UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNÉTICA PARA HOSPITAL PÚBLICO

AUTORES:

JOSÉ LUIS BUENAÑO QUINTANA
CHRISTIAN ADRIAN CUSME MEDINA

DIRECTOR:

MIGUEL ÁNGEL QUIROZ MARTÍNEZ

CUENCA – ECUADOR
2024

Autores:

Christian Adrian Cusme Medina
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
ccusme@est.ups.edu.ec

José Luis Buenaño Quintana
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
jbuenanoq@est.ups.edu.ec

Dirigido por:

Miguel Ángel Quiroz Martínez
Ingeniero en Sistemas.
Máster en Ingeniería.
mquiroz@est.ups.edu.ec

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS
2024 © Universidad Politécnica Salesiana.
CUENCA – ECUADOR – SUDAMÉRICA
JOSÉ LUIS BUENAÑO QUINTANA
CHRISTIAN ADRIAN CUSME MEDINA
Plan de respuesta a incidentes de seguridad cibernética para hospital público

DEDICATORIA

Dedico este trabajo a mi esposa, quien fue un gran apoyo para mí durante mis estudios, también a mis padres, hermano y otros familiares que tuvieron fe en mí para tener éxito en esta fase de mi educación. No puedo dejar de lado de mis compañeros y en especial a uno de ellos que fue el pilar fundamental para tomar esta maestría y dar un paso más a nivel profesional.

Christian Adrian Cusme Medina.

DEDICATORIA

A mi familia, por su amor incondicional y apoyo constante. A mis amigos, por su aliento en los momentos difíciles, aliento y apoyo en cada paso de este camino.

José Luis Buenaño Quintana.

AGRADECIMIENTO

Agradezco en primer lugar a Dios por brindarme la salud y fuerza para haber culminada esta nueva etapa de aprendizaje. A mi esposa, padres y hermano, quienes fueron personas que siempre me brindaron su apoyo durante este proceso.

Un agradecimiento especial para mi compañero de tesis, quien a su vez es mi jefe y una gran persona que con su confianza este camino de aprendizaje se hizo más llevadero y compartiendo conocimientos para seguir creciendo como profesionales.

Christian Adrian Cusme Medina.

AGRADECIMIENTO

El presente trabajo de investigación es el fruto de un gran esfuerzo y me complace expresar mi más profunda gratitud a quienes han hecho posible su culminación. Agradezco a mi familia, por su amor incondicional, a nuestro tutor de tesis por su invaluable guía, mentoría y apoyo durante todo el proceso. Por supuesto, deseo también expresar mi profunda gratitud a mi compañero de tesis, cuya colaboración, compromiso y trabajo en equipo han sido fundamentales para alcanzar este logro y sin duda enriquecido este viaje académico de forma significativa.

José Luis Buenaño Quintana.

Tabla de Contenido

Resumen 9
Abstract 10
1. Introducción 11
2. Determinación del Problema 15
2.1 Descripción del problema 15
2.2 Descripción del problema 15
2.3 Delimitación del problema 16
2.4 Justificación del problema 17
2.5 Objetivos 18
2.5.1 Objetivo General 18
2.5.1 Objetivos Específicos 18
3. Marco teórico referencial 20
3.1 ¿Qué es un Incidente? 20
3.2 ¿Qué es un Incidente de ciberseguridad? 20
3.3 Tipos de incidentes de ciberseguridad 21
3.3.1 Incidentes de día cero 21
3.3.2 Ataque de DDoS 21
3.3.2 Malware 22
3.3.3 Ransomware 22
3.3.4 Phishing 22
3.4 ¿Qué es NIST? 22
3.5 ¿Qué es NIST 800-61? 23
4. Metodología 24
5. Resultados y discusión 26
5.1 Preparación 26
5.2 Detección y análisis 34
5.3 Contención, erradicación y recuperación 43
5.4 Actividad Post-Incidente 46
5.5 Evaluación 49
6. Conclusiones 54
Referencias 56

Plan de respuesta de incidentes de seguridad cibernética para hospital público.

Autor(es):

Christian Adrian Cusme Medina

José Luis Buenaño Quintana

Resumen

La seguridad cibernética en hospitales públicos es crítica debido a la dependencia de la tecnología en la atención médica actual. Este estudio se centra en desarrollar un plan de respuesta a incidentes de seguridad cibernética adaptado a hospitales públicos.

Los hospitales son objetivos vulnerables para ataques cibernéticos debido a la abundancia de datos personales sensibles y la complejidad de los sistemas. Este plan proactivo involucra a personal de TI, administradores hospitalarios y profesionales de la salud.

El proceso comienza con la identificación de activos críticos y la evaluación de riesgos, incluyendo amenazas como ransomware. Se establecen procedimientos para la detección temprana y capacitación del personal en la identificación de señales de alarma.

En caso de un incidente, el plan detalla pasos como la notificación a autoridades y coordinación con expertos en seguridad cibernética. La comunicación interna y externa es esencial para mantener la continuidad de la atención y cumplir con obligaciones legales del Ecuador, todo esto acogiéndose a recomendaciones de normas y estándares internacionales.

La recuperación de datos y sistemas, junto con la evaluación post-incidente, son prioridades. El plan debe adaptarse a las nuevas amenazas y tecnologías en curso, brindando a través del plan de respuesta a incidentes un marco completo para abordar los riesgos que se pueden suscitar, protegiendo los datos y garantizando la continuidad del servicio de salud.

Palabras clave:

Seguridad cibernética, ransomware, plan de respuesta a incidentes.

ABSTRACT

Cybersecurity in public hospitals is critical due to the reliance on technology in modern healthcare. This study focuses on developing a cybersecurity incident response plan tailored to public hospitals.

Public hospitals are vulnerable targets for cyberattacks due to the abundance of sensitive personal data and the complexity of their systems. This proactive plan involves IT personnel, hospital administrators, and healthcare professionals.

The process begins with the identification of critical assets and risk assessment, including threats such as ransomware. Procedures are established for early detection and staff training on identifying warning signs.

In the event of an incident, the plan details steps such as notifying authorities and coordinating with cybersecurity experts. Internal and external communication is essential to maintain continuity of care and comply with Ecuador's legal obligations, all while adhering to recommendations from international standards and regulations.

Data and system recovery, along with post-incident evaluation, are priorities. The plan must adapt to new threats and new technologies, providing a comprehensive framework through the incident response plan to address the risks that may evidence, protecting data, and ensuring the continuity of the health service.

Palabras clave:

Cybersecurity, cyberattacks, data and system recovery.

1. Introducción

La creciente dependencia de las organizaciones a nivel mundial en el entorno digital ha generado un mayor nivel de exposición frente a agentes de amenazas y ataques cibernéticos. Estas pueden ocasionar pérdida de datos, divulgación no autorizada de datos personales, interrupción de servicios críticos y daños a la reputación de las organizaciones. Para reducir el posible impacto al momento de experimentar un incidente de seguridad, es necesario adoptar un enfoque proactivo, y sistemático a través de la implementación de un Plan de Respuesta a Incidentes de Seguridad Cibernética.

Un ciberataque es un acto malicioso llevado a cabo por individuos o grupos con el objetivo de comprometer, dañar o robar información de sistemas informáticos o redes de computadoras de cualquier tipo de organización, es decir, puede entenderse como cualquier evento o acción no autorizada, inesperada o indeseable que afecta la confidencialidad, integridad o disponibilidad de la información o de los sistemas de una organización.

Los objetivos y niveles de sofisticación pueden ser muy diversos, además de ser llevados a cabo por una variedad de actores, como: crackers, ciberdelincuentes o a través de hacktivistas, quienes buscan utilizar la tecnología y las técnicas de hacking para promover y defender causas, expresar su descontento con determinadas políticas, denunciar injusticias o difundir información que consideran relevante para el público.

Existe gran variedad de ciberataques, cada uno diseñado para lograr diferentes objetivos. A continuación, se presentan algunos de los tipos más comunes de ciberataques:

- **Malware:** Engloba una amplia variedad de software desarrollado con fines maliciosos, dentro de esta categoría se incluye:

- **Phishing:** Los atacantes envían correos electrónicos, mensajes o sitios web falsificados para revelar datos privados obteniendo información confidencial, como datos financieros, contraseñas, entre otros. (Mian, 2023)
- **Denegación de servicio (DoS) y Denegación de Servicio Distribuida (DDoS):** Los ataques DoS intentan abrumar un servidor o sistema con tráfico, mientras que los ataques DDoS utilizan múltiples dispositivos distribuidos para el mismo propósito, dejando los servicios inaccesibles para las personas autorizadas para usarlos.
- **Inyección de código**: Los atacantes introducen código malicioso en aplicaciones web, como SQL Injection, para obtener un acceso no autorizado o manipular los datos almacenados.
- **Ataques de día cero:** Explotan vulnerabilidades de seguridad que no han sido identificadas y por ende no cuentan con una solución. Son denominadas así porque el desarrollados, una vez descubierta la amenaza, dispone de cero días para encontrar una solución. (Cloudflare, s.f.)
- **Ataques a la infraestructura física conectada:** Atacan dispositivos y sistemas IoT (Internet de las cosas) o sistemas de control industrial (SCADA) para interrumpir operaciones críticas.
- **Ataques de ingeniería social:** Los atacantes utilizan el engaño para manipular a las personas y obtener acceso a información confidencial y tener un acceso no autorizado.
- **Ataques de fuerza bruta:** Intentan adivinar contraseñas probando todas las combinaciones posibles hasta encontrar la correcta.
- **Ataques de suplantación de identidad (spoofing):** Los atacantes falsifican direcciones IP, correos electrónicos o identidades para parecer legítimos y ganar acceso no autorizado.
- **Ataques de intercepción de datos:** Los atacantes capturan y descifran datos sensibles que se transmiten entre dispositivos o sistemas.

Lo cierto es que, así como la tecnología ha experimentado un crecimiento exponencial, también las capacidades, y herramientas disponibles por parte de los ciberdelincuentes han ido en crecimiento.

Así lo reflejan las estadísticas publicadas por el fabricante de soluciones de seguridad ESET, en su portal "welivesecurit.com" en este reporte anual publicado en el año 2023 se destacan algunas cifras de gran importancia: (Harán, 2022)

- Se encuestaron a más de 1,800 profesionales de seguridad, en 17 países
- 48% de las empresas en Latinoamérica, experimentó un incidente de seguridad
- el 24% de estos incidentes estuvo relacionado con infección por malware
- 13% de la organización encuestada, manifestó haber experimentado accesos no autorizados, y
- el 5% fue víctima de filtración de datos sensibles.

