septiembre). [COLCERT - CSIRT Presidencia] Boletín No. 8 PMU Ciber - IoC MarioLocker. https://www.colcert.gov.co/800/articles-280648_Documento_1.pdf

ColCERT. (2023a, 14 de septiembre). [COLCERT - CSIRT Presidencia] Boletín No. 2 PMU Ciber - Ciberseguridad. https://www.colcert.gov.co/800/articles-278842_Documento_1.pdf

Congreso de Colombia. (2009, 30 de julio). Ley 1341 de 2009. Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=36913

CONPES 3854. (2016, 11 de abril). DNP. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Diaz Rico, S. (2024, 29 de febrero). Colombia, uno de los países latinos más atacados cibernéticos en el 2023, según IBM. Portafolio.co. https://www.portafolio.co/tecnologia/colombia-uno-de-los-paises-latinos-mas-atacados-ciberneticos-en-el-2023-segun-ibm-599526

García Rico, J. C. (2023, 16 de septiembre). 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

González, S. (2023, 23 de febrero). Operación Absoluta: espionaje dirigido a empresas y organismos gubernamentales de Colombia. Award-winning news, views, and insight from the ESET security community. https://www.welivesecurity.com/la-es/2023/02/23/campana-espionaje-empresas-organismos-gubernamentales-colombia-asyncrat

Gutiérrez Amaya, C. (2022, 16 de diciembre). Las 5 vulnerabilidades más utilizadas por cibercriminales durante 2022 en LATAM. Award-winning news, views, and insight from the ESET security community. https://www.welivesecurity.com/la-es/2022/12/16/vulnerabilidades-mas-utilizadas-cibercriminales-2022-latam

INCIBE. (2016, diciembre). Inventario de activos y gestión de la seguridad en SCI. https://www.incibe.es/incibe-cert/blog/inventario-activos-y-gestion-seguridad-sci

INCIBE. (2020). Glosario de términos de ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

INFOBAE. (2023, 18 de octubre). Colombia sigue en la mira: 85% de las empresas con trabajo remoto son vulnerables a ataques de ransomware. infobae. https://www.infobae.com/inhouse/2023/10/18/colombia-sigue-en-la-mira-85-de-las-empresas-con-trabajo-remoto-son-vulnerables-a-ataques-de-ransomware

Ingeniería social, la técnica de los delincuentes cibernéticos. (s.f.). Universidad de La Sabana - Colombia. https://www.unisabana.edu.co/portaldenoticias/al-dia/ingenieria-social-la-tecnica-de-los-delincuentes-ciberneticos

InvGate. (2021, 6 de mayo). Gestión de seguridad de la información en un mundo ITIL 4. The Service Desk and IT Service Management blog. https://blog.invgate.com/es/gestión-de-seguridad-de-la-información-en-un-mundo-itil-4#:~:text=La%20gestión%20de%20la%20seguridad,amenazas%20cibernéticas%20y%20el%20malware

Invima. (2023). Guía para la implantación eficaz del programa de tecnovigilancia. https://www.invima.gov.co/sites/default/files/dispositivos-medicos/Vigilancia/Programa-nacional-de-Tecnovigilancia/Documentos-de-interes/GUÍA%20TECNOVIGILANCIA%202023-final.pdf

ISO (International Organization for Standardization). (2013). Gestión de incidentes de seguridad de la información (GTC-ISO/IEC 27035). Icontec. https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/pdfview/viewer.aspx?locale=es-

ES&Q=E435101E23F7800FEC0DC8A9B48A5CC62B1DA961E0A07526&Req=

ISO (International Organization for Standardization). (2020). Gestión de riesgos para la seguridad de la información (ISO/IEC 27005:2022). Icontec. https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/pdfview/viewer.aspx?locale=es-ES&Q=AC41B04169B52B5C98A9B98EFCECD3F6C5EF74007EEF8D70&Req=

ISO (International Organization for Standardization). (2022). Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos (NTC-ISO-IEC 27001:2022). Icontec. https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=102657

