ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

FORMATO DE APROBACIÓN DOCUMENTAL

CÓDIGO: DESI-FM-008 | **VERSIÓN: 11**

FECHA DE APLICACIÓN: MAYO 2019

INFORMACIÓN DOCUMENTADA:		CÓDIGO:		VERSIÓN:		JUSTIFICACIÓN:		
TIPO	NOMBRE	ANTERIOR	VIGENTE	ANTERIOR	VIGENTE	ELABORA	ACTUALIZA	ANULA
Formato	Bitácora de Incidentes de Seguridad de la Información	-	EGTI-FM-006	-	1	X		
Procedimiento	Gestión de incidentes de Seguridad	-	EGTI-PR-005		1	X		
Documento Interno	Política de Gestión de Incidentes de Seguridad de la Información	-	EGTI-DI-014	-	1	X		

DESCRIPCIÓN DE LA JUSTIFICACIÓN:

Se adopta el procedimiento EGTI-PR-005 Gestión de incidentes de Seguridad y el formato EGTI-FM-006 Bitácora de incidentes de seguridad para definir las actividades y los pasos a seguir para la atención de los incidentes de seguridad de la información que pueden presentarse, afectar la plataforma y los sistemas de información de la UAERMV.

Se implementa la política –EGTI-DI-014 Gestión de incidentes de seguridad para establecer el proceder para la atención de los incidentes y su utilización como lecciones aprendidas para evitar su ocurrencia.

AVALA: **LÍDER DE PROCESO** *(Puede ser el Líder Estratégico o Líder Operativo dependiendo del proceso)*	**ELABORA/ACTUALIZA/ANULA:** *(Colaborador del proceso en compañía del enlace)*	**ACOMPAÑAMIENTO:** **ASESOR OAP** *(Colaborador de la Oficina Asesora de Planeación a cargo de procesos)*
(Firma)	*(Firma)*	*(Firma)*
Nombre: Marcela Rocío Márquez Arenas	*Nombre: Gloria Méndez/ Jeison Medina/ Yuly González*	*Nombre: Andrea del Pilar Zambrano Barrios/ Christian Medina Fandiño*
Cargo: Secretaría General	*Cargo: Contratistas Secretaría General -Proceso EGTI*	*Cargo: Contratistas Proceso DESI*

TRÁMITE DE APROBACIÓN DOCUMENTAL (DILIGENCIADO POR LA OFICINA ASESORA DE PLANEACIÓN)	**¿ES APROBADO?** SI ☐ NO ☐	**FECHA DE APROBACIÓN:** 15-10-2019	**RESPONSABLE DEL SISTEMA DE GESTIÓN DE CALIDAD**
	OBSERVACIONES:		*(Firma)* Martha Patricia Aguiar Copete ***REPRESENTANTE DE LA ALTA DIRECCIÓN***

ÍTEM	FECHA DE REGISTRO	USUARIO / OBJETO AFECTADO	UNIDAD	ÁREA / PROCESO	CATEGORÍA

FORMATO BITÁCORA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

DESCRIPCIÓN DE LA INCIDENCIA	INICIO DE LA INCIDENCIA	FIN DE LA INCIDENCIA	DURACIÓN	CLASIFICACIÓN	CAUSA

IMPACTO	SOLUCIÓN	SERVICIOS AFECTADOS	REGISTRADO POR	TICKET	NOMBRE DE EQUIPO

ALCALDÍA MAYOR DE BOGOTÁ D.C. MOVILIDAD Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial	PROCESO ESTRATÉGICO	Código:	EGTI-PR-005	SIG UNIDAD DE MANTENIMIENTO VIAL
	PROCESO ESTRATEGIA Y GOBIERNO DE TI	Versión:	1	
	PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Fecha:	OCTUBRE DE 2019	

1. OBJETIVO

Establecer las actividades a realizar para la identificación, el reporte y la atención de los incidentes de seguridad de la información que puedan presentarse en la Unidad Administrativa Especial de Rehabilitación y Mantenimiento vial, gestionando la aplicación de actividades post-incidentes que permitan generar lecciones aprendidas, con el fin de evitar la ocurrencia de incidentes de similares características.

2. ALCANCE

El alcance del presente procedimiento es aplicable a cualquier tipo de incidente que afecte a la seguridad de la información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. Inicia con la detección del incidente y finaliza con la implementación de las actividades post-incidente propuestas para evitar la ocurrencia de un nuevo incidente de características semejantes.