De acuerdo con los datos del NCSI (National Cyber Security Index) el índice de seguridad cibernética de Ecuador es de 53.25 puntos sobre 100, ocupando la posición 64 de 160 a nivel mundial y en el mismo informe acorde al índice de Ciberseguridad Global, se ocupa la posición 119. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, s.f.)

Las amenazas en Ecuador han abarcado ciberataques a infraestructuras críticas digitales, sistemas tecnológicos obsoletos, altos costos para la adquisición de tecnología y marcos legales y regulatorios desactualizados, lo que ha aumentado la vulnerabilidad a los ataques cibernéticos. Además, es crucial abordar desafíos como la falta de un presupuesto continuo, la escasez de personal especializado en ciberseguridad en las organizaciones y la necesidad de crear una educación en ciberseguridad para que individuos y que las empresas sepan cómo protegerse ante las amenazas, incluyendo un equipo especializado. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, s.f.)

Cabe indicar que este trabajo de titulación se enmarca sobre la línea de investigación de Seguridad y criptografía, la cual pertenece al Grupo De Investigación En Inteligencia Artificial Y Reconocimiento Facial (GIIAR) de la UPS.

2. Determinación del Problema

2.1 Descripción del problema

Organizaciones con misión tan crítica como el cuidado de la salud, dependen cada vez en mayor medida de herramientas y recursos tecnológicos, con la misma o incluso mayor agilidad se incrementan las capacidades de los ciber delincuentes para comprometer o vulnerar información confidencial o sensible, por tanto, todas las organizaciones han experimentado o experimentarán un incidente de seguridad que comprometa la confidencialidad, disponibilidad o integridad de su información.

Las organizaciones que no cuentan con un plan previamente diseñado para la gestión de incidentes de seguridad antes de que estos se materialicen se exponen a:

1. Tiempo más extenso en la detección y respuesta frente a un incidente de seguridad.
2. Incrementar el riesgo de exposición de información confidencial durante un ciberataque.
3. Mayor nivel de afectación reputacional.
4. Mayores pérdidas financieras luego de un incidente
5. Posibles implicaciones legales, demandas, o litigios.
6. Interrupción de sus operaciones que forman parte de su cadena de valor.
7. Acciones improvisadas y decisiones apresuradas que genere un serio impacto en la organización.

2.2 Descripción del problema

Frente a la problemática descrita en la sección anterior se enmarcan tres preguntas:

1. ¿Cómo se pueden establecer lineamientos efectivos para organizar y desarrollar la capacidad de respuesta a incidentes de ciberseguridad en un

entorno hospitalario, considerando estándares reconocidos y principios de manejo de incidentes de ciberseguridad?

2. ¿De qué manera se puede diseñar una propuesta de plan de respuesta a incidentes de ciberseguridad adaptado a las necesidades y particularidades de un hospital, tomando como base los principios descritos en el NIST 800-61r2, Computer Security Incident Handling Guide, con el fin de mejorar la capacidad de respuesta a incidentes y reducir el riesgo de pérdida de continuidad prolongada en la atención a pacientes y beneficiarios?
3. ¿Qué metodología se puede emplear para evaluar la propuesta de plan de respuesta a incidentes de ciberseguridad, considerando la verificación por parte de un especialista imparcial, con el objetivo de validar su alineamiento con las mejores prácticas en respuesta a incidentes y asegurar su viabilidad de implementación para lograr los objetivos planteados en el contexto hospitalario?

2.3 Delimitación del problema

El presente trabajo de investigación se delimita en su alcance a fin de enfocar la investigación de manera efectiva, proporcionar una estructura clara para el desarrollo del trabajo y asegurar que los objetivos sean alcanzables en virtud del tiempo y recursos disponibles:

- **Ámbito Geográfico:** Se centrará en una entidad del sector salud ubicada en la ciudad de Guayaquil – Ecuador.
- **Tipo de Organización:** EL trabajo se centrará en un hospital de especialidades sin fines de lucro que debido a su alto volumen de pacientes y beneficiarios atendido tiene una elevada dependencia de su plataforma tecnológica.
- **Tipos de Incidentes de Ciberseguridad:** EL plan de respuesta a incidentes de seguridad será aplicable ante la materialización de los principales y más frecuentes incidentes de seguridad indistintamente de su tipo.

- **Marco Normativo y Legal:** El desarrollo del presente trabajo se alineará a lo indicado en el documento “NIST 800-61: Guía para la gestión de incidentes de ciberseguridad”. Los principios determinados en dicho documento son consistentes con lo indicado en la serie de normas ISO 27000, y contribuirá con el cumplimiento de la Ley Orgánica de Protección de Datos Personales actualmente en vigencia en Ecuador.
- **Herramientas y Tecnologías:** Durante el proceso de diseño del plan de respuesta a incidentes se hará referencia a diferentes herramientas aplicables durante el manejo del incidente sin embargo no se considera la implementación de ninguna de estas herramientas.

2.4 Justificación del problema

La estrategia nacional de ciberseguridad del Ecuador es una oportunidad para integrar y fomentar esta cultura de Valor al Riesgo cibernético (CyVaR). El asunto es simple, para mejorar la resiliencia cibernética en organizaciones de Ecuador ya sean del sector público o privado, es crucial fomentar una gestión de riesgos cuantitativa que estime el posible costo financiero de un ataque cibernético, tanto en los activos afectados como en los derechos y libertades de los ciudadanos. Ecuador ha dado pasos iniciales destacables para mejorar sus capacidades y habilidades de gestión de incidentes cibernéticos. Una muestra de ello ha sido la creación del Equipo del Centro de Respuesta a Incidentes de Seguridad Nacional (EcuCERT), que opera bajo supervisión de la Agencia para la Regulación y Control de las Telecomunicaciones (ARCOTEL), y se rige en cumplimiento con la Ley Orgánica de Telecomunicaciones. (Ecucert, s.f.)

El desarrollo de un plan de incidentes de seguridad cibernética es esencial en el entorno actual para proteger activos, información y mantener la confianza de los usuarios en las diversas organizaciones del Ecuador. Además, se puede contribuir al avance del conocimiento en ciberseguridad y mejorar la preparación general de las organizaciones frente a las amenazas cibernéticas en evolución. (Ecucert, s.f.)

Con esta propuesta se busca contribuir a la mejora de los centros de respuesta de incidentes de seguridad cibernética en los siguientes aspectos:

- Manejo de crisis durante un incidente de seguridad cibernética.
- Correcta detección y análisis de un incidente.
- Metodología de trabajo de un equipo de respuesta a incidentes.
- Conocer herramientas para el análisis, mitigación y recuperación ante incidentes de seguridad cibernética.
- Establecer actividades de coordinación para la comunicación de un incidente, de manera interna y externa a diversos CSIRT en caso de ser necesario y bajo qué aspectos este puede ayudar a otros grupos a identificar y prevenir incidentes.

El plan contribuirá con la protección de activos e información sensible, de acuerdo con lo establecido en la ley orgánica de protección de datos personales, y de esta manera evitar pérdidas financieras y daño a la reputación, minimizando así el impacto en la productividad y garantizar una guía adecuada para poder recuperarse de manera rápida y eficiente de un incidente.

2.5 Objetivos

2.5.1 Objetivo General

Diseñar un modelo de Plan de Respuesta a Incidentes de Ciberseguridad, que permita responder de forma apropiada ante la materialización de un incidente, y minimizando su impacto negativo, a través del alineamiento con la publicación especial de NIST 800-61 revisión 2, Computer Security Incident Handling Guide.

2.5.1 Objetivos Específicos

1. Establecer los lineamientos para la organización y desarrollo de la capacidad de respuesta a incidentes de ciberseguridad a través de la aplicación del proceso estándar y principios para el manejo de incidentes de ciberseguridad.

2. Desarrollar la propuesta de plan de respuesta a incidentes de ciberseguridad, para aplicarse en un hospital, aplicando y adaptando los principios descritos en el documento NIST 800-61 revisión 2, Computer Security Incident Handling Guide, a fin de mejorar la capacidad de respuesta a incidentes y reducir el riesgo de pérdida de continuidad prolongada en la atención a pacientes y beneficiarios.
3. Evaluar la propuesta de plan de respuesta a incidentes de ciberseguridad, realizando una verificación por parte de un especialista imparcial que valide el alineamiento del plan con las mejores prácticas en respuesta a incidentes, con el fin de asegurar que el plan desarrollado sea viable de implementar y logre alcanzar los objetivos.

3. Marco teórico referencial

3.1 ¿Qué es un Incidente?

Para conocer mucho más acerca de un incidente, se procederá a detallar las definiciones acordes a normas o buenas prácticas.

ITIL.- Un incidente se define como una interrupción no anticipada o planificada de un servicio, o una disminución en la calidad de este. Tiene como propósito minimizar el impacto negativo de los incidentes mediante la restauración del funcionamiento normal del servicio lo más rápido posible. (Chirinos Meza, 2022)

COBIT.- Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restablecer el servicio habitual, registrar y atender las solicitudes de los usuarios; así como registrar, investigar, diagnosticar, escalar y solucionar los incidentes.

NIST.- Define al incidente como un evento de cualquier ocurrencia observable en un sistema o red. (Marron & Mahn, 2021)

ISO 27001.- Esta al ser una norma orienta fundamentalmente a seguridad de la información nos indica que la gestión de incidentes de seguridad de la información y mejoras es, asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

3.2 ¿Qué es un Incidente de ciberseguridad?

Un incidente de ciberseguridad es un evento que representa una amenaza para un sistema, aunque no haya habido una confirmación de compromiso. En otras palabras, se refiere a una vulnerabilidad de seguridad que aún no ha sido explotada, pero que está presente en el sistema o en la aplicación web que se quiere proteger. Estos incidentes son bastante comunes y pueden encontrarse en abundancia en las

redes corporativas y en los programas informáticos. Por esta razón, el equipo de seguridad (Blue Team) debe ser capaz de identificarlos y corregirlos de forma regular para poder descubrirlos antes que los atacantes lo hagan. (Marron & Mahn, 2021)

3.3 Tipos de incidentes de ciberseguridad

3.3.1 Incidentes de día cero

Con frecuencia, los programas informáticos presentan fallos no intencionales conocidos como vulnerabilidades. Estos son errores o debilidades en el software que, teóricamente, podrían ser aprovechados. Un ejemplo sería un defecto que permita a un ciberdelincuente acceder a datos que, de otro modo, estarían seguros.