ISO (International Organization for Standardization). (2022a). Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información (GTC-ISO/IEC 27002:2022). Icontec. https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/pdfview/viewer.aspx?locale=es-ES&Q=8D4BC7E979061815389FF17C1A00C4946836FE5FE42C11A9&Req=

Jaimovich, D. (2021, 28 de julio). Robo de credenciales: cómo suceden y qué medidas de seguridad hay que tomar. infobae. https://www.infobae.com/america/tecno/2021/07/28/robo-de-credenciales-como-suceden-y-que-medidas-de-seguridad-hay-que-tomar/#:~:text=En%20los%20ataques%20de%20credential,sitios%20web%20con%20dicha%20información

Jiménez, M. M. (2023, 5 de abril). Riesgos de seguridad de la información en el sector salud. Pirani: We make risk management simple. https://www.piranirisk.com/es/blog/gestion-riesgos-seguridad-informacion-sector-salud

Kaspersky. (2023). Informe de los análisis Incident Response. https://content.kaspersky-labs.com/se/media/latam/business-security/enterprise/kaspersky-ir-analyst-report-2023.pdf

Las 7 fases de un ciberataque. ¿Las conoces? (2020, 16 de enero). INCIBE. https://www.incibe.es/empresas/blog/las-7-fases-ciberataque-las-conoces

Ley 1273 de 2009. (2009, 5 de enero). SIC. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ley_1581_2012. (2012, 17 de octubre). SECRETARÍA GENERAL DEL SENADO. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Libedinsky, P., Alzuri, P., Cabral, F., Paz, S., & Nowersztern, A. (2021). BID - Protegiendo la salud digital una guía de ciberseguridad en el sector de salud. Academia.edu - Share research. https://www.academia.edu/61487406/Protegiendo_la_salud_digital_una_guia_de_ciberseguridad_en_el_sector_de_salud

Martínez, F. (2020). Plan de concienciación sobre la importancia de la seguridad de la información en las entidades de salud del sector público de Bogotá. Repositorio Institucional Universidad Católica de Colombia - RIUCaC ::Inicio. https://repository.ucatolica.edu.co/server/api/core/bitstreams/475e6c4b-21f4-4716-a3c8-ed3b9e9e3fd4/content

Mesa, L. (2022, 15 de junio). Herramientas útiles para combatir la cibercriminalidad. CCIT - Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/articulos-tictac/herramientas-utiles-para-combatir-la-cibercriminalidad

Microsoft. (s.f.). ¿Qué es la inteligencia artificial para la ciberseguridad? | Seguridad de Microsoft. https://www.microsoft.com/es-co/security/business/security-101/what-is-ai-for-cybersecurity

Ministerio de Salud y. Protección Social. (2021, 25 de junio). Resolución 866 de 2021. MINSALUD. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/resolucion-866-de-2021.pdf

MinTIC, C. (s.f.). Glosario. MINTIC Colombia. https://www.mintic.gov.co/portal/inicio/Glosario

MinTIC. (2016, 15 de marzo). Guía para la Gestión y Clasificación de Activos de Información. MinTIC. https://gobiernodigital.mintic.gov.co/692/articles-150528_G5_Gestion_Clasificacion.pdf

MinTIC. (2023, 20 de noviembre). MinTIC ratifica su compromiso de hacer de Colombia una potencia en Ciberseguridad.

MinTIC. (s.f.). Estrategia Nacional Digital de Colombia 2023-2026. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

Mozo Rivera, O., & Ardila Contreras, J. V. (2022, enero). Vista de El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia |

Perspectivas en Inteligencia. Revistas Ejército. https://revistascedoc.com/index.php/pei/article/view/333/543

National Institute of Standards and Technology (NIST). (2021, 23 de abril). Computer Security Incident Handling Guide. NIST Technical Series Publications. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology (NIST). (2021b, 23 de abril). NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. NIST. https://www.nist.gov/privacy-framework/nist-sp-800-115

National Institute of Standards and Technology (NIST). (s.f.). Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Versión 1.1). National Institute of Standards and Technology. https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf#:~:text=El%20Marco%20se%20enfoca%20en,de%20riesgos%20de%20la%20organización

