POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIOÓN DE LA PRIVACIDAD

La Política de gestión de incidentes de seguridad de la información, está diseñada para proteger la información, ya que se centra en la identificación temprana de incidentes; Y todos los miembros del equipo deben estar alerta y reportar cualquier actividad sospechosa o incidente de seguridad potencial, con el fin minimizar el impacto, reducir al máximo los daños causados por incidentes de seguridad. Esto incluye la minimización de la interrupción de las operaciones, la pérdida de datos y la reputación de la institución. Promover la respuesta ordenada y efectiva. Esto ayuda a evitar la confusión y el caos que a menudo pueden acompañar a situaciones de emergencia. Aprender y mejorar enfocándose en el aprendizaje continuo y la mejora de las prácticas de seguridad de la información.

Para el Cumplimiento normativo la institución está sujeta a regulaciones y leyes que exigen la implementación de políticas de gestión de incidentes de seguridad de la información. Esta política ayuda a cumplir con estos requisitos. Por tal motivo el Gerente de la Empresa Social del Estado Instituto de Salud de Bucaramanga y el proceso de gestión de TIC'S se comprometen a implementar una política de gestión de incidentes de seguridad de la información a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

1. OBJETIVO

Establecer un enfoque estructurado y meticulosamente planificado para manejar eficazmente los incidentes de seguridad de la información en nuestra organización. Esto implica la definición clara de roles y responsabilidades dentro de la organización, lo que servirá como eje central para evaluar los riesgos y garantizar la operación, continuidad y disponibilidad de nuestros servicios. Además, nos comprometemos a gestionar los eventos de seguridad de la información de manera eficiente, identificando si deben ser clasificados como incidentes. Esto nos permitirá identificar y abordar los incidentes de seguridad de la información de manera eficaz, minimizando sus impactos adversos a través de salvaguardas adecuadas. Asimismo, nos esforzaremos por consolidar las lecciones aprendidas de cada incidente para facilitar un aprendizaje continuo, y estableceremos procedimientos formales de reporte y escalada de incidentes de seguridad.

2. ALCANCE

El alcance de la política de gestión de incidentes de seguridad de la información abarca a todos los activos de información, incluyendo sistemas, datos y aplicaciones, así como a los usuarios y el proceso de Gestión de TI.

3. RESPONSABLE

- Coordinador de TI
- Profesional especializado en seguridad Informática.
- Líder de sistemas de información
- Líder de infraestructura

4. DEFINICIONES

Auditoria: La auditoría se refiere a la evaluación sistemática, independiente y documentada para obtener evidencia objetiva y evaluarla de manera imparcial con el fin de determinar en qué medida se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).
Ciberseguridad: La ciberseguridad se refiere a la protección de los sistemas y datos informáticos contra el acceso no autorizado, el uso malintencionado, la modificación, el robo o la destrucción. La ciberseguridad incluye medidas técnicas, físicas y administrativas para proteger la información. (ISO/IEC 27001:2022).
Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (mintic, s.f.)
Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (mintic, s.f.)
Incidente de seguridad de la información: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.
Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
Información: Datos relacionados que tienen significado para la entidad1. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. (mintic, s.f.)
Riesgos: Los riesgos se refieren a la posibilidad de que ocurra un evento que pueda tener un impacto negativo en un proyecto, una organización o una persona. Los riesgos pueden ser internos o externos, y pueden ser gestionados mediante la identificación, evaluación y mitigación. (ISO/IEC 27001:2022).
Sistema de Información: Conjunto de aplicaciones, servicios, tecnología de información u otros componentes de manejo de información. (ISO/IEC 27001:2022).
Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. (mintic, s.f.)
Id.: Un Id. de usuario es un identificador único de cliente mediante el cual un anunciante elige identificar a un usuario que visita su sitio web. (Ayuda de Google Ads, s.f.)
TI.: El concepto de tecnología de la información refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. (Pérez Porto, 2014)

5. POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIOÓN DE LA PRIVACIDAD

5.1 ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES
Oficial de Seguridad de la Información (CISO)	▪ Supervisión general de la política de gestión de incidentes ▪ Toma decisiones estratégicas en incidentes graves. ▪ Coordinación de comunicación con la alta dirección y otros departamentos clave. ▪ Cumplimiento de regulaciones y estándares. ▪ Registro de incidentes de seguridad de la información que afecten datos personales ante la SIC (superintendencia de industria y comercio)
Ingeniero de Infraestructura	▪ Detección y monitoreo de incidentes en la red. ▪ Supervisión de servidores en busca de actividad maliciosa. ▪ Identificación de patrones y tendencias de incidentes. ▪ Implementación de medidas preventivas y de respuesta en la infraestructura de red. ▪ Colaboración con otros equipos para mitigar incidentes.
Líder de sistemas de Información	▪ Supervisión de sistemas y base de datos en busca de actividad maliciosa.

