INSTITUTO NACIONAL DE BIODIVERSIDAD

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

2021

INDICE

1. FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

	Nombre / Cargo	Firma	Fecha
Elaborado:	Rosa Bolaños Ibujés **OFICIAL DE SEGURIDAD DE LA INFORMACIÓN**	ROSA ELVIRA BOLANOS IBUJES Firmado digitalmente por ROSA ELVIRA BOLANOS IBUJES Fecha: 2021.09.14 12:47:45 -05'00'	14/09/2021
Revisado por:	María Belén Montenegro **PRESIDENTA DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN** Karol Ivonne Fierro Peralbo **DIRECTORA DE PLANIFICACIÓN Y GESTIÓN ESTRATÉGICA**	Firmado electrónicamente por: MARIA BELEN MONTENEGRO RODRIGUEZ Firmado electrónicamente por: KAROL IVONNE FIERRO PERALBO	14/09/2021
Aprobado por:	Diego Javier Inclán Luna **DIRECTOR EJECUTIVO**		

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del Cambio	Fecha de Actualización
1.0	Versión Inicial	14/09/2021

2. OBJETIVO

Establecer el procedimiento para la Gestión de Incidentes de Seguridad de la Información, por medio de la preparación, detección, análisis, contención, erradicación, recuperación y actividades post incidente; para proteger la confidencialidad, integridad y disponibilidad de la información del INABIO.

3. ALCANCE

Este procedimiento es aplicable para todos los servidores públicos y trabajadores que tengan acceso a los activos de información del INABIO.

4. DOCUMENTOS DE REFERENCIA

- Acuerdo Ministerial 025-2019, Registro Oficial Edición Especial Nro. 228 del 10 de enero de 2020, Esquema Gubernamental de Seguridad de la Información (EGSI), Acápite 12 Gestión de Incidente de Seguridad de la Información, 12.1.1 Responsabilidades y procedimientos 12.1 Gestión de los incidentes de seguridad de la información y mejoras, 12.1.2 Reporte de los eventos de seguridad de la información, 12.1.3 Reporte de debilidades de seguridad de la información, 12.1.4 Apreciación y decisión sobre los eventos de seguridad de la información, 12.1.5 Respuesta a incidentes de seguridad de la información, 12.1.6 Aprendizaje de los incidentes de seguridad de la información, 12.1.7 Recopilación de evidencias.
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001

5. ÁMBITO DE APLICACIÓN

- Oficina matriz. Pasaje Rumipamba N341 y Av. de los Shyris (Parque La Carolina). Quito.
- Oficina ubicada en la Av. Río Coca E6-115 e Isla Fernandina. Quito. Herbario Nacional del Ecuador.
- Oficina ubicada en el Piso 12 del Edificio Contempo. Av. Amazonas y Luis Cordero esquina. Quito.

6. GLOSARIO DE TÉRMINOS Y DEFINICIONES

Ciberseguridad	Es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos que están interconectados
Contención	Es la estrategia de tomar decisiones por medio de procedimientos determinados para evitar que se propague el incidente de seguridad de la información en la institución; la

	contención es relevante antes de que un incidente sobrecargue los recursos o aumente los daños, además, proporciona tiempo para desarrollar una estrategia de remediación a medida y ayuda en la toma de decisiones.
Cross-Site Request Forgery (CSRF)	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que permiten que se ejecuten acciones no deseadas mediante una sesión que ha sido autenticada. Suele utilizarse junto con XSS o inyección SQL
Cross-Site Scripting (XSS)	Estado de vulnerabilidad que se crea por métodos de codificación poco seguros y que tiene como resultado una validación de entradas inapropiada. Suele utilizarse junto con CSRF o inyección SQL.
CSIRT: Computer Security Incident Response Team	Equipo especializado para generar una respuesta a incidentes críticos que generen un alto riesgo para el INABIO.
Erradicación	Es eliminar los componentes del incidente de seguridad de la información, como por ejemplo la eliminación de programas informáticos malignos y la desactivación de las cuentas de usuario violadas, así como la identificación y mitigación de todas las vulnerabilidades que se hayan explotado.
EcuCert	Centro de respuesta a incidentes informáticos del Ecuador.
IDS (Intrusion Detection System)	Sistema de detección de intrusos, es un componente más dentro del modelo de seguridad. Consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior – interior de un sistema informático
INABIO	Instituto Nacional de Biodiversidad
Incidente de Seguridad de la Información	Es el evento asociado a interrupciones o alteración del proceso normal de seguridad de los activos de información digitales, la infraestructura tecnológica, componentes lógicos de información y las interacciones en el ciberespacio con probabilidad significativa de comprometer las operaciones del Instituto.
Ingeniería Social	Mecanismo para obtener información o datos de naturaleza sensible. Las técnicas de ingeniería social son tácticas de persuasión que suelen valerse de la buena voluntad y falta de precaución de los usuarios, y cuya finalidad consiste en obtener cualquier clase de información, en muchas ocasiones claves o códigos.
Inyección SQL	Tipo de ataque a sitios web que manejan bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema

	conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización, mediante la computadora que funciona como servidor de la base de datos.
IPS (Intrusion Prevention System)	Sistema de prevención de intrusos, es un software que ejerce el control de acceso en una red informática para proteger y prevenir a los sistemas institucionales de ataques y abusos.
IP spoofing	Consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
Lecciones aprendidas	Brinda la oportunidad de lograr el cierre con respecto a un incidente al revisar lo que ocurrió, lo que se hizo para intervenir y qué tan bien funcionó la intervención.
MINTEL	Ministerio de Telecomunicaciones y Sociedad de la Información
OSI	Oficial de Seguridad de la Información
Pharming	Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.
Phishing	Método de ataque que busca obtener información personal o confidencial de los usuarios, por medio del engaño, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
Precursores	Son señales de que un incidente puede ocurrir en el futuro.
Ransomware	Es un ataque mediante código malicioso con la intención de secuestrar datos. Una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado. (http://searchdatacenter.techtarget.com/es/)
RAT (Remote Access Tools)	Herramienta para Acceso Remoto. Pieza de software que permite a un "operador" controlar un sistema a la distancia, como si se tuviera acceso físico al mismo. Aunque tiene usos perfectamente legales, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos

	casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.
Recuperación de un incidente de Seguridad de la Información	La recuperación puede incluir acciones como restaurar sistemas limpios, reconstruir sistemas desde cero, reemplazar archivos comprometidos con versiones limpias, instalar parches, cambiar contraseñas y reforzar la seguridad del perímetro de la red de datos o física.
Rootkit	Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos (http://www.alerta-antivirus.es).
Scanning	Proceso mediante el cual se busca vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red de datos. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas.
Sniffing - sniffer	Programas que monitorizan la información que circula por la red de datos con el objeto de capturar información.
SOC - Security Operations Center	Están orientados a proteger la Seguridad (Confidencialidad, Integridad y Disponibilidad) en las redes de datos y servicios, debe tener capacidad para detectar cualquier actividad maliciosa presente en la red de datos, deben informar, gestionar y responder ante distintos incidentes.
Spam	Se denomina “spam” a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor. El “spam” generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias.
Spear Phishing	Es un Phishing dirigido, de forma que se maximiza la probabilidad de que el sujeto, objeto del ataque, pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la víctima).
Spoofing	El término spoofing es una técnica de suplantación de identidad, utilizando una dirección de remitente fraudulenta.
Spyware	Cualquier forma de tecnología que se usa para recoger información sobre una persona o empresa, o información

	referente a equipos o a redes de datos, sin su conocimiento o consentimiento. También puede venir implementado en su hardware. Puede capturar hábitos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet. Al igual que los virus puede ser instalado al abrir un adjunto de correo infectado, pulsando en una ventana de publicidad o camuflado junto a otros programas que instalemos.
TICs	Tecnologías de Información y Comunicación.
Troyano	Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc.
Usuario	Cualquier persona que utiliza una aplicación, programa o servicio tecnológico (internet, correo electrónico, base de datos, etc.) otorgado por el INABIO.
Virus	Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. CONTENIDO TÉCNICO DEL DOCUMENTO