Los desarrolladores de software suelen estar alerta ante estas vulnerabilidades. Cuando identifican una, la analizan, crean un "parche" para solucionarla y luego integran ese parche en una nueva versión del programa.

No obstante, este proceso lleva tiempo. Desde que se descubre la falla, los hackers de todo el mundo podrían comenzar a explotarla antes de que los desarrolladores encuentren una solución. Este período en el que existe una vulnerabilidad, pero aún no se ha desarrollado una solución se conoce como "vulnerabilidad zero day o de día cero".

3.3.2 Ataque de DDoS

Un ataque de Denegación de Servicio Distribuido (DDoS) es un esfuerzo por parte de un atacante para generar una gran cantidad de tráfico o congestión en una aplicación específica en Internet. Este intento tiene como objetivo bloquear o dificultar el flujo de tráfico de los usuarios regulares que intentan acceder a esa aplicación o sitio web.

3.3.2 Malware

El malware es un tipo de software que opera en un sistema informático sin el permiso ni el conocimiento del propietario o usuario del dispositivo infectado. Este software malicioso realiza acciones perjudiciales tanto para el usuario como para el sistema en el que se encuentra.

3.3.3 Ransomware

El ransomware es una categoría de malware que asume el control total del sistema bloqueando o encriptando los datos del usuario. Luego, solicita un rescate a cambio de liberar o desencriptar los archivos del dispositivo.

3.3.4 Phishing

El phishing es una estrategia en la que un ciberdelincuente envía un correo electrónico al usuario, fingiendo ser una entidad confiable como una red social, banco o institución pública. El objetivo es engañar al usuario para que revele información confidencial, realice pagos no autorizados o infecte su dispositivo. Para lograrlo, los atacantes adjuntan archivos maliciosos o enlaces a sitios web fraudulentos en el correo electrónico.

3.4 ¿Qué es NIST?

El Instituto Nacional de Estándares y Tecnología, es un pilar de la innovación estadounidense que fue fundado en 1901 y bajo el amparo del Departamento de Comercio de EE. UU. (NIST, s.f.)

El Instituto Nacional de Estándares y Tecnología (NIST) se ha convertido en uno de los laboratorios científicos más antiguos del país. Su creación respondió a una necesidad urgente: fortalecer la competitividad industrial estadounidense frente a potencias como el Reino Unido y Alemania, cuyas infraestructuras de medición superaban a la nación. (Marron & Mahn, 2021)

La influencia del NIST se extiende a todos los ámbitos, desde las tecnologías más diminutas hasta las mega construcciones más complejas. Sus mediciones precisas dan soporte a dispositivos nano escalares tan pequeños que miles caben en la punta de un cabello, así como a rascacielos resistentes a terremotos y redes de comunicación globales.

3.5 ¿Qué es NIST 800-61?

La Publicación Especial 800-61 (SP 800-61) del Instituto Nacional de Estándares y Tecnología (NIST), titulada "Guía para el manejo de incidentes de seguridad informática", es un referente ampliamente reconocido que ofrece recomendaciones prácticas a las organizaciones para establecer y gestionar un programa de respuesta a incidentes de ciberseguridad. (NIST SP 800-61, 2021)

4. METODOLOGÍA

Para la definición de la metodología de la presente tesis nos guiaremos en la norma NIST 800-61 también conocida como "Computer Security Incident Handling Guide" (Guía para el Manejo de Incidentes de Seguridad Informática), es un recurso importante en el campo de la seguridad cibernética. Esta guía proporciona lineamientos detallados y mejores prácticas para manejar incidentes de seguridad informática de manera efectiva y en este caso la orientaremos a plan de respuesta a incidentes de un hospital pública considerando todos los activos de información que se deben proteger. (NIST SP 800-61, 2021)

En base a la norma, detallamos las fases que se llevarán a cabo.

Fase 1 - Análisis Detallado. - Realizar un estudio exhaustivo de la norma NIST 800-61, identificando los principios, procesos y mejores prácticas en el manejo de incidentes de seguridad cibernética.

Fase 2 - Identificación de Requisitos Específicos del Hospital. - Revisar políticas, procedimientos y registros de incidentes de seguridad cibernética del hospital para comprender su postura actual en materia de ciberseguridad y áreas de mejora en las que se puede mejorar o desarrollar un plan mucho más agresivo para evitar incidentes.

Fase 3 - Diseño de plan de respuesta de incidente. - Crear matrices detalladas y procedimientos que describan los pasos específicos si se suscitan incidentes de seguridad cibernética en cualquiera de sus diversos tipos, alineado a la norma NIST.

Fase 4 – Desarrollo de procedimientos y protocolos. –

- Establecer roles y responsabilidades claras para el personal involucrado en la respuesta a incidentes de seguridad cibernética, incluyendo roles técnicos y de gestión.

- Desarrollar procedimientos detallados para la detección, evaluación y notificación de incidentes de seguridad, incluyendo criterios de priorización y canales de comunicación definidos que se encuentren socializados en cada nivel de participación dentro del procedimiento.
- Establecer protocolos detallados del paso a paso para contener y erradicar incidentes de seguridad de manera eficiente, minimizando el impacto en las operaciones del hospital y logrando una rápida restauración de los servicios que se puedan ver afectados.

Fase 5 – Pruebas y validación. - Realizar simulacros de incidentes de seguridad cibernética para probar la efectividad del plan de respuesta a incidentes y evaluar la capacidad del personal del hospital asignado en cada uno de sus roles y responsabilidades. Tras el simulacro hay que realizar una retroalimentación con personal interno y externo, si es posible, para detallar que tanto efectivo o puntos que se deban corregir inmediatamente.

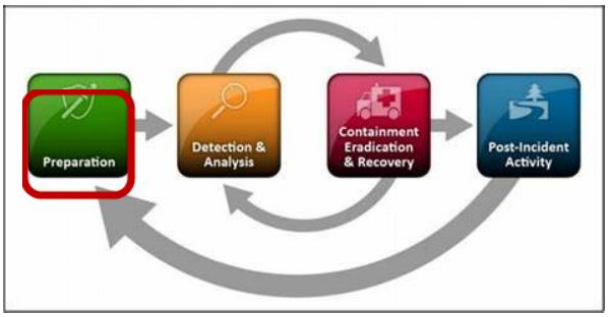
Fase 6 - Implementación. - Implementar el plan de respuesta a incidentes en el hospital, asegurando la capacitación adecuada del personal en los procedimientos y protocolos establecidos.

Fase 7 - Concientización. - Realizar sesiones de concientización y capacitación periódicas para garantizar que todo el personal esté familiarizado con el plan de respuesta a incidentes y sepa cómo actuar en caso de un incidente de seguridad, manteniendo en consideración de manera inicial los criterios para conocer un incidente de seguridad cibernética.

Fase 8 – Mejora Continua. - Realizar revisiones periódicas del plan de respuesta a incidentes implementado para incorporar nuevos hallazgos de seguridad, lecciones aprendidas de incidentes pasados y cambios que se implementaron en la infraestructura tecnológica del hospital.

5. Resultados y discusión

5.1 Preparación



En la fase de PREPARACION, se establece el marco normativo interno, estableciendo con claridad los principios que deberán observarse durante el proceso de manejo de un incidente. A continuación, se desarrolla la Política de Gestión de Incidentes de Ciberseguridad: (CISA, s.f.)

PUBLIC HOSPITAL

POLÍTICA DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Introducción
El Hospital almacena información de pacientes, personal y usuarios y son activos críticos susceptibles a un ciberataque. La presente política establece principios elementales que deberán aplicarse en caso de materialización de un incidente.

Ámbito de aplicación
Esta política se aplica a todos los empleados, contratistas y otras personas que tienen acceso a la información pública del hospital.

Propósito
El propósito de esta política es establecer procedimientos para identificar, clasificar, responder y recuperarse de incidentes de ciberseguridad.

Definición
Incidente de seguridad: Un incidente que viola o amenaza la seguridad de la información médica.

- **Evento de seguridad**: un evento que indica una posible vulnerabilidad de seguridad.

- **Equipo de respuesta a incidentes de ciberseguridad (CSIRT)**: equipo que maneja incidentes de ciberseguridad.

Responsabilidades

- **Gerente de Seguridad de la Información:** Responsable de implementar y mantener políticas.
- **CSIRT**: Responsable de investigar, responder y recuperarse de incidentes de ciberseguridad.
- **Empleados**: Obligados a informar de las incidencias de seguridad que observen.

Política de gestión de incidentes

- **Detección e informes**: Los empleados que tengan conocimiento de un incidente de seguridad deben informarlo inmediatamente al CSIRT.
- **Clasificación:** El CSIRT clasifica los incidentes según la gravedad y el impacto potencial.
- **Investigación**: El CSIRT está investigando el incidente para determinar su causa, alcance e impacto.
- **Contención**: El CSIRT trabaja para contener incidentes y minimizar daños.
- **Erradicación**: Activador de eliminación de CSIRT.
- **Recuperación**: El CSIRT restaura el sistema afectado a su funcionamiento normal.
- **Lecciones Aprendidas:** El CSIRT documentará las lecciones aprendidas de este incidente y recomendará cambios en las políticas y procedimientos de seguridad.

Comunicación

El CSIRT es responsable de comunicar los incidentes de seguridad cibernética a los gerentes, el personal y las partes interesadas, según corresponda.

Revisión y cambios

Esta política se revisará y actualizará periódicamente para reflejar los cambios en las áreas de riesgo y las mejores prácticas.

ELABORADO POR:

SEGURIDAD DE LA INFORMACION

Christian Cusme M.

José Luis Buenaño Q.

GERENCIA HOSPITALARIA

Carlos Mendoza M.

Actualmente, el equipo de Seguridad de la Información debido a su estructura ha decidido tercerizar como servicio, la disponibilidad de un CSIRT como parte del servicio de SOC (Security Operation Center). Como parte del alcance del servicio, el proveedor debe evidenciar que se mantiene un permanente plan de capacitación en respuesta a incidentes de seguridad para el personal que forma parte del CSIRT, garantizando que la estructura proporcionada como servicio sea plenamente competente. A continuación, se describe la estructura del CSIRT y herramientas que se han determinado que se utilicen para su operación.