	▪ Respuesta a incidentes relacionados con sistemas y aplicaciones. ▪ Colaboración en la recuperación y parcheo de sistemas. ▪ Documentación de incidentes y medidas tomadas.
Usuario	▪ Notificación de incidentes de seguridad de la información
Alta Dirección	▪ Aprobación final en situaciones críticas. ▪ Autorización de recursos y acciones a gran escala. ▪ Participación clave en decisiones estratégicas.

5.2 FLUJOS DE COMUNICACIÓN Y ESCALADO EN LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

PASO	ROL	ACCIÓN	PLAZO DE NOTIFICACIÓN	COMUNICACIÓN / ESCALADO
1	Usuario / Equipo Técnico	Detecta un incidente de seguridad de la información y lo notifica al Oficial de Seguridad de la Información (CISO).	Inmediatamente	Notifica al CISO.
2	CISO	Evalúa la gravedad del incidente y realiza una primera respuesta para contenerlo.	1 hora	Comunica con la Alta Dirección si el incidente es grave, así como la notificación a **clientes** y **super intendencia de industria y comercio** – SIC si existe violación a dato personal.
3	CISO	Toma decisiones estratégicas y asigna recursos según la gravedad.	2 horas	Comunica con la Alta Dirección si es necesario.
4	Líder de infraestructura / Líder de sistemas de información	Trabajan en la contención y mitigación del incidente en sus áreas respectivas.	3 horas	Informan al CISO sobre las acciones tomadas.
5	Alta Dirección	Si el incidente es grave, aprueba recursos y toma decisiones estratégicas.	4 horas	Recibe actualizaciones y toma decisiones con el CISO.

PASO	ROL	ACCIÓN	PLAZO DE NOTIFICACIÓN	COMUNICACIÓN / ESCALADO
6	Alta Dirección	Recibe actualizaciones regulares y toma decisiones estratégicas si es necesario.	Según situación	Participa en la toma de decisiones con el CISO.
7	Todos los Roles	Participan en la implementación de medidas preventivas para futuros incidentes.	Según situación	Colaboran en la implementación de medidas preventivas.

5.3 ETAPAS DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Para lograr estos objetivos, la gestión de incidentes de seguridad de la información involucra las siguientes etapas de manera cíclica como lo muestra la imagen:

5.4 PROCESO DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Este proceso le permitirá a la entidad estar preparada para afrontar cada una de las etapas anteriores, y adicionalmente definiendo responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

PREVENCIÓN

- La entidad cuenta con la preparacion antes de la materialización de una amenaza. Se cuentan con campañas de concienciación y sensibilización hacia los funcionarios en materia de ciberseguridad

PROTECCIÓN Y DETECCIÓN

- La entidad cuenta dispositivos hardawre y herramienta de software con el fin de proteger la infraestructura tecnológica de la entidad, entre ellos se encuentran Firewall, sistemas de antivirus corporativo.

RESPUESTA Y COMUNICACIÓN

- La entidad dependiendo de la criticidad del evento y de sus consecuencias,aislara equipos, detendra servicios y deshabilitara cuentas de usuarios entre otros; alterno a ello, se realiza un análisis más profundo de la amenaza para indicar ubicaciones en la infraestructura tecnológica donde puede existir una copia del malware o de artefactos asociados a este. La evidencia se conserva para entender el comportamiento de la campaña.

RECUPERACIÓN Y APRENDIZAJE

- Las lecciones aprendidas siempre se tomar en cuenta en el plan de mejoramiento de la entidad, una vez se identifican las brechas de seguridad y vulnerabilidades en el entorno tecnológico; también se realiza un seguimiento periódico para observar los factores que aún se deben mejorar.

5.5 EQUIPO DE ATENCIÓN A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad ha conformado un equipo de atención de incidentes de seguridad, quienes se encargan de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, este grupo está conformado por:

- Coordinador de TI
- Profesional especializado en seguridad Informática.
- Líder de sistemas de información
- Líder de infraestructura
- Apoyo profesional sistemas

5.6 FUNCIONES DEL EQUIPO DE ATENCIÓN A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

a) **Detección de Incidentes de Seguridad:** Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
b) **Atención de Incidentes de Seguridad:** Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
c) **Recolección y Análisis de Evidencia Digital:** Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
d) **Anuncios de Seguridad:** Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
e) **Auditoria y trazabilidad de Seguridad Informática:** El equipo debe realizar verificaciones periódicas del estado de la seguridad de la información para analizar nuevas vulnerabilidades y brechas de seguridad.

f) **Certificación de productos:** El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
g) **Configuración y Administración de Dispositivos de Seguridad Informática:** Se encargarán de la administración adecuada de los elementos de seguridad informática.
h) **Clasificación y priorización de servicios expuestos:** Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
i) **Investigación y Desarrollo:** Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos de información de la entidad.