7.1 Procedimiento

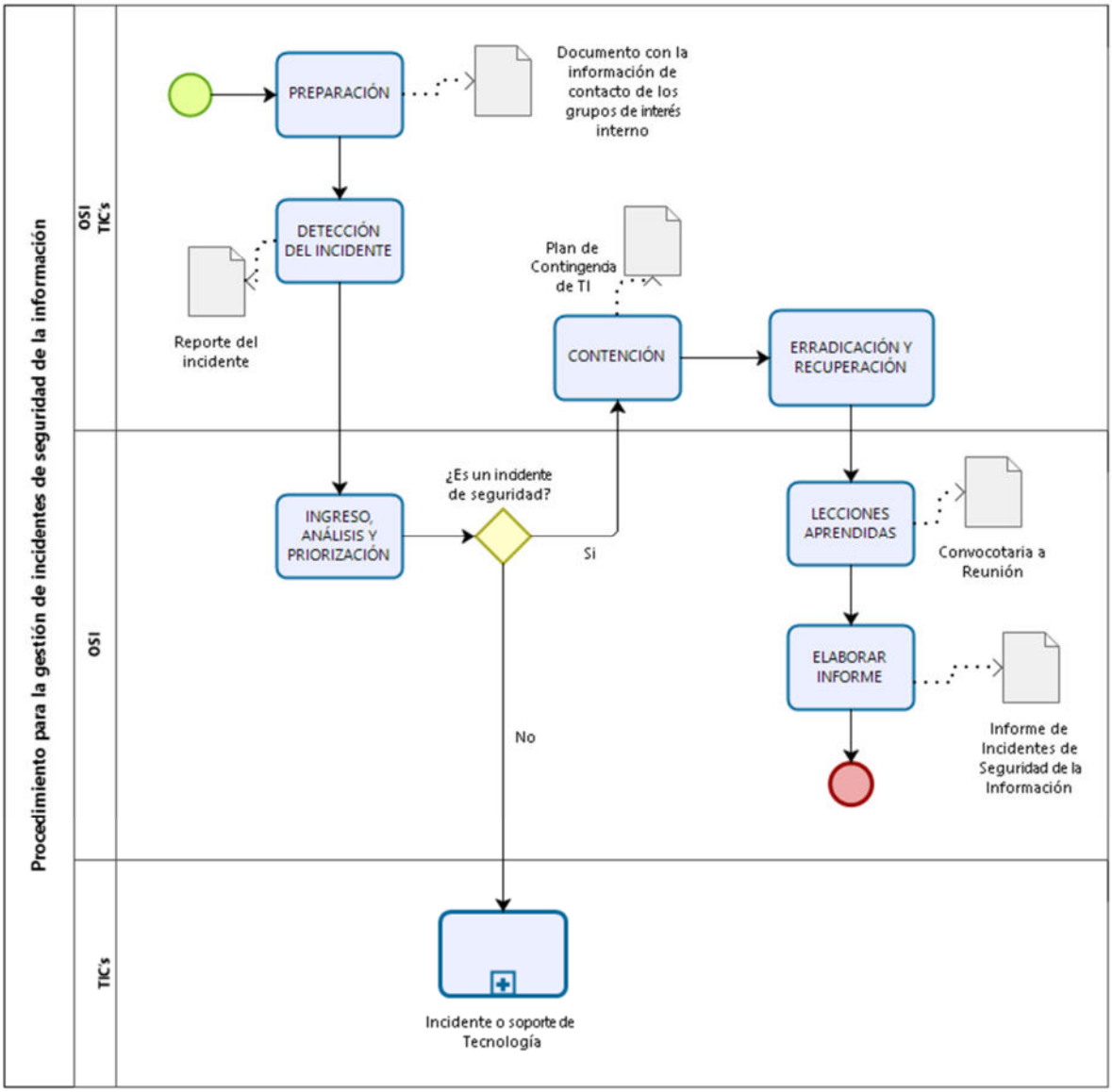
Nombre del procedimiento:	Procedimiento para la gestión de incidentes de seguridad de la información
Objetivo:	Normar la atención, tratamiento y solución de incidentes de seguridad de la información
Responsable:	Oficial de Seguridad de la Información
Disparador:	Notificación de incidentes de seguridad de la información
Responsabilidades:	Todos los servidores públicos y trabajadores que tengan acceso a los activos de información del INABIO, deben reportar por el mecanismo que se encuentre disponible (correo electrónico, mensaje, llamada telefónica) los incidentes de seguridad de la información y ciberseguridad cuando ocurran o exista presunción de ocurrencia, al Oficial de Seguridad de la Información y al Responsable de TIC's. Los incidentes de seguridad de la información catalogados como de incidencia crítica, serán reportados por el OSI al Comité de Seguridad de la Información.