3. DEFINICIONES

Amenaza: Cualquier situación o evento que tiene el potencial de hacer daño a los recursos de información de la Corporación.

Incidente: Cualquier comportamiento fuera de lo normal o error (voluntario o involuntario), que pueda afectar o disminuir la calidad de los servicios ofrecidos por el área de Sistemas, sus proyectos y procedimientos.

Monitoreo: Actividades de revisión para determinar el grado de cumplimiento de las políticas de seguridad de la información.

Recurso de información: Elemento tecnológico que contiene información de la Corporación. Ejemplo de un recurso de información lo constituye una aplicación, una carpeta compartida de red, una base de datos, un dispositivo móvil, etc.

4. DESCRIPCIÓN DE LOS SIMBOLOS

SÍMBOLO	SIGNIFICADO	SÍMBOLO	SIGNIFICADO	SÍMBOLO	SIGNIFICADO
	Inicio y fin.		Conector página.		Conector de actividades
	Operación: desarrollo de actividad o tarea.		Decisión: toma de decisión		Punto de control: se debe describir el control. Son medidas de seguridad o Prevenciones para ejecutar la actividad de acuerdo con las normas o requisitos establecidos

DESCRIPCIÓN (ACTIVIDAD Y/O TAREA)	PUNTO CONTROL	TIEMPO ESTIMADO	RESPONSABLE	DEPENDENCIA INVOLUCRADA	REGISTRO	OBSERVACIONES
INICIO						
1. Comunicar el posible incidente por medio de un ticket al área de Mesa de Ayuda.		Inmediatamente ocurra	Usuario	Todas la áreas UAERMV	Reporte incidente Mesa de ayuda	La alerta puede provenir de un usuario, de un tercero o de la revisión de cumplimiento de Seguridad de la información, se debe alertar cualquier situación sospechosa o extraña. Se debe dirigir a la política y validar los ejemplos de incidente
2. Crear un ticket de Incidente en el Sistema de Mesa de Ayuda		1-2 horas	Integrante Mesa de Ayuda	Sistemas de Información y Tecnología Secretaría General	Ticket de Incidente Mesa de Ayuda	El ticket debe clasificarse dentro de los temas de Internet y Seguridad.
3. Notificar la existencia del incidente al Especialista de Seguridad de la Información		1-2 horas	Integrante Mesa de Ayuda	Sistemas de Información y Tecnología Secretaría General	Ticket de Incidente Mesa de Ayuda	
A						

DESCRIPCIÓN (ACTIVIDAD Y/O TAREA)	PUNTO CONTROL	TIEMPO ESTIMADO	RESPONSABLE	DEPENDENCIA INVOLUCRADA	REGISTRO	OBSERVACIONES
A 4. Evaluar el incidente (impacto) y notificar al área responsable del incidente		1 a 2 días	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Notificación Área Responsable de incidente	Si el incidente afecta a un área o proceso critico, se envía correo y se hace reunión notificando del incidente a los lideres de proceso involucrados y se incluye en el informe de seguridad que se debe realizar prioritariamente.
5. Establecer si es necesario realizar bloqueo de servicios		Depende el impacto, de ser posible inmediatamente	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Informe del Incidente de Seguridad	Correo formal informando al Jefe del usuario el porqué del bloqueo el equipo.
¿Es necesario bloquear los servicios? NO SI			Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General		De ser necesario, en caso de que el incidente se expanda por toda la red o el impacto sea la total indisponibilidad de los servicios, se bloquean los servicios y sistemas que se encuentran en riesgo, producto del incidente, para neutralizar la amenaza.
6. Realizar el bloqueo del equipo(S)		1-2 Horas	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Correo formal al Jefe Inmediato para bloquear el equipo	Correo al Jefe inmediato
7. Realizar las actividades de contención del incidente.		1-2 Horas	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General		Las actividades de contención del incidente son las siguientes: bloqueo de los servicios y/o la desconexión de los equipos comprometidos.
8. Efectuar las actividades de solución del incidente responsable		1-3 días	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Las actividades se deben registrar en la bitácora	Inicialmente se realizaran actividades para ofrecer soluciones de servicio para los afectados, de acuerdo con la vulnerabilidad de los servicios afectados. Dentro de las actividades iniciales está: Detección y registro del incidente, la clasificación y soporte inicial, Investigación y diagnóstico, el escalamiento, la solución y restablecimiento del servicio, el cierre del incidente y el monitoreo, seguimiento y comunicación del incidente.
9. Investigar las causas que originaron el incidente responsable		2 días	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	EGTI-FM-006 Bitácora de Incidentes de Seguridad	Se debe realizar la actividad desde el comienzo del incidente
10. Obtener las evidencias de la ocurrencia del incidente del		2 días	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	EGTI-FM-006 Bitácora de Incidentes de Seguridad Informe del incidente	Las evidencias se obtienen tomando cadena de custodia del equipo o equipos involucrados, realizando la respectiva gestión forense, sacando copia a los equipos de tal manera que la información no sea alterada y con herramientas especializadas que permitan ayudar a dar claridad al incidente
11. Registrar el Incidente B		Inmediato	Especialista Seguridad de la Información o Contratista Designado	Sistemas de Información y Tecnología Secretaría General	EGTI-FM-006 Bitácora de Incidentes de Seguridad	La conservación de registro de incidentes va en la bitácora y en las herramientas destinadas para tal fin