5.7 DEFINICIÓN DE LAS ETAPAS DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.7.1 PREPARACIÓN

Esta etapa dentro del ciclo de vida de respuesta a incidentes se busca que la entidad este en capacidad de responder ante incidentes de seguridad de la información, también se define la forma como pueden ser detectadas, evaluadas y gestionadas las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros. El equipo de respuesta a incidentes actúa como una herramienta de experiencia en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los soporta. En esta etapa el equipo de gestión de incidentes vigila la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del mismo, creando y validando los procedimientos necesarios y programas de capacitación. En esta etapa se incluyen las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, entre ellas están:

a) **Gestión de Parches de Seguridad:** La entidad dentro de su infraestructura de servidores y parque computacional, deshabilitó las actualizaciones automáticas con el objetivo de evitar fallos en los sistemas operativos, es por ello que el equipo de infraestructura y sistemas de información analiza cada actualización para ver si esta es aplicada.
b) **Aseguramiento de plataforma:** La entidad configura la menor cantidad de servicios bajo la política de mínimo acceso con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se revisan configuraciones por defecto (usuarios, contraseña) con el propósito de no contar con usuarios por defecto en los sistemas que puedan aumentar el riesgo de acceso no autorizado, de igual forma los servidores tienen habilitados sus sistemas de auditoría que permiten hacer trazabilidad a los diferentes eventos.
c) **Seguridad en redes:** La entidad realiza una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls son revisadas continuamente para mitigar la materialización de amenazas. Las firmas y actualizaciones de dispositivos como IDS o IPS se encuentran al día, de igual forma todos los elementos de seguridad y de red se encuentran sincronizados con sus respectivos logs.
d) **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores como parque computacional) cuentan con una herramienta de antivirus corporativo, antimalware con las firmas de actualización al día.
e) **Sensibilización y entrenamiento de usuarios:** Los usuarios en la entidad incluidos los administradores de TI son sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad.

5.7.2 Recursos de comunicación

INFORMACIÓN DE CONTACTO		
CARGO	**CORREO**	**EXTENSION**
Coordinador de TI	coordinador_it@isabu.gov.co	205
Profesional especializado en seguridad Informática	seguridad.informatica@isabu.gov.co	205
Líder de sistemas de información	sistemas@isabu.gov.co	205
Líder de infraestructura	Sistemas.infraestructura@isabu.gov.co	205
Apoyo profesional sistemas	documentacionsistemas@isabu.gov.co	205

INFORMACIÓN DE ESCALAMIENTO			
CARGO	**CORREO**	**DETALLE**	**EXTENSION**
Profesional especializado en seguridad Informática	seguridad.informatica@isabu.gov.co	Direccionar solicitudes de incidentes de seguridad de la información	205
Líder de sistemas de información	sistemas@isabu.gov.co	Administrador del sistema de información PANACEA	205
Líder de infraestructura	Sistemas.infraestructura@isabu.gov.co	Administrador de la infraestructura tecnológica	205
Talento Humano	talentohumano@isabu.gov.co	Líder del proceso de talento humano por si se requieren acciones disciplinarias	205
CSIRT Gobierno	csirtgob@mintic.gov.co	Identificado el incidente cibernético, por el CISO o encargado de seguridad digital de la entidad, diligenciar el formato de reporte de incidentes en su totalidad y enviarlo al CSIRT Gobierno para su gestión y acompañamiento.	
COLCERT	contacto@colcert.gov.co	Grupo de Respuesta a Emergencias Cibernéticas de Colombia	+57 601 344 2222
Centro cibernético Policía Nacional	N/A	Reportar en la siguiente ruta: https://caivirtual.policia.gov.co/	
Bomberos	N/A	Cuerpo oficial de Bomberos de Bucaramanga	PBX: +(57) 607652 66 66 Central de Emergencias: 119

5.7.3 Políticas de comunicación

La política de comunicación de los incidentes de seguridad es una herramienta importante para una entidad, ya que establece pautas claras sobre cómo se gestionarán y comunicarán los incidentes de seguridad al público y a los medios de comunicación.