Siguiendo la guía del documento NIST 800-61 en la sección 2.4.1 Team Models, y considerando que al momento la institución no ha contado anteriormente con un equipo de respuesta a incidentes, se ha adoptado el modelo “Central Incedent Response Team” en el cual un único equipo de respuesta atiende a la totalidad de la institución, la cobertura del CSIRT se mantendrá en 24x7x365.

Descripción de la estructura:

El equipo CSIRT está estructurado en 4 niveles principales:

1. Nivel Directivo:

- Gerente de Seguridad de la Información: Lidera el equipo CSIRT y es responsable de la implementación y el mantenimiento de la política de gestión de incidentes de ciberseguridad.
- Gerente CSIRT: Supervisa las operaciones diarias del equipo CSIRT y coordina con otras áreas del hospital.

2. Nivel de Gestión:

- Especialista Líder de Respuesta: Dirige las investigaciones y respuestas a incidentes de ciberseguridad.
- Analista de Inteligencia de Amenazas: Investiga las últimas amenazas cibernéticas y proporciona información al equipo CSIRT.

- Analista Forense: Analiza evidencia digital para identificar la causa y el alcance de los incidentes de ciberseguridad.

3. Nivel Técnico:

- Especialista en Respuesta a Incidentes: Realiza investigaciones y responde a incidentes de ciberseguridad.
- Ingeniero de Seguridad de Redes: Protege la infraestructura de red del hospital contra ataques cibernéticos.
- Ingeniero de Seguridad de Aplicaciones: Protege las aplicaciones del hospital contra ataques cibernéticos.

4. Nivel de Soporte:

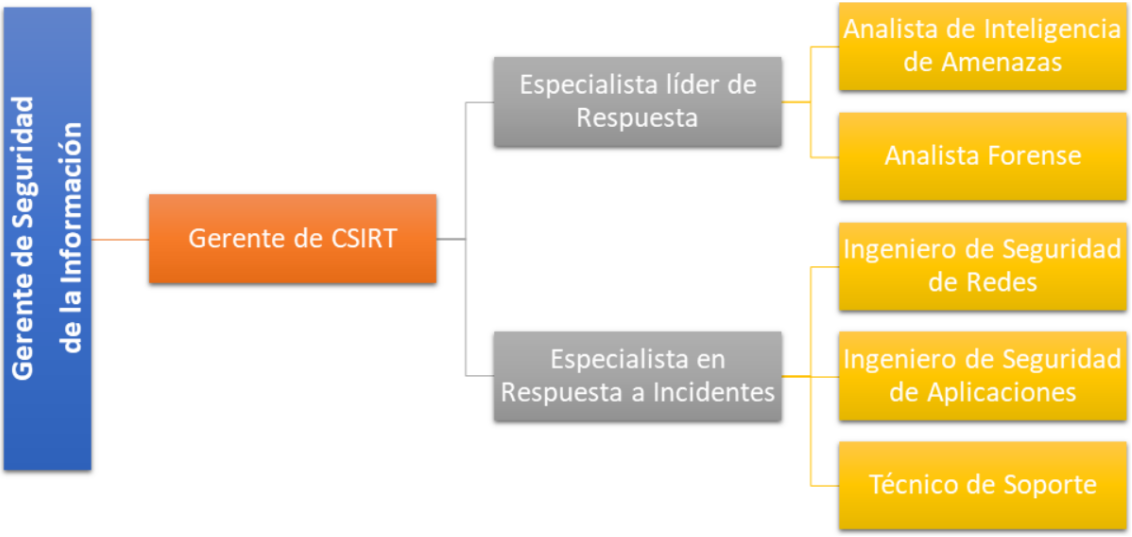
- Técnico de Soporte: Brinda soporte técnico al equipo CSIRT y a los usuarios del hospital.

Consideraciones de Operación:

- Esta estructura puede variar según ajustes a nivel institucional tales como variaciones en el tamaño de la estructura y la complejidad de las operaciones del hospital.
- El equipo CSIRT deberá mantener las habilidades y experiencia necesarias para responder a una amplia gama de incidentes de ciberseguridad.
- El equipo CSIRT colaborará estrechamente con otras áreas del hospital, como TI, Operaciones Legales y Comunicaciones.

ORGANIGRAMA DE EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD (CSIRT)

(NIST SP 800-53, s.f.)



Herramientas utilizadas por el CSIRT

A fin de cumplir con las actividades de investigación y respuesta a incidentes de seguridad, se contempla el uso de las siguientes herramientas:

Tipo	Nombre	Descripción
Computadores	Computador	Computador para uso de los diferentes miembros del equipo CSIRT
Software	Herramienta de adquisición de imágenes:	Herramienta que pueda crear una copia exacta o imagen de un disco duro.
	Software de duplicación de discos	Software para obtención de copia exacta de un disco duro.
	Herramienta de análisis forense	Analizar una imagen de disco duro para recuperar datos y realizar investigaciones
	Herramienta de recuperación de datos	Recuperar datos de un disco duro, incluso si ha sido borrado o formateado.
Herramientas de investigación, detección y respuesta	Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):	Monitoreo de tráfico de red en busca de actividades sospechosas y potencialmente maliciosas, generando alertas o tomando acciones automáticas para prevenir el daño. Ejemplo: Snort, Suricata.
	Herramientas de Monitoreo de Red	Captura y análisis de flujos de tráfico de red para identificar patrones inusuales o actividad sospechosa que pueda indicar un incidente de seguridad. Ejemplo: Wireshark, Nagios.
	Herramientas de Gestión de Información y Eventos de Seguridad (SIEM):	Recopilar, correlacionar y analizar registros de múltiples fuentes para detectar y responder a incidentes de seguridad en tiempo real. Ejemplo: Splunk, IBM QRadar.
	Herramientas de Respuesta y Contención de Incidentes:	Identificación, contención y remediación de amenazas en endpoints (puntos finales) a través de la detección avanzada y respuestas

		automatizadas. Ejemplo: Carbon Black Response, CrowdStrike Falcon.
	Herramientas de Análisis de Malware	Análisis de archivos sospechosos en entornos controlados para identificar comportamientos maliciosos y comprender mejor el malware involucrado en un incidente. Ejemplo: Cuckoo Sandbox, VirusTotal.
	Plataformas de Orquestación, Automatización y Respuesta de Seguridad (SOAR)	Diversas herramientas de seguridad integradas automatizan flujos de trabajo y coordinan la respuesta a incidentes, mejorando la eficiencia y efectividad del equipo. Ejemplo: Demisto, Phantom.
Comunicación	Herramientas de Comunicación y Colaboración	Comunicación rápida y eficiente entre los miembros del equipo de respuesta a incidentes y otros stakeholders durante un incidente. Ejemplo: Slack, Microsoft Teams.

Plan de formación y capacitación para el CSIRT

Objetivo:

Desarrollar y mantener las habilidades y conocimientos necesarios para que los miembros del Equipo de Respuesta a Incidentes de Seguridad (CSIRT) prevengan, detecten, analicen, controlen, mitiguen y se recuperen de manera efectiva de incidentes de seguridad.

Alcance: Este plan de formación anual está destinado a todos los miembros del CSIRT, incluidos:

- Analistas de Seguridad: Responsables de detectar, analizar y contener incidentes de seguridad.
- Investigadores de seguridad: responsables de investigar completamente los incidentes de seguridad y determinar la causa raíz.
- Especialistas en respuesta a incidentes: Responsables de la coordinación y gestión general del proceso de respuesta a incidentes.
- Gerente de CSIRT: responsable de la supervisión general del equipo de CSIRT y de garantizar que se cumplan los objetivos de respuesta a incidentes.

Duración: Este plan de formación anual se desarrollará a lo largo de un periodo de 12 meses.

Metodología: La formación se llevará a cabo mediante diversos métodos, los cuales incluyen:

- Entrenamiento personal: clases impartidas por instructores experimentados en respuesta a incidentes de seguridad.
- Capacitación en línea: cursos en línea a su propio ritmo sobre temas específicos de respuesta a incidentes.
- Ejercicios prácticos: ejercicios de simulación y juegos de roles para practicar las habilidades de respuesta a incidentes.
- Mentoría: tutoría personalizada con expertos en respuesta a incidentes.

Contenido: El contenido de la capacitación se basará en las necesidades específicas del CSIRT y las últimas amenazas y vulnerabilidades de seguridad. Los temas cubiertos pueden incluir:

1. Fundamentos de respuesta a incidentes: introducción a los principios y prácticas de respuesta a incidentes de seguridad.
2. Detección y análisis de incidentes: Técnicas de detección y análisis de incidentes de seguridad.
3. Contención y erradicación de incidentes: Técnicas de contención y erradicación de incidentes de seguridad.
4. Recuperación de incidentes: Técnicas de restauración de sistemas y datos afectados por incidentes de seguridad.
5. Investigación de incidentes: Técnicas para investigar a fondo los incidentes de seguridad y determinar la causa raíz.
6. Gestión de Incidentes: Técnicas para gestionar eficazmente el proceso de respuesta a incidentes.
7. Leyes y regulaciones: Leyes y regulaciones relacionadas con la respuesta a incidentes de seguridad.
8. Herramientas de respuesta a incidentes: herramientas comunes utilizadas para responder a incidentes de seguridad.

Evaluación: El aprendizaje de los participantes se evaluará mediante una combinación de métodos que incluyen:

- Pruebas: Pruebas escritas y prácticas para evaluar los conocimientos de los participantes.
- Ejercicios prácticos: Evaluación del desempeño de los participantes durante ejercicios de simulación y juegos de roles.
- Comentarios: comentarios de los participantes sobre el contenido y la impartición de la capacitación.