Neira, J. (2023, 24 de agosto). Ciberataque: el phishing se ha incrementado en Colombia. Valora Analitik. https://www.valoraanalitik.com/2023/08/24/ciberataque-el-phishing-se-ha-incrementado-en-colombia

Nieto Rodríguez, C. O., & Sanches Rojas, A. L. (2023a, 12 de mayo). Riesgos cibernéticos en el sector financiero colombiano situación actual y tendencias. Repositorio Institucional Areandina. https://digitk.areandina.edu.co/bitstream/handle/areandina/5022/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Organización Panamericana de la Salud. (2023). 8 Principios rectores de la transformación digital del sector salud Caja de herramientas de transformación digital. IRIS PAHO Home. https://iris.paho.org/bitstream/handle/10665.2/57372/OPSEIHIS230016_spa.pdf?sequence=1&isAllowed=y

Overview of ransomware trends in 2023. (2023, 24 de mayo). Securelist | Kaspersky's threat research and reports. https://securelist.com/new-ransomware-trends-in-2023/109660

Parra, J., & Rodríguez, P. (2024, 16 de febrero). Las dos caras de la agencia nacional de seguridad digital. La Silla Vacía. https://www.lasillavacia.com/red-de-expertos/red-social/las-dos-caras-de-la-agencia-nacional-de-seguridad-digital/

Revista Hospitalaria. (2024, enero). Ciberseguridad en el sector hospitalario. Revista Hospitalaria. https://revistahospitalaria.org/wp-content/uploads/2024/01/REVISTA-HOSPITALARIA-144.pdf

Rosero, J. (2024, 15 de mayo). Recomendar las mejores prácticas en el sector salud basadas en frameworks de ciberseguridad aplicables a hospitales del sector público en colombia. Universidad Nacional Abierta y a Distancia UNAD. https://repository.unad.edu.co/bitstream/handle/10596/61501/JEROSEROC.pdf?sequence=1&isAllowed=y

Semana. (2023, 2 de enero). Sector de la salud, a ponerse pilas con la ciberseguridad. Semana.com. https://www.semana.com/economia/empresas/articulo/sector-de-la-salud-a-ponerse-pilas-con-la-ciberseguridad/202328/

Serna Navarro, T., & González Guerrero, A. (2022, 11 de mayo). El SOC "Autónomo": Inteligencia Artificial para la nueva ciberseguridad | RUIDERAe: Revista de Unidades de

Información. (ISSN 2254-7177). Revistas UCLM. https://revista.uclm.es/index.php/ruiderae/article/view/3088

Superintendencia de Industria y. Comercio. (2020). Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales. SIC. https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

TicTac. (2023, abril). Estudio anual de Ciberseguridad 2022-2023. CCIT - Cámara colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/#:~:text=Precisamente,%20el%20estudio%20revela%20que,con%20mayor%20número%20de%20registros

Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. (2020, 4 de agosto). INTERPOL | The International Criminal Police Organization. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Vidal Ledo, M. J., & Delgado Ramos, A. (2022, mayo). Salud y transformación digital. Scielo. http://scielo.sld.cu/scielo.php?pid=S0864-21412022000200009&script=sci_arttext&tlng=es

Glosario

A continuación, se relaciona las palabras clave conforme a las definiciones dadas por el MINTIC: (MINTIC COLOMBIA, s.f.)

Activo: En línea con la seguridad de la información, un activo es cualquier elemento o información que tenga valor para la organización.

Amenaza: Son eventos, personas o circunstancias con el potencial de generar daño como destrucción, robo, modificación, divulgación o indisponer un activo tecnológico.

Ataques Web: Este ataque se direcciona a la aplicación cliente y tiene origen desde la web, pueden darse desde sitios maliciosas creados con este fin, como desde sitios legítimos.

Ciberseguridad: Son los recursos destinados para la protección de los activos y usuarios en el ciberespacio.

Ingeniería Social: Método que busca engañar a los usuarios para que realicen actividades maliciosas y con consecuencias negativas.