A continuación, se definen los lineamientos a tener en cuenta para determinar qué incidentes pueden ser comunicados a los medios y cuáles no,

a) **Definir criterios de clasificación:** La entidad define criterios claros para clasificar los incidentes de seguridad según su gravedad y el impacto potencial en la entidad y sus stakeholders.
b) **Evaluar el impacto:** La entidad realiza una evaluación de impacto para determinar cómo cada incidente puede afectar a la entidad y a sus stakeholders.
c) **Considerar requisitos legales y regulatorios:** La entidad se asegura de cumplir con las leyes y regulaciones aplicables en cuanto a la divulgación de incidentes de seguridad.
d) **Analizar el interés público:** La entidad evalúa si el incidente puede generar un interés público significativo o si puede tener un impacto más amplio en la comunidad.
e) **Considerar la reputación de la entidad:** La entidad evalúa el impacto potencial en la reputación de la entidad al comunicar un incidente de seguridad. Si el incidente puede dañar significativamente la confianza de los clientes, proveedores u otros stakeholders, es importante considerar la divulgación y cómo se manejará la comunicación.
f) **Definir la forma de comunicación:** La entidad especifica cómo se llevará a cabo la comunicación de los incidentes de seguridad, incluyendo el momento adecuado para hacerlo, los canales de comunicación a utilizar y el contenido de los mensajes. Se considera la transparencia y la claridad en la comunicación, brindando información relevante y acciones que se están tomando para abordar el incidente.

5.7.4 Recursos para el análisis de incidentes

El análisis de un incidente de seguridad de la información requiere de diversos recursos para llevar a cabo una investigación exhaustiva. A continuación, se enumeran algunos de los recursos que se utilizaran en este proceso:

a) **Registro de eventos y registros de auditoría:** Los registros de eventos generados por los sistemas, aplicaciones y dispositivos de red contienen información detallada sobre las actividades que tuvieron lugar. Estos registros pueden proporcionar pistas sobre la causa y el impacto del incidente, y ayudar en la identificación de patrones o comportamientos anómalos.
b) **Herramientas de monitoreo de seguridad:** Estas herramientas recopilan datos sobre el tráfico de red, eventos de seguridad y comportamiento del sistema en tiempo real. Aquí se encuentran soluciones Firewall.
c) **Herramientas de detección de malware:** Se cuenta con herramienta de antivirus para identificar, analizar, detectar el código malicioso en busca de características y comportamientos sospechosos.
d) **Fuentes de inteligencia de amenazas**: Se cuenta con inscripción a foros, boletines y comunidades de intercambio de información de seguridad.
e) **Equipo de expertos en seguridad:** La entidad cuenta con un equipo de gestión de incidentes de seguridad de la información que dará respuesta dependiendo el impacto del incidente identificado.
f) **Políticas y procedimientos de respuesta a incidentes:** Se cuenta con procedimiento de gestión de incidentes de seguridad de la información que proporcionan una guía estructurada sobre cómo responder y analizar los incidentes de seguridad. En ellos se establecen los pasos a seguir, las responsabilidades y los flujos de trabajo para garantizar una respuesta efectiva.

5.7.5 Recursos para el análisis de incidentes

a) Es definido por la entidad un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque cibernético, entre los cuales se encuentran:

- Puerto 80 (HTTP): Es el puerto utilizado para comunicaciones web estándar. Los ataques de inyección de código, como los ataques XSS (Cross-Site Scripting), a menudo se dirigen a aplicaciones web a través de este puerto.
- Puerto 443 (HTTPS): Es el puerto utilizado para comunicaciones seguras a través de HTTPS. Los ciberdelincuentes pueden realizar ataques de phishing o intentar explotar vulnerabilidades en conexiones seguras.
- Puerto 22 (SSH): Es el puerto utilizado para el protocolo de acceso seguro de Shell (SSH). Los atacantes pueden intentar realizar ataques de fuerza bruta para obtener acceso no autorizado a servidores y dispositivos a través de este puerto.
- Puerto 3389 (RDP): Es el puerto utilizado para el Protocolo de Escritorio Remoto (RDP) de Microsoft. Los atacantes pueden intentar acceder a escritorios remotos de forma no autorizada o realizar ataques de fuerza bruta para obtener acceso a sistemas a través de este puerto.
- Puerto 445 (SMB): Es el puerto utilizado para el Protocolo de Bloque de Mensajes del Servidor (SMB) de Microsoft. Los ciberdelincuentes pueden buscar vulnerabilidades en este puerto para realizar ataques de Ransomware, como el conocido ataque WannaCry.
- Puerto 23 (Telnet): Es el puerto utilizado para el protocolo Telnet, que proporciona acceso remoto a un sistema. Los atacantes pueden buscar sistemas con servicios de Telnet habilitados para intentar obtener acceso no autorizado.

Estos son solo algunos ejemplos de los puertos más utilizados en ataques cibernéticos. Es importante tener en cuenta que los ciberdelincuentes están en constante evolución y pueden adaptarse para utilizar diferentes puertos o métodos en sus ataques.

b) La entidad cuenta con un diagrama de red para tener la ubicación rápida de los recursos existentes
c) La entidad cuenta con una línea base de Información de: Servidores (Nombre, IP, Aplicaciones, entre otros aspectos importantes).
d) La entidad realiza un análisis del comportamiento de red en la cual se incluyen puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

5.7.6 Recursos para la mitigación y remediación

En este punto se consideran los elementos básicos para la contención de un posible incidente, Backup de la base de datos del sistema de información de forma diaria a las 12:10 con retención de las tres últimas copias de seguridad y con replica en sitio alterno; De igual forma se generar imagen del servidor de forma diaria a las 10:00 pm con retención de las tres últimas copias de seguridad.