7.2 Descripción del procedimiento

#	Responsable(s)	Tareas
1	OSI TIC's	**PREPARACIÓN** 1. Revisar los controles para reforzar la seguridad en la infraestructura tecnológica y las configuraciones, aplicación de controles y recomendaciones como: A) Reforzar todos los Equipos de Usuario final (host), utilizar configuraciones estándar, mantener actualizado los sistemas operativos, configurar de acuerdo con el principio de privilegio mínimo, entre otros. B) Configurar el perímetro de la red de datos para denegar toda actividad que no esté expresamente permitida. Esto incluye, asegurar todos los puntos de conexión, como redes de datos privadas virtuales (VPN) y conexiones dedicadas a otras organizaciones. C) Configurar las reglas de seguridad, mantener las firmas y actualizaciones de dispositivos, así como firewalls, IDS o IPS, entre otros. El OSI debe revisar continuamente estas configuraciones. D) Implementar en los equipos de usuario final de toda la institución el software para detectar y detener el malware, con las firmas de actualización al día. E) Revisar los perfiles y usuarios en el acceso a Internet para poder identificar un posible incidente mediante el incremento del uso del ancho de banda. F) Analizar, definir y revisar la correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal; así como identificar la causa del incidente. G) Sincronizar los relojes, para un correcto análisis del incidente y facilitar la correlación de eventos y el análisis de la información. H) Capacitar a los usuarios sobre las políticas y procedimientos de incidentes de seguridad de la información, con el fin de reducir la frecuencia de los incidentes. I) Considerar las medidas detalladas en el Anexo 2 para establecer las actividades y tareas. 2. Revisar los riesgos de los sistemas y aplicaciones. 3. Elaborar un documento con la información de contacto de los grupos de interés interno: el Equipo de Respuesta de Incidentes de Seguridad de la Información (CSIRT) y externo el EcuCert, MINTEL, CSIRT privados, ISP entre otros.
2	OSI TIC's	**DETECCIÓN DEL INCIDENTE** Los incidentes pueden ser detectados mediante el análisis de logs de los servicios implementados o pueden ser reportados por un usuario:

		1. Reporte del incidente por un usuario mediante los canales regulares de comunicación (correo electrónico, teléfono o mesa de ayuda). 2. Detectar el incidente por medio del monitoreo de los precursores e indicadores (Anexo 3), descrito en las mejores prácticas como NIST, Guía para la gestión de incidentes, normas ISO entre otras. 3. Informar a las autoridades pertinentes
3	OSI	**INGRESO, ANÁLISIS Y PRIORIZACIÓN** 1. Al incidente reportado o detectado le es asignado un número de caso. 2. Se evalúa si se trata de un incidente de seguridad o no. 3. Cuando no es un incidente de seguridad, se pasa el control a TIC's y se lo atiende como un incidente o soporte de Tecnología. 4. Si el evento se confirma como un incidente de seguridad, se asigna una categoría de criticidad, considerando la tabla descrita en el Anexo 1 como guía, para definir la criticidad (prioridad) del incidente en función de la importancia.
4	OSI TIC's	**CONTENCIÓN** 1. Analizar la contención del incidente de seguridad de la información una vez priorizado. 2. Aplicar la estrategia de contención que varía según el tipo de incidente. 3. Contener el incidente de seguridad de la información (Anexo 4) a través de mejores prácticas como NIST - Guía para la gestión de incidentes, normas ISO entre otras. 4. Activar el Plan de Contingencia de TI, en caso que un incidente de seguridad de la información de impacto alto, afecte gravemente a un activo de información de la infraestructura tecnológica.
5	OSI TIC's	**ERRADICACIÓN Y RECUPERACIÓN** 1. Erradicar identificando y mitigando todas las vulnerabilidades que fueron explotadas del incidente. 2. Erradicar el incidente de seguridad de la información, a través de la implementación del Plan de Mitigación del incidente (Anexo 4) y según mejores prácticas como NIST - Guía para la gestión de incidentes, entre otras. 3. Recuperar la funcionalidad de los sistemas afectados, y realizar la implementación de controles preventivos a los sistemas o servicios afectados, que permita prevenir incidentes similares en el futuro.
6	OSI	**LECCIONES APRENDIDAS** 1. Coordinar reunión de "lecciones aprendidas" para comunicar los incidentes de seguridad de la información, categorizados de impacto alto, con las partes involucradas.
7	OSI	**ELABORAR INFORME** 1. Elaborar el Informe de Incidentes de Seguridad de la Información.