Documentación y Registro de Incidentes

A continuación, se establece el formato de registro y documentación para los incidentes de seguridad, de tal forma que puedan detallarse d manera sistemática y facilitar su análisis y aprendizaje

FORMATO DE REGISTRO DE INCIDENTES DE CIBERSEGURIDAD

INFORMACIÓN DEL INCIDENTE
ID DEL INCIDENTE: HOSP-002XXX
FECHA Y HORA DEL INCIDENTE: _____

TIPO DE INCIDENTE:
( ) PHISHING ( ) MALWARE ( ) ATAQUE DDOS ( ) RANSOMWARE ( ) ACCESO NO AUTORIZADO ( ) PÉRDIDA DE DATOS ( ) OTRO (ESPECIFICAR): _____

DESCRIPCIÓN DEL INCIDENTE:
_____
_____

INFORMACIÓN DEL REPORTANTE
NOMBRE DEL REPORTANTE: _____
ORREO ELECTRÓNICO DEL REPORTANTE: _____
TELÉFONO DEL REPORTANTE: _____

IMPACTO DEL INCIDENTE: _____
_____

SISTEMAS AFECTADOS:
_____
_____

GRAVEDAD DEL INCIDENTE:
( ) BAJA ( ) MEDIA ( ) ALTA ( ) CRÍTICA ( ) IMPACTO EN EL NEGOCIO:

ACCIONES TOMADAS

_____
_____

FECHA Y HORA DE LAS ACCIONES INMEDIATAS: _____
PERSONAL INVOLUCRADO EN LA RESPUESTA: _____
RESOLUCIÓN DEL INCIDENTE:
_____
_____

FECHA Y HORA DE LA RESOLUCIÓN DEL INCIDENTE: _____

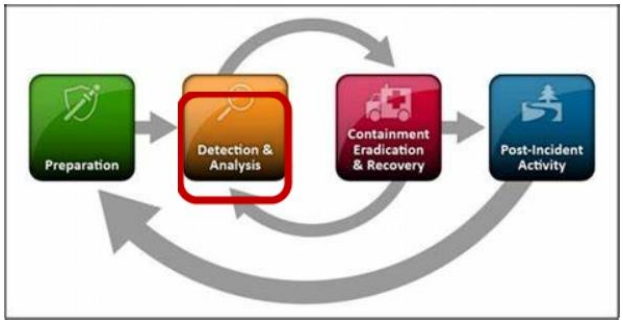
LECCIONES APRENDIDAS:
_____
_____
_____

FIRMA

_____
RESPONSABLE DE EQUIPO DE RESPUESTA A INCIDENTES

FECHA DE APROBACIÓN DEL INFORME: _____

5.2 Detección y análisis



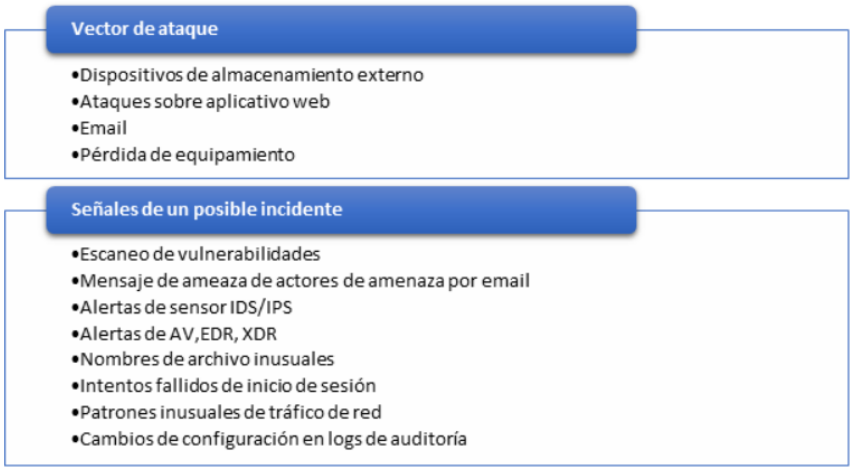
En esta etapa del plan de respuesta a incidentes de ciberseguridad, se establecen las actividades que deben realizarse a fin de supervisar, detectar y alertar cuando se produce un incidente.

Estrategia de detección

Como parte del presente plan se establecen las herramientas, directrices y medidas que se utilizarán para detectar un incidente:

Vectores de ataque y señales un posible ataque

En virtud de la operación del hospital se determinan que se priorizará el análisis sobre los siguientes vectores de ataque:



VECTORES DE ATAQUE

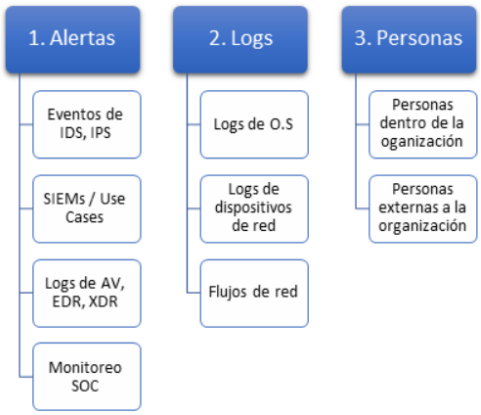
- **Dispositivos de almacenamiento externo:** Ejecución de un ataque desde un medio extraíble o un dispositivo periférico, por ejemplo, malware que se propaga a un sistema desde una unidad flash USB infectada. (CybserSecurityNews)
- **Ataques web:** Ataque desde una aplicación web, por ejemplo, un ataque Cross-site-scripting, con el fin de robar credenciales o realizar redirección hacia un sitio fraudulento, o que infecta de malware al endpoint local.
- **Email:** Ataque mediante el envío de un mensaje de correo electrónico con un enlace o un archivo adjunto malicioso.
- **Pérdida o robo de equipamiento:** Pérdida o robo de un dispositivo informático utilizados por la organización, tal como como un ordenador portátil, un smartphone o un token de autenticación.
- **Dispositivos de almacenamiento externo:** Ejecución de un ataque desde un medio extraíble o un dispositivo periférico, por ejemplo, malware que se propaga a un sistema desde una unidad flash USB infectada.

Fuentes de indicadores de un incidente

A continuación, se describen las fuentes que se utilizarán para realizar la detección y análisis de un posible incidente, con estas herramientas se podrá identificar y posteriormente declarar un incidente de ciberseguridad:

- **Eventos IDS, IPS:** Identifican eventos sospechosos y registran los datos pertinentes sobre ellos, incluida la fecha y hora en que se detectó el ataque, el tipo de ataque, las direcciones IP de origen y destino, y el nombre de usuario (si corresponde y se conoce). La mayoría de los productos IDPS utilizan firmas de ataque para identificar actividades maliciosas; a menudo produce falsos positivos, es decir, alertas que indican que se está produciendo una actividad maliciosa, cuando en realidad no ha habido ninguna. Los analistas deben validar manualmente las alertas de IDS / IPS.
- **SIEM: Security Information and Event Management (SIEM),** generan alertas basadas en el análisis de datos provenientes de logs generados por diferentes componentes de la red, que se centralizan en la plataforma SIEM. (CybserSecurityNews)
- **Logs de AV, EDR, XDR:** El software antivirus detecta varias formas de malware, genera alertas y evita que el malware infecte los hosts. Los productos antivirus, EDR, XDR actuales son eficaces para detener muchos casos de malware conocidos y desconocidos
- **Monitoreo / SOC:** Servicios de monitoreo de seguridad realizadas por un Centro de Operaciones de Seguridad (SOC), así como otras fuentes externas confiables
- **Logs de Sistema Operativo (O.S.):** Los registros de los sistemas operativos, los servicios y las aplicaciones (en particular, los datos relacionados con las auditorías) suelen ser de gran valor cuando se produce un incidente, como el registro de las cuentas a las que se accedió y las acciones que se realizaron. Las organizaciones deben requerir un nivel de referencia de registro en todos los sistemas y un nivel de referencia más alto en los sistemas críticos. Los registros se pueden utilizar para el análisis correlacionando la información de eventos.

- **Logs de Dispositivos de red:** Los registros de dispositivos de red, como firewalls y enrutadores. Aunque estos dispositivos suelen estar configurados para registrar los intentos de conexión bloqueados, proporcionan poca información sobre la naturaleza de la actividad. Aun así, pueden ser valiosos para identificar las tendencias de la red y correlacionar los eventos detectados por otros dispositivos.
- **Flujos de red:** Sesión de comunicación particular que se produce entre hosts. Los enrutadores y otros dispositivos de red pueden proporcionar información sobre el flujo de la red, que se puede utilizar para encontrar actividad anómala en la red causada por malware, exfiltración de datos y otros actos maliciosos. Existen muchos estándares para los formatos de datos de flujo, incluidos NetFlow, sFlow e IPFIX. (Cyberpedia)
- **Personas dentro de la organización:** Los usuarios, los administradores de sistemas, los administradores de red, el personal de seguridad y otras personas de la organización pueden informar de signos de incidentes
- **Personas externas a la organización:** Informes de incidentes que se originan externamente. Por ejemplo, la organización puede ser contactada por una parte que afirma que un sistema de la organización está atacando sus sistemas. Los usuarios externos también pueden informar de otros indicadores, como una página web desfigurada o un servicio no disponible. (NIST, s.f.)



Análisis del Incidente

Utilizando el insumo previamente determinado en el presente plan, se realizarán las siguientes actividades a ejecutarse:

Plan De Respuesta A Incidentes De Ciberseguridad LINEAMIENTOS PARA LA ETAPA DE ANÁLISIS DEL INCIDENTE

• **Perfilamiento de Redes y Sistemas**
  ○ Realizar mediciones periódicas de las características de la actividad esperada en redes y sistemas.
  ○ Utilizar software de verificación de integridad de archivos para obtener checksums de ficheros que puedan ser de gran relevancia.
  ○ Establecer mediante monitoreo el consumo normal (baseline) de ancho de banda.
• **Aprendizaje de Comportamientos Normales**
  ○ Estudiar y documentar el comportamiento normal de redes, sistemas y aplicaciones del hospital.
  ○ Realizar revisiones frecuentes de registros y alertas de seguridad para identificar comportamientos anómalos.
  ○ Utilizar filtros para reducir la cantidad de datos a revisar y enfocarse en entradas inexplicadas.
• **Crear una Política de Retención de logs**
  ○ Se debe documentar de manera formal cuál será el lineamiento referente a la conservación de los datos de registro.
  ○ Debe asegurarse de que los registros de firewall, IDPS y aplicaciones sean conservados durante un período adecuado para análisis futuros.
• **Realizar Correlación de Eventos**
  ○ Correlacionar datos de múltiples registros, como registros de firewall y aplicaciones, para validar incidentes y comprender su alcance.
  ○ Examinar los registros de los hosts para determinar si un ataque fue exitoso y recopilar información adicional.
• **Mantener Relojes de Hosts Sincronizados**
  ○ Debe mantenerse configurado el protocolo NTP para sincronizar los relojes de todos los hosts del hospital.
  ○ Verificar periódicamente la consistencia de los ajustes de reloj en todos los dispositivos para asegurar la precisión de los registros.
• **Mantener y Usar una Base de Conocimientos**
  ○ Se mantendrá una base de conocimientos con información relevante para los analistas de incidentes.
  ○ Se debe Incluir explicaciones sobre la significancia y validez de precursores e indicadores de un incidente, estos pudieran ser alertas generadas por las soluciones de seguridad defensiva como IPS / IDS, logs a nivel de sistema operativo y otros eventos generados por las aplicaciones.
• **Usar Motores de Búsqueda en Internet para Investigación**

- Se utilizarán buscadores en internet para ubicar información sobre actividades inusuales.
- Se deben realizar estas búsquedas en estaciones de trabajo separadas para minimizar riesgos de seguridad.