5.8 DETECCIÓN, ANALISIS Y EVALUACIÓN

5.8.1 Detección

a) Identificación y Gestión de Elementos Indicadores de un Incidente

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido y se define n los siguientes:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Fallas en el sistema de información
- Reportes de usuarios
- Software antivirus dando informes
- Otros funcionamientos fuera de lo normal del sistema

La identificación y gestión de elementos que alertan sobre un incidente nos proveen información que puede alertarnos sobre la futura ocurrencia de este y preparar procedimientos para minimizar su impacto. Algunos de estos elementos son:

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad

5.8.2 Análisis

Las actividades de análisis del incidente involucran una serie de componentes, y se tiene en cuenta lo siguiente:

- Se cuenta con conocimientos de las características normales a nivel de red y de los sistemas.
- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.
- Toda información que permita realizar análisis al incidente está en los Logs de servidores, equipos de comunicaciones y aplicaciones.
- Se cuenta con Sincronización de Relojes ya que esto facilita la correlación de eventos y el análisis de información.

5.8.3 Evaluación

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad, se realiza la siguiente clasificación:

Impacto	Descripción	Valoración
MUY GRAVE	Si el evento genera impacto en la disponibilidad, integridad y/ o confidencialidad de la información impidiendo desarrollar la labor de misional con apoyo tecnológico por más de 4 horas	Alto
GRAVE	Si el evento genera impacto en la disponibilidad, integridad y confidencialidad de la información impidiendo desarrollar la labor misional con apoyo tecnológico por hasta 2 horas	

MODERADA	Si el evento genera impacto en la disponibilidad, integridad y confidencialidad de la información impidiendo desarrollar la labor misional con apoyo tecnológico por más de 1 hora	Medio
LEVE	El evento negativo se soluciona rápidamente y no genera suspensión de la labor misional con apoyo tecnológico	Baja
MUY LEVE	El evento negativo no tiene consecuencias para la labor misional con apoyo tecnológico	

5.8.4 Clasificación de incidentes de seguridad de la información

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por

a) **Acceso no autorizado:** Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
b) **Modificación de recursos no autorizado:** Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.
c) **Uso inapropiado de recursos:** Un incidente que involucra a una persona que viola alguna política de uso de recursos.
d) **No disponibilidad de los recursos:** Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.
e) **Daño o pérdida de información:** Se produce cuando la información almacenada en sistemas o dispositivos es dañada, eliminada o alterada, lo que puede resultar en la pérdida de datos valiosos o confidenciales.
f) **Fuga y/o robo de información:** Ocurre cuando la información sensible o confidencial se divulga o se obtiene de forma no autorizada, pudiendo ser utilizada para fines maliciosos o ilegales.
g) **Robo de credenciales o información mediante Phishing:** Los atacantes engañan a los usuarios mediante la creación de sitios web o correos electrónicos falsos que imitan a entidades legítimas para obtener sus credenciales (nombres de usuario, contraseñas) u otra información confidencial.
h) **Comportamiento anormal del computador y/o sistema de información:** Se refiere a situaciones en las que un sistema o computadora presenta un funcionamiento inusual, como lentitud, bloqueos frecuentes o actividad sospechosa, lo que puede indicar la presencia de un malware o una intrusión.
i) **Suplantación de identidad:** Implica hacerse pasar por otra persona o entidad para engañar a los usuarios y obtener acceso a información confidencial o realizar actividades fraudulentas.
j) **Pérdida o alteración de registros de base de datos:** Se produce cuando los registros almacenados en una base de datos son eliminados o modificados de manera no autorizada, lo que puede comprometer la integridad de la información y afectar la operatividad del sistema.
k) **Pérdida de un activo de información:** Se refiere a la situación en la que se pierde un activo valioso de información, como un dispositivo de almacenamiento, un equipo o una copia de seguridad, lo que puede llevar a la pérdida de datos y a la exposición de información sensible.
l) **Código malicioso "malware, Ransomware":** Se trata de programas o software diseñados para infiltrarse en sistemas y dispositivos con el fin de dañar, robar información o bloquear el acceso a los archivos y exigir un rescate (en el caso del Ransomware) para su liberación.
m) **Denegación del servicio:** Consiste en inundar un sistema o red con una cantidad abrumadora de tráfico o solicitudes maliciosas, lo que provoca la interrupción o la degradación significativa del servicio, impidiendo que los usuarios legítimos accedan o utilicen los recursos correctamente.
n) **Multicomponente:** Un incidente que involucra más de una categoría anteriormente mencionada.

o) **Otros:** Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías

TABLA DE URGENCIA	
Urgencia	**Descripción**
Alto	El incidente de seguridad digital debe atenderse de forma inmediata y menor a 4 horas, contadas a partir del reporte al CSIRT de Gobierno.
Medio	El incidente de seguridad digital debe atenderse de forma inmediata de (0 – 12) contadas a partir del reporte al CSIRT de Gobierno.
Bajo	El incidente de seguridad digital debe atenderse de forma inmediata de (0 – 48) contadas a partir del reporte al CSIRT de Gobierno.