8. DIAGRAMA DE FLUJO



9. ANEXOS

9.1 Anexo 1

Se clasificará la infraestructura crítica en 3 categorías de importancia de acuerdo al proceso crítico de la institución:

a. Muy importante	Infraestructuras de información crítica de la categoría de mayor importancia. • Servicio de virtualización (VMWARE).

	• Servidor de correo electrónico. • Equipos de seguridad perimetral ubicados en las tres oficinas del INABIO. • Servidor de Directorio Activo. • Servidor de la BNDB. • Servidor del portal WEB. • Servidor de antivirus corporativo.
b. Importante	Infraestructuras de información crítica de categoría de importancia media. • Servicio de pruebas de la BNDB. • Servidores de RedBio, INABIO (portal web alterno), BioWiki.
c. Normal	Infraestructuras de información crítica restantes. • Equipos de usuario final. • Impresoras, escáneres. • Otros.

La gravedad del incidente se define en 3 niveles:

a. Altamente riesgoso	El incidente tiene un efecto real en el sistema o la disponibilidad de información, integridad o confidencialidad, o tiene signos de un crimen cometido o una amenaza persistente avanzada (APT), por ejemplo, ransomware, rootkit, intrusiones, violación de información de identificación personal, DoS / DDoS principales, acoso / contenido abusivo de niños / sexuales / violencia, fraude de phishing.
b. Riesgoso	El incidente tiene una probabilidad muy alta de efecto real en el sistema o la disponibilidad de información, integridad o confidencialidad, por ejemplo, código malicioso, violación de la seguridad de la información, vulnerabilidad explotable.
c. Normal	El incidente tiene una probabilidad baja a la normal de afectar el sistema o la disponibilidad de información, la integridad o la confidencialidad, por ejemplo. Spam, recopilación de información, intentos de intrusión, fraudes / enmascaramiento, vulnerabilidad.

Importancia Gravedad	Muy Importante	Importante	Normal
Altamente Riesgoso	Crítico	Crítico	Mediano
Riesgoso	Mediano	Mediano	Mediano
Normal	Mediano	Bajo	Bajo

El tiempo de respuesta inicial para cada clase de evento:

Nivel de prioridad del Incidente	Primer mensaje al (los) usuario(s)
Crítico	en 30-60 minutos
Medio	2-4 horas
Bajo	24 horas

9.2 Anexo 2

- Robustecer la seguridad de la infraestructura tecnológica institucional crítica/sensible.
- Revisar la protección de redes internas.
- Implementar mecanismos de monitoreo para la detección de tráfico atípico o anómalo.
- Disponer se establezcan claves seguras a los usuarios de los sistemas.
- Proteger los equipos informáticos con antimalware actualizado.
- Proteger los portales Web institucionales.
- Proteger y respaldar las bases de datos institucionales.
- Mantener respaldos actualizados de los servidores informáticos e información crítica y mantenerlos en sitios seguros.
- Mantener actualizados los sistemas informáticos y de software.
- Revisar las políticas de seguridad definidas en los equipos de seguridad perimetral.
- Verificar el funcionamiento de los sistemas de respaldo de energía eléctrica institucionales como UPS.
- Difundir las políticas de seguridad de la información a los/as funcionarios/as.
- Utilizar únicamente medios institucionales para el envío y recepción de documentación oficial.

- Implementar las actividades que garanticen la continuidad de las operaciones y servicios.
- Cumplir con lo dispuesto por el Esquema Gubernamental de Seguridad de la Información.