- **Ejecutar Capturadores de Paquetes para Recopilar Datos Adicionales**
  - Utilizar capturadores de paquetes para recolectar tráfico de red relevante cuando los indicadores no proporcionen suficiente detalle.
  - Configurar los capturadores para registrar únicamente el tráfico que coincida con criterios específicos, minimizando la captura de información no deseada.
  - Obtener permisos necesarios antes de usar capturadores de paquetes debido a posibles preocupaciones de privacidad.
- **Filtrar Datos**
  - Implementar estrategias de filtrado para investigar solo la actividad más sospechosa y significativa.
  - Filtrar categorías de indicadores que tienden a ser insignificantes y enfocar los esfuerzos en las categorías de mayor relevancia.
- **Buscar Asistencia de Otros**
  - Consultar con expertos internos o personal fuera de la organización que pueda aportar información relevante tal como los CERT o CSIRT, cuando no se pueda determinar completamente la causa y naturaleza de un incidente.
  - Asegurar una determinación precisa de la causa de cada incidente para poder contenerlo completamente y mitigar las vulnerabilidades explotadas.

Documentación del incidente

Durante todo el proceso de manejo del incidente deberán registrarse todos los detalles relevantes del incidente, tales como:

- Etiqueta del estado del incidente
- Información general sobre el incidente incluyendo un resumen
- Indicadores que hayan sido observados en el manejo del incidente
- Referencias de otros incidentes de seguridad que pudieran guardar relación con el actual.
- Acciones específicas que se han ejecutado
- Descripción de los mecanismos para el cuidado de la integridad y custodia de las evidencias (cadena) de las evidencias relevadas
- Evaluaciones que se hayan realizado sobre las consecuencias o posible impacto del incidente.

- Datos de contacto de otras personas involucradas en la gestión del incidente (propietarios de sistemas, administradores de sistemas)
- Listado de las pruebas recopiladas durante la investigación del incidente
- Comentarios del equipo CSIRT
- Siguientes pasos sugeridos
- Otros detalles del incidente a documentarse

El equipo de respuesta a incidentes se encargará de salvaguardar los datos del incidente y restringir el acceso a estos, dado que todo detalle del incidente es considerado información confidencial. (Cyber.gov.au, s.f.)

Toda comunicación formal con respecto al incidente debe enviarse siempre a través de medios o canales seguros, cifrados y que cuenten con la protección necesaria cuidando que solo el personal autorizado pueda leerlos.

El CSIRT utilizará para la documentación de los incidentes la herramienta RTIR (Request Tracker for Incident Response) que cuenta con las siguientes características:

Request Tracker for Incident Response (RTIR) es un sistema de seguimiento y gestión de incidentes robusto diseñado para optimizar las actividades del equipo CSIRT y contar con la información oportuna para su correcto seguimiento.12. RTIR se basa en todas las características de Request Tracker (RT) y proporciona colas y workflows preconfigurados específicamente diseñados para CSIRT. Estos son algunos aspectos clave de la herramienta RTIR:

Flujo de Trabajo de Manejo de Incidentes:

- RTIR ofrece información por separada y segregada para un correcto análisis, manejo, y ejecución de medidas de remediación por incidente.
- Permite comunicar de manera simple las acciones en respuesta al incidente, personalizables mediante el sistema de plantillas de correo electrónico flexible de RT.
- La configuración permite flujos de trabajo paralelos con diferente personal.

- Los datos de los tickets se registran, la información personalizada se almacena en campos y se rastrean las fechas clave cumplir los acuerdos de servicio previamente acordados con respecto al manejo del incidente.

Funcionalidades Clave:

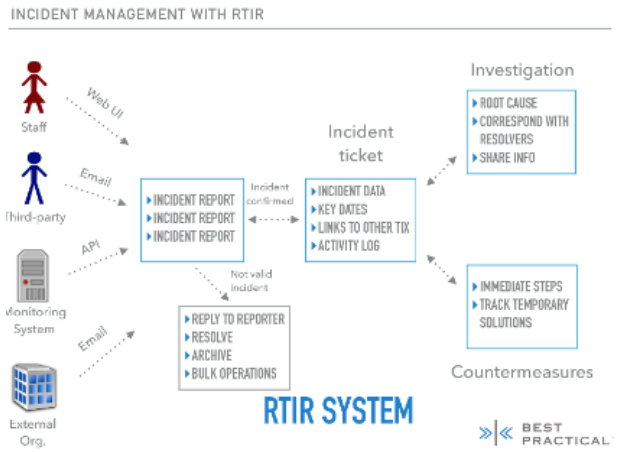
- Cambio de Estado vinculados: Permite que las tareas o acciones que se han ejecutado se registren en lo tickets relacionados.
- Comunicación: Responde a la persona o personas interesadas que hayan sido registradas en el ticket del incidente de seguridad.
- Consolidar / Segregar: Manejo flexible a medida que evolucionan los incidentes.
- Operaciones Masivas: Maneja lotes grandes de tickets a la vez (por ejemplo, Abandonar en Masa, Rechazar en Masa).
- Integración con la API de RT: Acepta feeds de datos automáticos de sistemas externos (por ejemplo, Splunk, ArcSight, Nagios).
- Colas de Informes de Incidentes: Separa los informes entrantes según diferentes criterios.
- Compatibilidad con Extensiones: RTIR funciona perfectamente con las extensiones de Request Tracker.

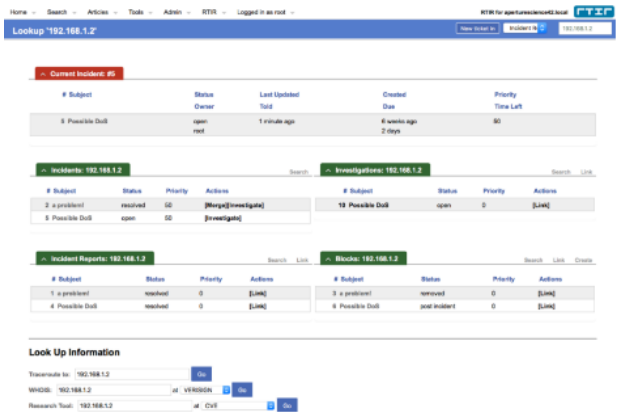
Panel de Incidentes Dedicado:

- Proporciona listados predefinidos de los tickets más urgentes.
- Personalizable para mostrar datos esenciales del incidente.
- Campos personalizados convenientes para rastrear detalles del incidente.

Vinculación y Análisis de Direcciones IP:

- Vincula fácilmente tickets relacionados con un incidente.
- Analiza automáticamente y completa campos personalizados de IP para informes relacionados con redes.





Priorización y Notificación del Incidente

La priorización durante la respuesta al incidente de seguridad es un aspecto crítico en el proceso. Dado que los incidentes no deberán gestionarse por orden de llegada estos se clasificarán en función del impacto que pueden generar en la operación normal del hospital. Este criterio se elige siguiendo las prioridades y objetivos estratégicos del hospital, los cuales demandan como prioridad mantener los servicios disponibles, dado que están directamente vinculados con la atención médica a pacientes y vidas en juego.

Impacto	Definición
Ninguno	El hospital puede seguir prestando todos los servicios a sus usuarios
Bajo	Mínimo impacto: El hospital sigue en capacidad de brindar al menos los servicios más críticos a la totalidad de sus usuarios y clientes, pero se ha visto afectada su eficiencia
Medio	EL hospital perdió su capacidad de brindar servicios críticos a un grupo de usuarios o clientes

Alto	El hospital está impedido de brindar ciertos servicios críticos a ningún usuario o cliente

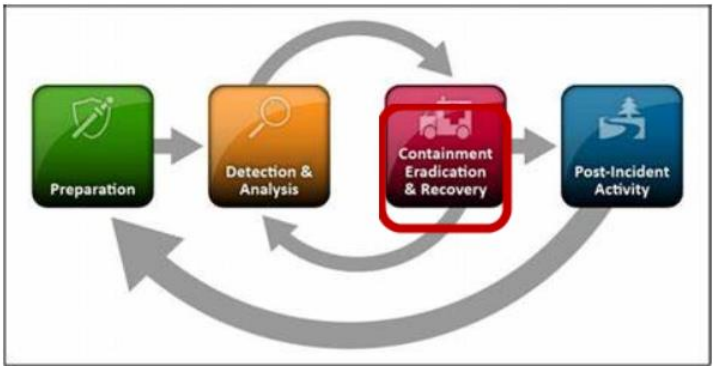
El nivel de impacto será definido entre el CSIRT y el responsable gerencial del área de seguridad de la información (CISO). En función del nivel de impacto del incidente,

Impacto	Nivel de notificación
Ninguno	Supervisor de CSIRT
Bajo	Líder de CSIRT
Medio	CISO, Gerente de Operaciones Hospitalarias
Alto	CISO, Gerente de Operaciones Hospitalarias, Gerente de Hospital

Los detalles del incidente serán comunicados a través de los siguientes canales:

- Correo electrónico
- Llamada telefónica
- Reunión presencial o por videoconferencia
- Informe escrito

5.3 Contención, erradicación y recuperación



A continuación, se detalla la estrategia general de contención, erradicación y recuperación de incidentes de seguridad a aplicarse:

Definiciones:

1 Contención: Proceso de limitar el alcance del incidente y minimizar el daño potencial.

Objetivo: Limitar el alcance del incidente y minimizar el daño potencial. (Incibe, s.f.)