5.8.5 Declaración y notificación del incidente

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad. La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

A continuación, se describe el proceso de notificación de incidentes de seguridad que será adoptado por la entidad:

a) Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad debe notificarlo por medio del canal implementado por la entidad.
b) Se identificará el tipo de incidente de acuerdo con la tabla de clasificación de incidentes.
c) Se analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI.
d) En caso de ser catalogado como un incidente de seguridad se notificarán a la persona encargada de la atención de incidentes o a quien haga sus veces para que tome las decisiones correspondientes.
e) El profesional de seguridad de la información será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo.
f) Se notificará al primer punto de contacto sobre la presentación de un incidente de seguridad para que realice la documentación respectiva y esté atento al seguimiento y desarrollo de este. El punto de contacto clave dentro.
g) La persona encargada de la atención de incidentes tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad y es la persona que notificará a las altas directivas de la entidad.

5.9 CONTENCIÓN, ERRADICACION Y RECUPERACIÓN

La entidad implementó una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase se descompone claramente en tres componentes

a) **Contención:** Esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad posee una estrategia de contención previamente definida para poder tomar decisiones, de la siguiente forma:

INCIDENTE	ESTRATEGIA DE CONTENCIÓN
Acceso no autorizado	Bloquear o revocar las credenciales comprometidas. Identificar y desconectar al atacante, en caso de no poder aislar la máquina. Fortalecer la seguridad con autenticación multifactor y controles de acceso adecuados. Registrar y analizar el evento para prevenir futuros intentos de acceso no autorizado.
Modificación de recursos no autorizado	Restaurar los recursos afectados a un estado seguro y conocido. Analizar y corregir la vulnerabilidad que permitió la modificación no autorizada. Implementar sistemas de detección de cambios no autorizados para una respuesta temprana ante futuros intentos.
Uso inapropiado de recursos	Identificar al responsable del uso inadecuado y aplicar sanciones adecuadas. Implementar herramientas de monitoreo para detectar actividades inusuales. Reforzar la capacitación en políticas y procedimientos de uso aceptable de recursos.
No disponibilidad de los recursos	Identificar y solucionar la causa de la indisponibilidad. Redirigir el tráfico o la carga a recursos alternativos si es posible. Implementar medidas de redundancia y tolerancia a fallos para garantizar la continuidad del servicio.
A Daño o pérdida de información	Restaurar la información desde copias de seguridad fiables. Identificar la causa del daño o pérdida y fortalecer las medidas de protección de datos. Capacitar a los usuarios para prevenir errores que puedan provocar pérdidas de información.
Fuga y/o robo de información	Detener la filtración o el acceso no autorizado. Notificar a las autoridades pertinentes y a las partes afectadas según las regulaciones y políticas de notificación aplicables. Reforzar la seguridad y monitorear la propagación de información sensible.
Robo de credenciales o información mediante Phishing	Alertar a los usuarios sobre la amenaza y proporcionar instrucciones para proteger sus credenciales. Monitorear el uso indebido de las credenciales comprometidas y bloquear o revocar accesos sospechosos. Reforzar la educación en seguridad y concienciación sobre el phishing.
Comportamiento anormal del computador y/o sistema de información	Aislar la máquina o el sistema afectado para evitar una propagación mayor. Analizar y eliminar el malware o comportamientos maliciosos. Reforzar las medidas de seguridad con actualizaciones y parches para prevenir futuros ataques.
Suplantación de identidad	Notificar a los usuarios afectados y a las autoridades correspondientes. Reforzar la autenticación y verificar la identidad de los usuarios en los sistemas críticos. Monitorear y bloquear actividades sospechosas que puedan indicar suplantación.
Pérdida o alteración de registros de base de datos	Restaurar los registros afectados desde copias de seguridad confiables. Implementar controles de acceso y auditorías más rigurosos para prevenir futuras pérdidas o alteraciones. Identificar y corregir las vulnerabilidades que permitieron el incidente.
Pérdida de un activo de información	Realizar un análisis forense para determinar la causa y el alcance de la pérdida. Notificar a las partes afectadas y a las autoridades competentes según las regulaciones aplicables. Fortalecer las medidas de seguridad, como encriptar datos sensibles, implementar copias de seguridad y mejorar el control de acceso a los activos de información.
Código malicioso "malware, Ransomware"	Aislar la máquina, realizar un análisis de malware para identificar el tipo y la extensión del código malicioso. Limpiar y eliminar el malware de los sistemas afectados. Restaurar los datos desde copias de seguridad confiables. Mejorar la seguridad con soluciones antivirus actualizadas, sistemas de detección de intrusiones y concienciación sobre la seguridad cibernética.
Denegación del servicio	Identificar y mitigar el ataque de denegación de servicio (DDoS) mediante la implementación de soluciones de mitigación de DDoS y el análisis del tráfico para identificar patrones y fuentes de ataques. Restaurar el servicio afectado y mejorar la infraestructura de red para resistir futuros ataques de denegación de servicio.
Multicomponente	Evaluar los diferentes componentes afectados y aplicar medidas correctivas específicas para cada uno de ellos. Esto puede incluir la aplicación de parches de seguridad, la actualización de software, la revisión de configuraciones de red y sistemas, y la implementación de medidas de seguridad adicionales según corresponda a cada componente afectado.
Otros	Para incidentes no especificados, es importante evaluar cada caso individualmente y determinar las estrategias de contención adecuadas según la naturaleza y el impacto del incidente. Esto puede incluir acciones como el aislamiento de los sistemas afectados, la recuperación de datos desde copias de seguridad, el análisis forense para identificar la causa raíz, y la implementación de medidas correctivas y preventivas específicas para evitar futuros incidentes similares.