Malware: Es un programa o software con objetivos maliciosos dentro de ellos están los troyanos, gusanos, virus y puertas traseras.

Phishing: Método usado para estafar y obtener información confidencial de las víctimas.

Riesgo: El efecto de incertidumbre sobre el cumplimiento de los objetivos.

Sistema de Detección de Intrusos: Este servicio analiza y monitorea los eventos que ocurran los sistemas en tiempo real, su objetivo es detectar intentos de intrusión y ataques.

Vulnerabilidad: La presencia de una vulnerabilidad genera un estado viciado de un sistema informático lo que puede afectar la integridad, confidencialidad y disponibilidad.

Resumen Analítico Especializado – RAE

Información general	
Tema	Revisión sistemática documental de la respuesta incidentes de seguridad de la información en el sector salud en Colombia.
Titulo	Panorama de la respuesta a incidentes de seguridad de la información en las organizaciones del sector salud en Colombia.
Autora	Ivonne Rocio Bernal Núñez
Directora	Yenny Stella Núñez Álvarez
Fuente Bibliográfica	Se utilizaron 62 fuentes bibliográficas, a continuación, se listan las principales: Almanza J, A. R. (2022, 1 de julio). Vista de XXII Encuesta Nacional de Seguridad Informática. Revista Sistemas. https://sistemas.acis.org.co/index.php/sistemas/article/view/186/146 Almanza J, A. R. (2023, 14 de diciembre). Vista de XXIII Encuesta Nacional de Seguridad Informática. Revista Sistemas. https://sistemas.acis.org.co/index.php/sistemas/article/view/Investigación%20169/199 Ministerio de Salud y. Protección Social. (2021, 25 de junio). Resolución 866 de 2021. MINSALUD. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/resolucion-866-de-2021.pdf MinTIC. (s.f.). Estrategia Nacional Digital de Colombia 2023-2026. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf Revista Hospitalaria. (2024, enero). Ciberseguridad en el sector hospitalario. Revista Hospitalaria. https://revistahospitalaria.org/wp-content/uploads/2024/01/REVISTA-HOSPITALARIA-144.pdf
Año	2024
Resumen	Dentro de este trabajo de grado se buscará abordar la gestión que las organizaciones del sector salud en Colombia dan a los incidentes de seguridad de la información y la respuesta ante su materialización, siendo esta un proceso crítico para estas, esto teniendo presente que de acuerdo con las cifras presentadas por el Centro Cibernético de la Policía Nacional se presentaron 54.121 denuncias relacionadas con ataques cibernéticos y Colombia se posiciona en el tercer lugar de los países más atacados en América Latina, los ataques han sido dirigidos a organizaciones de todo tipo, sin embargo, las que han tenido un mayor impacto son las entidades gubernamentales y las del sector de la salud, en los que estos ataques pusieron en riesgo la vida o el libre desarrollo de millones de ciudadanos. Este trabajo abordara las siguientes temáticas, todas ellas dentro del contexto de las organizaciones del sector salud en Colombia: Los principales vectores de ataque más explotados en las organizaciones, donde se identificarán las principales tendencias y su materialización en Colombia, para el entendimiento de estos en el contexto del país, identificar el estado actual la gestión de la seguridad de la información, así como identificar los factores que influyen en la respuesta a incidentes de seguridad de la información.
Palabras claves	Incidentes de seguridad de la información, vectores de ataque, seguridad de la información.
Contenidos	Introducción Planteamiento del Problema Justificación