9.3 Anexo 3

Fuentes comunes de precursores e indicadores	
Fuente	**Descripción**
IDPSs	Los productos IDPS identifican los eventos sospechosos y registran los datos pertinentes sobre ellos, incluida la fecha y la 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 o se conoce). La mayoría de los productos IDPS usan firmas de ataque para identificar actividad maliciosa; las firmas se deben mantener actualizadas para poder detectar los ataques más recientes. El software IDPS a menudo produce falsos positivos: alertas que indican que se está produciendo actividad maliciosa, cuando en realidad no ha habido ninguna. Los analistas deben validar manualmente las alertas IDPS ya sea revisando de cerca los datos de soporte grabados u obteniendo datos relacionados de otras fuentes.
SIEMs	Los productos de información de seguridad y gestión de eventos (SIEM) son similares a los productos IDPS, pero generan alertas basadas en el análisis de registros. Su objetivo principal es el de proporcionar una visión global de la seguridad de la tecnología de la información.
Antivirus y antispam	El software antivirus detecta varias formas de malware, genera alertas y evita que el malware infecte hosts. Los productos antivirus actuales son efectivos para detener muchas instancias de malware si sus firmas se mantienen actualizadas. El software antispam se usa para detectar spam y evitar que llegue a los buzones de los usuarios. El spam puede contener malware, ataques de phising y otro código malicioso, por lo que las alertas del software antispam pueden indicar intentos de ataque.
Software de comprobación de integridad de archivos	Este software puede detectar cambios realizados en archivos importantes durante los incidentes. Utiliza un algoritmo hash para obtener una suma de comprobación criptográfica para cada archivo designado. Si se modifica el archivo y se vuelve a calcular la suma de comprobación, existe una probabilidad extremadamente alta de que la nueva suma de comprobación no coincida con la suma de comprobación anterior. Al recalcular regularmente las sumas de comprobación y compararlas con valores anteriores, se pueden detectar cambios en los archivos.
Servicios de monitoreo de terceros	Los terceros ofrecen una variedad de servicios de monitoreo gratuitos y basados en suscripción. Un ejemplo son los servicios de detección de fraude que notificarán a una organización si sus direcciones IP, nombres de dominio, etc, están asociados con actividades de incidentes actuales que involucran a otras organizaciones. También hay listas negras en tiempo real gratuitas con información similar. Otro ejemplo de un servicio de monitoreo extremo es una lista de notificaciones CSIRC; estas listas a menudo solo están disponibles para otros equipos de respuesta a incidentes.
Registros de sistema operativo,	Los registros de los sistemas operativos, servicios y aplicaciones (particularmente los datos relacionados con la auditoría) suelen ser de gran

servicio y logs de aplicación	valor cuando ocurre un incidente, como el registro de cuentas a las que se accedió y las acciones que se realizaron. Las organizaciones deben requerir un nivel de inicio de sesión en todos los sistemas y un nivel de referencia más alto en los sistemas críticos. Los registros se pueden usar para el análisis al correlacionar la información del evento. Dependiendo de la información del evento, se puede generar una alerta para indicar un incidente.
Registro de dispositivos de red	Los registros de dispositivos de red como firewalls y enrutadores generalmente no son una fuente primaria de precursores o indicadores. Aunque estos dispositivos generalmente están configurados para registrar intentos de conexión bloqueados, brindan poca información sobre la naturaleza de la actividad. Aun así, pueden ser valiosos para identificar tendencias de red y para correlacionar eventos detectados por otros dispositivos.
Flujos de red	Un flujo de red es una sesión de comunicación particular que ocurre entre hosts. Los enrutadores y otros dispositivos de red pueden proporcionar información de flujo de red, que se puede usar para encontrar actividad de red anómala causada por malware, exfiltración de datos y otros actos maliciosos. Existen muchos estándares para formatos de flujo de datos, incluidos NetFlow, sFlow e IPFIX}.
Información sobre nuevas vulnerabilidades y exploits	Mantenerse al día con las nuevas vulnerabilidades puede prevenir algunos incidentes y ayudar a detectar y analizar nuevos ataques. La Base de datos nacional de vulnerabilidad (NVD) contiene información sobre vulnerabilidades. 32 organizaciones tales como US-CER33 y CERT/CC periódicamente brindan información de actualización de amenazas a través de reuniones informativas, publicaciones web y listas de correo.
Personas dentro de la organización	Los usuarios, los administradores del sistema, los administradores de red, el personal de seguridad y otros dentro de la organización pueden reportar indicios de incidentes. Es importante validar todos esos informes. Un enfoque es preguntar a las personas que brindan dicha información qué tan seguros están de la exactitud de la información. Registrar esta estimación junto con la información proporcionada puede ayudar considerablemente durante el análisis de los incidentes, especialmente cuando se descubren datos conflictivos.
Gente de otras organizaciones	Los informes de incidentes que se originan en el exterior deben tomarse en serio. Por ejemplo, la organización puede ser contactada por una parte que alega que un sistema de la organización está atacando sus sistemas. Los usuarios externos también pueden informar otros indicadores, como una página web desfigurada o un servicio no disponible. Otros equipos de respuesta a incidentes también pueden informar incidentes. Es importante contar con mecanismos para que las partes externas informen los indicadores y para que el personal capacitado monitoree esos mecanismos cuidadosamente: esto puede ser tan simple como configurar un número de teléfono y una dirección de correo electrónico para reenviar mensajes a la mesa de ayuda.
SOC	Servicio de monitoreo y control a la seguridad implementada en hardware, software, redes y comunicaciones, e identificar oportunamente las posibles vulnerabilidades de seguridad, con el objeto de garantizar una adecuada gestión de incidentes de seguridad.
Referencia – NIST 800-61	