b) **Erradicación y recuperación:** Luego de que el incidente ha sido contenido se realiza una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el líder de

infraestructura o el líder de sistemas de información debe restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

INCIDENTE	ESTRATEGIA DE ERRADICACIÓN	ESTRATEGIA DE RECUPERACIÓN
Acceso no autorizado	- Implementar autenticación de múltiples factores (por ejemplo, contraseña y verificación de SMS)	- Revocar de inmediato los accesos no autorizados y restablecer las credenciales de usuario comprometidas
	- Establecer permisos y roles de usuario adecuados y revisar periódicamente los privilegios de acceso	- Realizar una revisión exhaustiva de los sistemas y registros para identificar cualquier actividad sospechosa
Modificación de recursos no autorizado	- Aplicar controles de integridad y firmas digitales para detectar modificaciones no autorizadas en los recursos	- Restaurar los recursos afectados a partir de copias de seguridad verificadas
	- Utilizar sistemas de detección de intrusos para alertar sobre cambios inesperados en los archivos o recursos	- Realizar análisis de malware para asegurarse de que no hay archivos maliciosos presentes
Uso inapropiado de recursos	- Establecer políticas y directrices claras sobre el uso aceptable de los recursos y comunicarlas a los usuarios	- Identificar y educar a los usuarios que han incurrido en uso inapropiado de los recursos
	- Implementar sistemas de monitoreo para identificar actividades inapropiadas y tomar acciones correctivas	- Implementar medidas de monitoreo continuo para detectar y prevenir futuros casos de uso inapropiado
No disponibilidad de los recursos	- Implementar redundancia y balanceo de carga para garantizar la disponibilidad de los recursos	- Restaurar los servicios afectados utilizando sistemas de respaldo y recuperación
	- Establecer mecanismos de respaldo y recuperación de datos para restaurar los servicios en caso de interrupción	- Realizar análisis de causa raíz para identificar y abordar las causas de la interrupción
Daño o pérdida de información	- Realizar copias de seguridad periódicas de los datos y almacenarlas de forma segura	- Restaurar los datos perdidos o dañados a partir de copias de seguridad verificadas
	- Implementar medidas de protección contra malware y realizar análisis regulares para detectar posibles amenazas	- Realizar análisis forense para determinar la causa y el alcance de la pérdida o daño de la información
Fuga y/o robo de información	- Implementar políticas de clasificación de datos y acceso restringido a información sensible	- Notificar a las partes afectadas y cumplir con los requisitos legales y regulatorios
	- Utilizar cifrado para proteger datos confidenciales y controlar los puntos de salida de datos	- Realizar un análisis exhaustivo para determinar cómo se produjo la fuga o robo de información
Robo de credenciales o información mediante Phishing	- Brindar capacitación en concientización sobre seguridad a los usuarios para que puedan identificar ataques de phishing	- Restablecer las credenciales comprometidas y notificar a los usuarios afectados
	- Implementar filtros de correo electrónico y navegación web para bloquear sitios de phishing conocidos	- Realizar una revisión de los sistemas y registros para detectar posibles brechas de seguridad relacionadas
Comportamiento anormal del computador y/o sistema de información	- Utilizar herramientas de monitoreo de red y sistemas de detección de anomalías para identificar comportamientos sospechosos	- Analizar y remediar cualquier compromiso o infección detectada
	- Mantener actualizados los sistemas operativos y aplicaciones con los últimos parches y actualizaciones de seguridad	- Realizar auditorías de seguridad regulares para identificar posibles vulnerabilidades y prevenir futuros incidentes
Suplantación de identidad	- Implementar autenticación robusta, como autenticación biométrica o autenticación de dos factores	- Realizar una revisión exhaustiva de los sistemas y registros para identificar cualquier actividad sospechosa
	- Establecer políticas de contraseñas fuertes y cambiarlas regularmente	- Restablecer las credenciales comprometidas y notificar a los usuarios afectados
Pérdida o alteración de registros de base de datos	- Realizar copias de seguridad regulares y almacenarlas de forma segura	- Restaurar los registros afectados a partir de copias de seguridad verificadas
	- Utilizar sistemas de monitoreo y registros de auditoría para detectar cambios no autorizados en la base de datos	- Realizar una revisión exhaustiva de los sistemas y registros para identificar cualquier actividad sospechosa
Pérdida de un activo de información	- Realizar un inventario de activos de información y establecer medidas de seguridad física y lógica	- Realizar un análisis de impacto para determinar las consecuencias y la criticidad de la pérdida
	- Implementar sistemas de rastreo y localización de dispositivos para facilitar la recuperación en caso de pérdida	- Realizar acciones de mitigación y recuperación según la criticidad del activo perdido
Código malicioso "malware, Ransomware"	- Utilizar software antivirus y antimalware actualizados para detectar y eliminar posibles amenazas	- Realizar un análisis forense para determinar la causa y el alcance del código malicioso
	- Establecer políticas de seguridad que prohíban la descarga e instalación de software no autorizado	- Restaurar los sistemas afectados a partir de copias de seguridad verificadas
Denegación del servicio	- Utilizar sistemas de protección contra ataques de denegación de servicio (DDoS)	- Restaurar los servicios afectados utilizando sistemas de respaldo y recuperación
	- Establecer límites de tráfico y filtrado de paquetes para prevenir y mitigar ataques DDoS	- Realizar análisis de causa raíz para identificar y abordar las causas de la interrupción
Multicomponente	- Implementar una estrategia de seguridad en capas, que incluya firewall, sistemas de detección de intrusos, cifrado, etc.	- Realizar pruebas de penetración y auditorías de seguridad regulares para identificar posibles vulnerabilidades y prevenir ataques