	Objetivos Objetivo General Objetivos Específicos Marco Referencial Antecedentes o Estado Actual Marco Conceptual La Triada de la Seguridad Gestión de Incidentes de Seguridad de la Información Marco Teórico Marco Legal Marco Contextual Panorama Actual de la Seguridad de la Información en las Organizaciones del Sector Salud en Colombia Vectores de ataque más explotados por los ciberdelincuentes en las organizaciones de Colombia y el sector salud Vectores de ataque Amenazas persistentes avanzadas (APT) Ransomware Sistemas sin parches Phishing Spoofing Credential stuffing Ataques a la cadena de suministros Recopilación de información Dominios malignos Factores internos y externos que influyen en la capacidad de respuesta incidentes de seguridad de la información Factores internos Factores externos Mecanismos que contribuyan en el aseguramiento y la capacidad de gestión de incidentes en las organizaciones del sector salud. Plan estratégico de seguridad de la información Plan de concientización de seguridad de la información Gestión de activos de información Gestión de riesgos de seguridad de la información Integración de la inteligencia artificial y aprendizaje automático para la respuesta a incidentes de seguridad de la información Buenas prácticas para la gestión de incidentes ISO 27001:2022. NIST V 1.1 ITIL V4 Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales de la SIC Conclusiones Referencias Glosario
Descripción del problema de investigación	
La pandemia adelanto la llegada de la cuarta revolución industrial y con ella llego la hiper conectividad, no solo las organizaciones son objeto de ataques cibernéticos, también los ciudadanos y estos se han visto en aumento durante los últimos tres años, actualmente Colombia es el tercer país más atacado de Latinoamérica, por lo que es indispensable lograr identificar la	

gestión y respuesta a los incidentes de seguridad, así como la efectividad al momento de la materialización de estos.

De acuerdo con el CCIT y su programa de Seguridad Aplicada al Fortalecimiento Empresarial, una organización colombiana puede llegar a perder de $400 a $1.200 millones de pesos a raíz de un ciberataque. (Mesa, 2022)

De igual forma en su informe anual de ciberseguridad, en retrospectiva con las denuncias generadas en 2023 cuando iniciaron los ataques con Ransomware se conocieron 3.380 reportes, ahora con una década en transcurso se cuentan con 65.794 reportes, durante el 2022 se presentó un repunte en el incremento de casos, el mayor se presentó en el 2020. (TicTac, 2023)

Pregunta, ¿Cómo se da respuesta a los incidentes de seguridad de la información en Colombia?

Objetivos

General: Analizar el estado actual de las organizaciones del sector salud en Colombia en cuanto a su capacidad de respuesta frente a incidentes de seguridad de la información, a través de una revisión sistemática de literatura e informes especializados para la identificación de brechas existentes y como base para el desarrollo de mecanismos y buenas prácticas de aseguramiento adaptados a las necesidades específicas de dicho sector.

Específicos:

- Realizar una revisión exhaustiva de la literatura y de informes especializados para obtener un panorama actual de la seguridad de la información en las organizaciones del sector salud en Colombia.
- Examinar los vectores de ataque de los que ha sido víctima las infraestructuras TI de las organizaciones del sector salud.
- Analizar los factores internos y externos que influyen en la capacidad de respuesta ante incidentes de seguridad de la información en las organizaciones del sector salud en Colombia, dentro de un contexto operativo y regulatorio.
- Proponer mecanismos que contribuyan en el aseguramiento y la capacidad de gestión de incidentes en las organizaciones del sector salud.

Metodología

Para el desarrollo de la presente monografía se realiza la revisión sistemática documental para la identificación del panorama actual de la seguridad de la información en el sector salud, así como los vectores de ataque, factores internos y externos que impacten la capacidad para la respuesta a los eventos e incidentes e identificar mecanismos que permitan a las organizaciones del sector salud fortalecer su postura de seguridad y garantizar una eficiente respuesta a los incidentes de seguridad.

Referentes teóricos

De acuerdo con la información presentada en la XXI Encuesta Nacional de Seguridad Informática el 72% de las personas encuestadas tuvieron un incidente de SI en sus organizaciones, teniendo un aumento del 4% respecto al año anterior, adicionalmente se evidencia que los principales tipos de incidentes presentados fueron errores humanos, phishing, accesos no autorizados en la web, ingeniería social y por último la instalación de software no autorizado y solo el 28% de las empresas realiza el reporte de estos a las diferentes autoridades nacionales (Almanza J, 2021), dentro de la XXII Encuesta Nacional de Seguridad Informática se evidencia que el 3,67% de los encuestados no tienen conocimiento de la cantidad de incidentes de SI que se presentaron en sus organizaciones y el número de personas que estuvieron en contacto con un incidentes de SI disminuyo al 56% y una cifra bastante interesante es que el 17% de los encuestados han tenido más de 7 incidentes de SI, frente a los tipos de incidentes de SI se evidencia los siguientes cambios, frente a phishing aumento del 6%, la ingeniera social paso al tercer lugar con un aumento del 5% y entra dentro de los principales 5 tipos de incidentes el fraude electrónico (Almanza J, 2022).