Actividades clave:

- **Iniciar aislamiento:** Desconectar los sistemas afectados de la red o Internet para evitar que el incidente se propague.
- **Contener el acceso a datos**: Restringir el acceso a los datos afectados para evitar su pérdida o alteración.
- **Preservar la evidencia**: Documentar y preservar la evidencia del incidente para su posterior análisis.
- **Comunicar el incidente:** Comunicar la materialización del incidente y consecuencias (impacto) a las partes interesadas

Las acciones de contención que pueden ejecutarse dependerán del tipo y naturaleza del incidente, a continuación, se detallan algunas acciones de contención:

Tipo	Detalles del incidente	Estrategia de contención
Acceso no autorizado	Inicios de sesión fallidos	Bloquear la cuenta
Malware	Infección por malware	Desconectar equipo de la red para evitar propagación
Acceso no autorizado	Cuenta de altos privilegios comprometida	Cambio de contraseña, MFA, desconectar equipo de la red
Escaneos no autorizados	Escaneo de puertos sobre servidor	Establecer bloqueos perimetrales (FW)

2 Erradicación: Proceso de eliminar la causa del incidente y restaurar los sistemas afectados a su estado normal. (Incibe, s.f.)

Tipo	Detalles del incidente	Estrategia de erradicación
Acceso no autorizado	Inicios de sesión fallidos	• Cambiar la contraseña de la cuenta comprometida. • Verificar si hay cuentas adicionales afectadas. • Investigar la causa raíz de los fallos de inicio de sesión.
Malware	Infección por malware	• Escanear y limpiar sistemas infectados. • Identificar la fuente de la infección.

		• Actualizar firmas de antivirus y aplicar parches.
Acceso no autorizado	Cuenta de altos privilegios comprometida	• Investigar cómo se comprometió la cuenta. • Escanear sistemas en busca de malware. • Restablecer la cuenta a un estado seguro. • Implementar MFA
Escaneos no autorizados	Escaneo de puertos sobre servidor	• Verifica la seguridad del servidor • Cerrar cualquier puerto innecesario. • Actualizar las políticas de firewall.

3 Recuperación: Proceso de restaurar los sistemas afectados a su estado normal y reanudar las operaciones normales.

Tipo	Detalles del incidente	Estrategia de Recuperación
Acceso no autorizado	Inicios de sesión fallidos	• Restablecimiento de las credenciales de la cuenta afectada • Comunicación sobre las medidas tomadas.
Malware	Infección por malware	• Restauración de los archivos y sistemas afectados desde copias de seguridad limpias.
Acceso no autorizado	Cuenta de altos privilegios comprometida	• Restablecimiento total de los privilegios y contraseña de la cuenta
Escaneos no autorizados	Escaneo de puertos sobre servidor	• Restauración total de la configuración original del servidor • Monitoreo permanente en busca de actividad sospechosa.

La erradicación y la recuperación se realizarán, de modo que se dé prioridad a las medidas correctivas. Dado que en incidentes a gran escala, la recuperación puede tardar meses; las primeras fases deberán orientarse en elevar la seguridad del entorno, y realizar cambios rápidos que permitan reducir el riesgo de un nuevo incidente. (Cyberwarmag, s.f.)

Durante el proceso de contención, erradicación y recuperación deberá preservarse evidencia a fin de apoyar el proceso de resolución, e incluso ser necesarias para apoyar las acciones legales que correspondan. Por tanto, mantener un registro

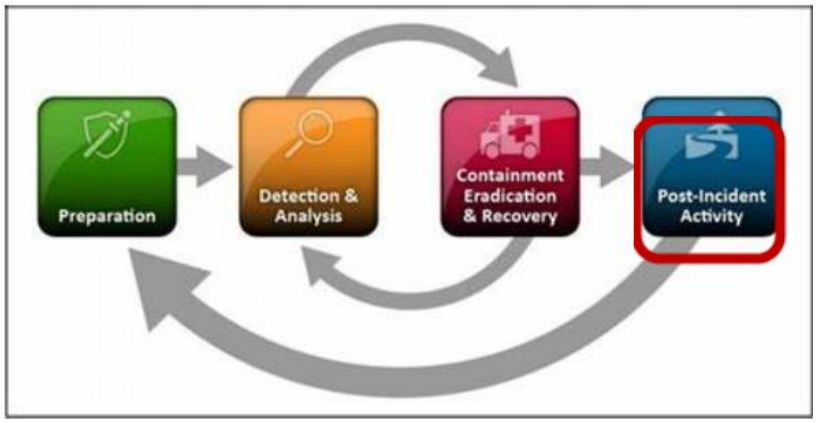
escrito que indique con claridad la manera en que han sido tratadas las posibles evidencias y qué medidas de conservación se han tomado para los sistemas que han llegado a ser comprometidos.

Toda evidencia será recopilada siguiendo los lineamientos establecidos y en cumplimiento con las leyes ecuatorianas de tal forma que cualquier prueba pueda ser admisible en los tribunales.

Se mantendrá un registro detallado de todas las pruebas, tales como:

- Datos que brinden información de identificación tales como: nombre del dispositivo, direcciones IP, dirección física o MAC, etc.
- Nombres y contacto de toda persona que levantó o manipuló algún tipo de evidencia a lo largo del proceso
- Información de fecha y hora para cada evento en el que se realizó algún tipo de manejo de evidencia
- En qué lugares o medios se almacenaron las pruebas.
- Cadena de custodia

5.4 Actividad Post-Incidente



Una vez que se ha realizado las actividades de contención, erradicación y recuperación del incidente, deben realizarse las actividades necesarias para que aproveche s el aprendizaje y fomentar la mejora.

Se debe realizar una reunión de "lecciones aprendidas" con todos los involucrados después de un incidente grave, y establecer con claridad qué medidas pueden tomarse para mejorar las medidas de seguridad y cómo podría optimizarse el proceso de manejo de incidentes. (NIST SP 800-61, 2021)

Esta reunión permite cerrar el ciclo del incidente revisando lo que sucedió, las acciones tomadas y su efectividad. Idealmente, se debe realizar a los pocos días de la finalización del incidente.

A continuación, se resumen algunos puntos que debería abarcar la reunión de lecciones aprendidas siguiendo las recomendaciones de la Guía de Respuesta a Incidentes NIST-800-61:

- Reconstrucción del incidente: ¿Qué sucedió exactamente y cuándo?
- Desempeño del equipo: ¿Cómo fue el accionar del personal del CSIRT?, ¿Se siguieron fielmente las instrucciones y lineamientos documentados? ¿El accionar del personal fue adecuado y efectivo?
- Información que fue necesaria: ¿Qué información se requería con mayor urgencia?
- Impacto en la recuperación: ¿Se tomaron medidas que pudieran haber retrasado la recuperación?
- Lecciones para el futuro: ¿Qué se podría hacer de mejor manera para una ocasión posterior?
- Mejora en la compartición de información con terceros: ¿Qué cosas podrían hacerse mejor en la relacionado con el intercambio o compartición de información con entes externos al hospital?
- Acciones correctivas: ¿Qué acciones de remediación podrían aplicarse desde ya para evitar una materialización similar en el futuro?
- Detección temprana: ¿Existen indicios o señales se deberían monitorear para detectar incidentes similares en el futuro?

Finalmente, se deberá emitir un informe que resuma los puntos clave recopilados durante el manejo del incidente, incluyendo las lecciones aprendidas siguiendo el formato establecido:

GESTION DE INCIDENTES DE CIBERSEGURIDAD
INFORME DE LECCIONES APRENDIDAS

Título del Informe: Informe de Lecciones Aprendidas del Incidente de Seguridad
Fecha del Informe: [Fecha]
Preparado por: [Nombre del Responsable]

1. RESUMEN EJECUTIVO

Descripción del Incidente: Breve resumen del incidente, incluyendo el tipo de incidente y su impacto.
Fecha y Hora del Incidente: Inicio y resolución del incidente.
Impacto: Descripción del impacto en las operaciones, datos y sistemas.

2. DESCRIPCIÓN DETALLADA DEL INCIDENTE

Fecha y Hora del Descubrimiento: [Fecha y Hora]
Fecha y Hora de la Resolución: [Fecha y Hora]
Sistemas Afectados: Listado de los sistemas y datos afectados.
Descripción del Incidente: Detalle del incidente, cómo fue descubierto y cómo se desarrolló.

3. ANÁLISIS DE LA CAUSA RAÍZ

Identificación de la Causa Raíz: Descripción de la causa principal del incidente.
Factores Contribuyentes: Identificación de cualquier factor adicional que contribuyó al incidente.
Métodos Utilizados para el Análisis: Descripción de los métodos y herramientas utilizados para identificar la causa raíz.

4. ACCIONES TOMADAS

Contención: Descripción de las acciones tomadas para contener el incidente.
Erradicación: Medidas implementadas para eliminar la causa raíz del incidente.
Recuperación: Pasos tomados para restaurar los sistemas y operaciones afectadas.

5. ANALISIS DE LA RESPUESTA

Acciones Ejecutadas: Analizar qué tan efectivos fueron los pasos inmediatos que se ejecutaron para la contención, erradicación y recuperación.
Desafíos Encontrados: Descripción de cualquier desafío o problema encontrado durante la respuesta al incidente.
Lecciones Aprendidas: Detalle de las lecciones aprendidas durante la gestión del incidente.

6. RECOMENDACIONES

Mejoras en Políticas y Procedimientos: Recomendaciones para mejorar las políticas y procedimientos de seguridad.
Capacitación y Educación: Propuestas de capacitación adicional para el personal.
Actualización de Herramientas y Tecnologías: Sugerencias para actualizar o adquirir nuevas herramientas y tecnologías de seguridad.

7. PLAN DE ACCIÓN

Acciones Inmediatas: Listado de las acciones que deben tomarse inmediatamente para mitigar riesgos futuros.
Acciones a Mediano y Largo Plazo: Acciones a tomar en el futuro para fortalecer el esquema de seguridad de la información del hospital.
Responsables: Asignación de responsabilidades para cada acción propuesta.

8. DOCUMENTACIÓN DE SOPORTE

Registros y Logs: Incluye cualquier registro o log relevante que respalde el análisis del incidente.
Evidencia Recopilada: Descripción de la evidencia recopilada durante el análisis del incidente.

Informes Adicionales: Cualquier otro informe o documento relevante relacionado con el incidente.