9.4 Anexo 4

Contención-Erradicación y Recuperación de Incidentes de Seguridad de la Información				
Subservicio	**Descripción**	**Tipo**	**Contención**	**Erradicación y Recuperación**
Código malicioso	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus	Desconexión de la red del equipo afectado	Corrección de efectos producidos. Sanitización o Borrado Seguro Restauración de backups
		Gusano		
		Troyano		
		Spyware		
		Ransomware (secuestro informático)		
		Rootkit		
		Herramienta para Acceso Remoto Remote Access Tools (RAT)		
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen	Denegación [Distribuida] del Servicio DoS / DDoS	DDoS incident response CERT	Cierre de vulnerabilidades Restitución del servicio
		Fallo (Hardware/Software/Electrico)	Activación de la contingencia	
		Error humano		
		Sabotaje		
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades	Identificación de vulnerabilidades (scanning)	Incorporación de reglas de filtrado en el firewall	
		Sniffing		
		Ingeniería social	Comunicado a funcionarios	Feedback del incidente para erradicar y comunicado insitucional
		Phishing	Comunicado a funcionarios	
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas.	Compromiso de cuenta de usuario	Bloqueo de cuenta	
		Defacement (desfiguración)	Baja de página y mensaje mantenimiento	Cierre de vulnerabilidades Reparación del sitio web
		Cross-Site Scripting (XSS)	Aplicación de Parches	Cierre de vulnerabilidades Restitución del servicio
		Cross-Site Request Forgery (CSRF)		
		Inyección SQL		
		Spear Phishing	Comunicado a funcionarios	incidente para erradicar y comunicad
		Pharming	Comunicado y bloque de IP atacante por medio del Antimalware	Cierre de vulnerabilidades Restitución del servicio
		Ataque de fuerza bruta	Bloqueo de cuenta	
		Inyección de Ficheros Remota	Aplicación de Parches	
		Explotación de vulnerabilidad software		
		Explotación de vulnerabilidad hardware		
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública	Acceso no autorizado a información	Bloqueo de cuenta	
		Modificación y borrado no autorizada de información		
		Publicación no autorizada de información		
		Exfiltración de información	Bloque de medios de exfiltración	
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes	Suplantación / Spoofing	Comunicado y bloqueo de atacante	Feedback del incidente para erradicar y comunicado insitucional
		Uso de recursos no autorizado	Comunicado y bloqueo de atacante	
		Uso ilegítimo de credenciales	Notificación a Seguridad Física	
Contenido abusivo	Ataques dirigidos a dañar la imagen o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura)	Comunicado y bloqueo por el Antispam	
		Acoso/extorsión/ mensajes ofensivos	Notificación a Talento Humano	
		Pederastia/ racismo/ apología de la violencia/delito, etc.	Notificación a Talento Humano	
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad.	Abuso de privilegios por usuarios	Notificación a funcionario-proveedor de violación de la Política de Seguridad de la Información	
		Almacenamiento de Información como música, videos....		
		Instalación de Software no autorizado		
		Otros		
Referencia-Nist 800-61				