Referentes conceptuales

Se realizo el estudio de: La triada de la seguridad y Gestión de incidentes de seguridad de la información NIST SP 800-61, guía para el manejo de incidentes, GTC-ISO/IEC 27035, Gestión de incidentes de seguridad de la información, NTC-ISO/IEC 27005, Gestión de riesgos para la seguridad de la información y NIST SP 800-115, Guía técnica para pruebas y evaluaciones de seguridad de la información.

Resultados

Conforme con la identificación del estado actual de la seguridad de la información en organizaciones del sector salud se identifica que las entidades no cuentan con mecanismos de acceso basado en roles y perfiles, falencias en la actualización frente a nuevas amenazas y tendencias, ausencia de planes de capacitación para los colaboradores, personal especializado en seguridad de la información y ciberseguridad limitado, falta de mecanismos para la detección y respuesta a incidentes de seguridad y ciberseguridad y uno de los principales retos es de obtener el apoyo de la alta dirección para lograr el mantenimiento y gestión de la seguridad de la información.

Si bien, las amenazas presentadas mayoritariamente fueron orientadas hacia los usuarios finales como son el caso de ataques de ransomware, phishing, spoofing y recopilación de información, también se identificaron ataques sobre los cuales no se contaba con mecanismos de seguridad suficientes para prevenirlos e identificarlos como los son ataques a sistemas sin parches, ataques APT y a la cadena de suministros.

Se realiza la verificación los factores internos y externos, identificando que, a nivel interno los factores identificados corresponden a la cultura de seguridad de la información, gestión de los riesgos y plan de respuesta a incidentes. A nivel externo se logra evidenciar el entorno regulatorio, el crecimiento de las amenazas cibernéticas y aseguramiento de la cadena de suministros.

Para el fortalecimiento de la postura de seguridad de las organizaciones del sector salud se propone adoptar los siguientes mecanismos y estrategias: Plan estratégico de seguridad de la información, plan de concientización de seguridad de la información, gestión de activos, gestión de riesgos de seguridad de la información, integración de la inteligencia artificial y aprendizaje automático y un plan de respuestas a incidentes de seguridad de la información y ciberseguridad.

Conclusiones

Desde el inicio de la pandemia los ciberataques han ido en aumento, como hemos logrado evidenciar dentro de los vectores de ataque más representativos en Colombia y el sector salud se encuentran los ataques por medio de ramsomware, generando importantes retos en materia de capacitación y adopción de la ciberseguridad por parte de los colaboradores, ya que estos ataques siguen teniendo un alto impacto y de fácil ejecución, adicionalmente, se logró evidenciar que las vulnerabilidades más explotadas en el país en promedio tienen 7 años desde su descubrimiento, lo que muestra la gran brecha que tienen las organizaciones para llevar a cabo una correcta gestión de la capacidad o renovación tecnológica y una gestión de parchado, adicional a esto el sector salud presenta brechas frente a la articulación de los controles técnicos con controles normativos y estos a su vez orientados con la estrategia de la organización.

Es de vital importancia que las organizaciones del sector salud logren adoptar marcos de seguridad que les permitan fortalecer su postura de seguridad. Las organizaciones en Colombia han incrementado la adopción de estas buenas prácticas durante la última década, sin embargo, las brechas a tratar aún son extensas en materia de ciberseguridad, como una adopción del proceso de gestión de activos, gestión de riesgos y gestión de incidentes de seguridad de la información, siendo el sector salud uno de los más atacados los avances deben realizarse en el corto y mediano plazo, así como obtener el compromiso de la dirección y sumar a la agenda estratégica la seguridad y ciberseguridad.