9. APROBACIONES

Aprobado por: [Nombre y Cargo]
Fecha de Aprobación: [Fecha]

5.5 Evaluación

A través de este documento, se ha desarrollado un modelo de plan de respuesta incidentes de seguridad cibernética orientado a una institución hospitalaria, siguiendo las mejores prácticas y metodología descrita en el documento NIST 800-61 Computer Security Incident Handling Guide. Dado que el presente plan está basado en buenas prácticas, se espera que la implementación del plan propuesto logre mejorar significativamente la forma en que los incidentes son manejados, reduciendo su impacto y aprovechando el aprendizaje de estos, lo cual contribuirá a reducir las probabilidades de materialización de un nuevo incidente.

Para evaluar la factibilidad de aplicación del presente plan, se llevó a cabo una encuesta dirigida a 8 profesionales expertos en ciberseguridad y manejo de incidentes que brindan sus servicios a organizaciones de gran tamaño y complejidad tecnológica. A continuación de brinda más detalle de la encuesta y los resultados consolidados de esta:

Encuesta de Evaluación

Plan de respuesta a Incidentes de Seguridad Cibernética para hospital público

Pregunta	Respuesta
1. ¿Considera que es factible la implementación del presente plan?	[ ] Sí [ ] No
2. ¿En la práctica, en qué plazo considera que puede implementarse?	[ ] Corto plazo [ ] Mediano plazo [ ] Largo plazo
3. ¿Considera que este plan es completo y cubre todos los aspectos mínimos que deberían contemplarse para una adecuada gestión de los incidentes?	[ ] Sí [ ] No
4. Los formatos y documentos presentados en el presente plan son prácticos, comprensibles y serían de fácil adopción en su organización?	[ ] Sí [ ] No
5. Adoptaría el presente plan basado en la guía NIST-800-61 para establecer un marco para el manejo de	[ ] Sí [ ] No

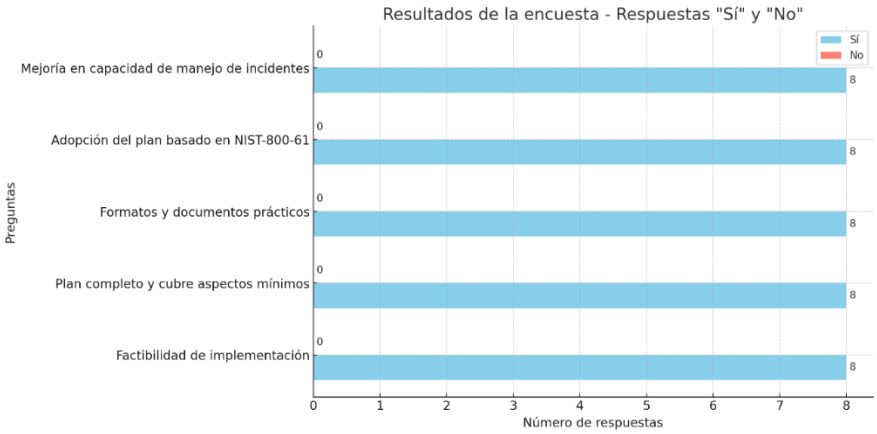
incidentes de seguridad cibernética en su organización?	
6. ¿Considera que a través de la aplicación de los lineamientos descritos en este plan, mejoraría su capacidad actual de manejo de incidentes?	[ ] Sí [ ] No

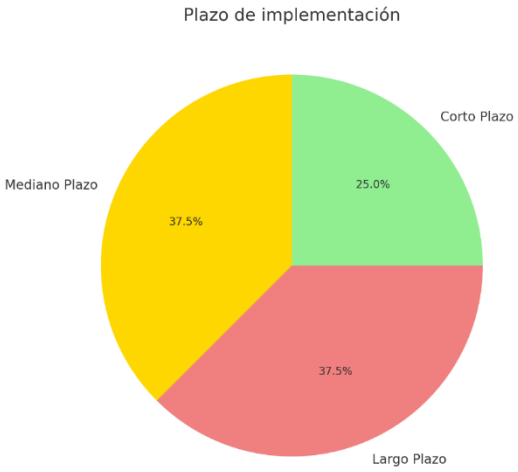
Especialistas Encuestados

Especialista	Cargo	Industria	Tamaño
1	Director de Seguridad de la Información	Banca	Más de 5000 empleados
2	Gerente de Ciberseguridad	Retail	Entre 1000 y 3000 empleados
3	Jefe de Seguridad Cibernética	Gobierno	Entre 500 y 1000 empleados
4	Especialista en Incidentes de Seguridad	Hospitales	Más de 5000 empleados
5	Jefe de Seguridad de Datos	Banca	Más de 5000 empleados
6	Consultora de Seguridad en la Nube	Retail	Entre 1000 y 3000 empleados
7	Responsable de Cumplimiento Normativo	Gobierno	Entre 500 y 1000 empleados
8	Líder de Respuesta a Incidentes	Hospitales	Entre 200 y 500 empleados

Resultados de encuesta de evaluación

Pregunta	Especialista 1	Especialista 2	Especialista 3	Especialista 4	Especialista 5	Especialista 6	Especialista 7	Especialista 8
1. ¿Considera que es factible la implementación del presente plan?	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí
2. ¿En la práctica, en qué plazo considera que puede implementarse?	[x] Corto	[x] Mediano	[x] Largo	[x] Corto	[x] Mediano	[x] Largo	[x] Mediano	[x] Largo
3. ¿Considera que este plan es completo y cubre todos los aspectos mínimos que deberían contemplarse para una adecuada gestión de los incidentes?	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí
4. ¿Los formatos y documentos presentados en el presente plan son prácticos, comprensibles y serían de fácil adopción en su organización?	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí
5. Adoptaría el presente plan basado en la guía NIST-800-61 para establecer un marco para el manejo de incidentes de seguridad cibernética en su organización?	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí
6. ¿Considera que a través de la aplicación de los lineamientos descritos en este plan, mejoraría su capacidad actual de manejo de incidentes?	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí	[x] Sí





Con base en el criterio experto obtenido a través de la encuesta de evaluación realizada producto del presente estudio, se concluye que la propuesta de presente plan es factible y su implementación puede realizarse en organizaciones del sector hospitalario e incluso de otras verticales.

6. Conclusiones

La implementación de un plan que permita una adecuada respuesta frente a un incidente de seguridad es una medida que en la actualidad todo hospital público o centro de salud debería tener instaurado dentro de sus procesos y procedimientos internos, en este caso basado en la guía NIST 800-61, se torna crucial para proteger la información que es considerada muy sensible, y contribuir a mantener de forma continua los servicios de salud que se brinden. A través de este estudio, se ha demostrado que la adopción de un enfoque estructurado y sistemático no solo mejora la capacidad del hospital para detectar, contener y mitigar incidentes de seguridad, sino que también fortalece su resiliencia frente a las crecientes amenazas cibernéticas.

El marco NIST 800-61 proporciona una metodología robusta y adaptable que permite a las organizaciones de salud en este caso, identificar rápidamente las vulnerabilidades, responder de manera efectiva a los incidentes y recuperar las operaciones normales con el mínimo impacto posible. Este plan enfatiza la importancia de la preparación, la identificación temprana, las acciones para responder de forma coordinada y lograr recuperar de manera rápida la operación, siendo esto esencial en un entorno en el cual la disponibilidad y la integridad de los datos son críticas para la atención al paciente.

La capacitación continua del personal, mantener actualizadas las normativas internas (políticas y procedimientos), el despliegue de tecnologías avanzadas de defensa, son elementos fundamentales que se deben aplicar para asegurar la eficacia del plan de respuesta incidentes. Además, la colaboración interdepartamental y la comunicación efectiva juegan un papel vital en la rápida identificación y resolución de incidentes.

En conclusión, mantener un plan adecuado, frente a la materialización de un incidente, y complementado con las herramientas necesarias es indispensable para

proteger los activos digitales de un hospital. Este plan no solo permite mantener la información confidencial, íntegra y disponible, sino que también asegura que el hospital pueda continuar proporcionando atención de calidad a sus pacientes, incluso frente a las amenazas cibernéticas. La adherencia a las directrices establecidas por el NIST 800-61 permite una respuesta más proactiva y efectiva, contribuyendo significativamente a la seguridad global del hospital.

Referencias

Chirinos Meza, O. D. (2022). Gestión de incidentes basado en ITIL 4 para la mejora del servicio de soporte técnico en el instituto cultural peruano norteamericano Región Centro. Obtenido de https://repositorio.uncp.edu.pe/handle/20.500.12894/10349

CISA. (s.f.). Recuperado el 14 de 05 de 2024, de https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Cloudflare. (s.f.). Recuperado el 10 de 6 de 2024, de https://www.cloudflare.com/es-es/learning/security/threats/zero-day-exploit/

Cyber.gov.au. (s.f.). Obtenido de https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

Cyberpedia. (s.f.). Recuperado el 05 de 05 de 2024, de https://cyberpedia.reasonlabs.com/EN/data%20flow%20analysis.html

Cyberwarmag. (s.f.). Recuperado el 26 de 04 de 2024, de https://cyberwarmag.com/gestionar-los-incidentes-de-ciberseguridad/

CybserSecurityNews. (s.f.). Recuperado el 10 de 04 de 2024, de https://cybersecuritynews.com/best-siem-tools/

Ecucert. (s.f.). Recuperado el 24 de 04 de 2024, de https://www.ecucert.gob.ec/centro-de-respuesta-a-incidentes-informaticos-del-ecuador/

Harán, J. M. (04 de 08 de 2022). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2022/08/04/empresas-america-latina-incidentes-seguridad/

Incibe. (s.f.). Recuperado el 19 de 04 de 2024, de https://www.incibe.es/incibe-cert/blog/conoces-guia-nacional-notificacion-y-gestion-ciberincidentes

Marron, J., & Mahn, A. (08 de 2021). *nist.gov.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf

Mian, A. K. (2023). Una revisión de las técnicas de phishing: clasificación, ciclo de vida y enfoques de detección. *IEEE*, 336-339.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (s.f.). Recuperado el 05 de 05 de 2024, de https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/

NIST. (s.f.). Obtenido de https://www.nist.gov/

NIST SP 800-53. (s.f.). Recuperado el 04 de 04 de 2024, de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST SP 800-61. (23 de 04 de 2021). Obtenido de https://www.nist.gov/privacy-framework/nist-sp-800-61