INCIDENTE	ESTRATEGIA DE ERRADICACIÓN	ESTRATEGIA DE RECUPERACIÓN
	- Establecer procedimientos de respuesta a incidentes claros y definidos para abordar rápidamente cualquier incidente de seguridad	

En algunas ocasiones durante el proceso de Atención de Incidentes de Seguridad de la información específicamente en la fase de "Contención, Erradicación y Recuperación" se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.

5.10 ACTIVIDADES POST-INCIDENTES

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

5.10.1 Lecciones aprendidas

Una de las partes más importantes de un plan de respuesta a incidentes de TI es la de aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones aprendidas. Mantener un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los incidentes menores, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes.

Mantener un adecuado registro de lecciones aprendidas permite conocer:

a) Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
b) Los procedimientos documentados.
c) Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
d) Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
e) Acciones correctivas pueden prevenir incidentes similares en el futuro.
f) Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

5.11 ROLES Y PERFILES NECESARIOS PARA LA ATENCION A INCIDENTES

A continuación, presentaremos una descripción de los actores que intervienen y conforman el proceso de atención de Incidentes, para cada actor se presentará una breve descripción sobre su perfil y la función dentro del proceso de respuesta a Incidentes de Seguridad de la información.

a) **Usuario Sensibilizado:** Es un empleado, empleados de firmas contratista o terceros con acceso a la infraestructura de la entidad, quien debe estar educado y concientizado sobre las guías implementadas sobre la seguridad de la información y en particular la guía de atención de incidentes, estos usuarios serán muchas veces quienes reporten los problemas
b) **Profesional especializado en seguridad Informática:** Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes también debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención de incidentes. Cuenta adicionalmente con capacitación en

Seguridad de la Información (con un componente tecnológico fuerte) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes.

c) **Líder de sistemas de información:** Se define como la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el profesional de seguridad informática sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al profesional de seguridad Informática sobre el incidente la solución del mismo.

d) **Líder de infraestructura**: Personas encargadas de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo. También debe ser notificado por el Profesional especializado en seguridad Informática sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al Profesional especializado en seguridad Informática sobre el incidente y la solución del mismo.

e) **Coordinador de TI:** Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos. El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI).

6 REFERENCIAS

-, M. d.-M. (2022). *Gestión de Incidentes de seguridad de la información*. Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

7 CONTROL DE MODIFICACIONES

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	03-10-2023	Emisión inicial del documento	Ingeniero de seguridad y privacidad de la información – Proceso de gestión de TI
2	07-02-2025	Cambio en la imagen institucional	Oficina de calidad