DESCRIPCIÓN (ACTIVIDAD Y/O TAREA)	PUNTO CONTROL	TIEMPO ESTIMADO	RESPONSABLE	DEPENDENCIA INVOLUCRADA	REGISTRO	OBSERVACIONES
B 12. Formular el Informe del incidente de seguridad		1 semana	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Informe del Incidente de Seguridad	En caso de ser un incidente grave o que contenga datos personales, formular el informe de incidente y enviar al Líder de Tecnología, como al Líder de Infraestructura.
13. Informar a los involucrados		1 día	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Informe del Incidente de Seguridad	Informa a los involucrados, según lo definido en la política de sanciones por parte de Control Interno Disciplinario.
¿EL incidente compromete datos personales? NO SI			Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General		De ser necesario, en caso de que el incidente se expanda por toda la red o el impacto sea la total indisponibilidad de los servicios, se bloquea los servicios y sistemas que se encuentran en riesgo producto del incidente para neutralizar la amenaza.
14. Informar al titular de datos personales sobre el incidente y su solución		1 día	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Informe del Incidente de Seguridad	Se debe enviar el informe el incidente al titular de Datos Personales o la persona que posee la afectación por la pérdida de la información.
15. Comunicar al titular de datos personales sobre el incidente y su solución		1 día	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Informe del Incidente de Seguridad EGTI-FM-006 Bitácora de Incidentes de Seguridad	Se debe informar al titular de los datos personales los siguientes datos: a) Naturaleza del incidente b) Datos personales comprometidos c) Recomendaciones d) Medidas correctivas implementadas.
16. Cerrar el incidente		1 día	Especialista Seguridad de la Información o personal designado	Sistemas de Información y Tecnología Secretaría General	Informe del Incidente de Seguridad	Se realiza el cierre del incidente, enviando un informe, donde se encuentre lo relacionado con lecciones aprendidas, cierre del caso y registro en la bitácora de incidente.
FIN						

REVISÍON Y APROBACIÓN

Elaborado y/o Actualizado por	Validado por Líderes (Estratégico u Operativo) del Proceso:	Aprobado:
JEISON MEDINA VALDEZ /GLORIA MENDEZ Contratistas / Proceso SIT		
Acompañamiento Asesor OAP: ANDREA DEL PILAR ZAMBRANO/ CRISTIAN MEDINA Contratistas/ Proceso DESI	Firma: MARCELA ROCIO MARQUEZ ARENAS Secretaría General	Firma: MARTHA PATRICIA AGUILAR COPETE Representante de la Alta Dirección

Participó en la Elaboración del Procedimiento

Nombre	Cargo	Firma
JEISON MEDINA VALDEZ	CONTRATISTA	
YULY ANDREA GONZÁLEZ RODRPIGUEZ	CONTRATISTA	
CARLOS ABEL BASTIDAS CUBILLOS	CONTRATISTA	

CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA	APROBADO Representante de la Alta Dirección
1	Se adopta el procedimiento presentado para la atención de los incidentes de seguridad de la información que pueden presentarse, afectar la plataforma y los sistemas de información de la UAERMV.	Octubre de 2019	Jefe Oficina Asesora de Planeación

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Bogotá, D.C.,
(OCTUBRE DE 2019)

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Este documento ofrece los lineamientos básicos para iniciar el plan de ejecución del Sistema de Gestión de Incidentes de Seguridad de la información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial-UAERMV, a través de un modelo propuesto, el cual está concebido para integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

2. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

2.1 OBJETIVO

El objetivo principal de la política de gestión de incidentes de seguridad de la información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial es contar con un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

Los objetivos de esta política son:

- Definir roles y responsabilidades dentro de la entidad, como eje puntual para evaluar los riesgos y que se permita mantener la operación, la continuidad y la disponibilidad del servicio.
- Gestionar los eventos de seguridad de la información desde su detección, con el fin de identificar si se requiere clasificarlos como incidentes de seguridad de la información.
- Minimizar los impactos adversos de los incidentes en la entidad y sus operaciones, mediante la utilización de las salvaguardas establecidas en esta política.
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para evitar la repetición de estos eventos. Con lo anterior, se reduce la ocurrencia de futuros incidentes, mejora la implementación y el uso de las salvaguardas y mejora el esquema global de la gestión de incidentes de seguridad de la información.
- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes basada en la bitácora de incidentes, según el procedimiento de gestión de incidentes de seguridad de la información.
- Definir los lineamientos para el procedimiento formal de reporte y escalamiento de los incidentes de seguridad de la información.

3. GLOSARIO

- **ACUERDO DE CONFIDENCIALIDAD:** Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

- **ANÁLISIS DE BRECHA (GAP):** El GAP Análisis es un estudio preliminar que permite conocer la manera en la que se desempeña una empresa en materia de seguridad de la información, con relación a las mejores prácticas reconocidas en la industria, para esto se utilizan criterios establecidos en normas o estándares. El análisis establece las diferencias entre el desempeño actual y el deseado. Este análisis se puede aplicar a cualquier estándar certificable, lo normal es que se lleve a cabo para nuevos esquemas de certificación.

- **COPIA DE SEGURIDAD (BACKUP):** En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.

- **CSIRT (en inglés Computer Security Incident Response Team):** Equipo de Respuesta a Incidentes de Seguridad Informática.

- **ENCARGADO DE SEGURIDAD:** Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información a la UAERMV y supervisar el cumplimiento de la presente Política.

- **EVENTO**: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2013].

- **FIREWALL:** Dispositivo tecnológico que tiene como función proteger la red interna de una compañía, de accesos no autorizados del interior y del exterior vía Internet.

- **FORTIANALYZER:** Sistema de análisis de eventos de seguridad.

- **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.

- **INCIDENTE:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. **[ISO/IEC 27000:2013].**

- **ISO 27001:** ISO 27001 es una norma emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

- **LAN:** Local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.

- **LOTE (BATCH):** Archivo magnético que tiene almacenada una secuencia de comandos. Al ejecutarse, reemplaza la operación de digitar los comandos de secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.

- **MIPG:** Modelo Integrado de Planeación y Gestión.

- **MSPI:** Modelo de Seguridad y Privacidad de la Información.

- **NOC:** Centro operativo de red.

- **OTI:** Oficina de Tecnología e Informática.

- **PHVA:** Ciclo de mejora continua, Planear, Hacer, Verificar y Actuar.

- **PRIVACIDAD DE LA INFORMACIÓN:** Derecho que tienen todos los titulares de la información, en relación con la información que involucre datos personales y la información clasificada que éstos hayan entregado o esté en poder de la entidad, en el marco de las funciones que a ella le compete realizar y que generan en las entidades, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.[1]

- **SEGURIDAD DE LA INFORMACIÓN:** Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.

- **SEGURIDAD INFORMÁTICA:** Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar la materialización de las amenazas que se propagan por la red.

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.

- **SOC:** Los Centros de Operaciones de Seguridad se encargan de realizar un seguimiento y analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.

- **SPAM:** Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

[1] 1 Modelo de Seguridad y Privacidad de la Información.

- **SEGURIDAD DE LA INFORMACIÓN:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

- **TIC:** Tecnologías de la información y comunicaciones.

- **UAERMV:** Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

- **USB:** El Universal Serial Bus (USB) (bus universal en serie BUS) es un estándar industrial desarrollado en los años 1990 que define los cables, conectores y protocolos usados en un bus para conectar, comunicar y proveer de alimentación eléctrica entre ordenadores y periféricos y dispositivos electrónicos.

- **USUARIO:** Este concepto cobija a todos los clientes internos, servidores públicos y contratistas que utilicen la red de la entidad.

- **VPN:** Una red privada virtual -RPV- o VPN (de acuerdo con las siglas en inglés de Virtual Private Network), es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

- **WAN:** Wide área network o red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales (LAN).

4. METODOLOGÍA

Para lograr los objetivos, la gestión de incidentes de seguridad de la información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial involucra los siguientes procesos de manera cíclica como lo muestra la siguiente imagen:

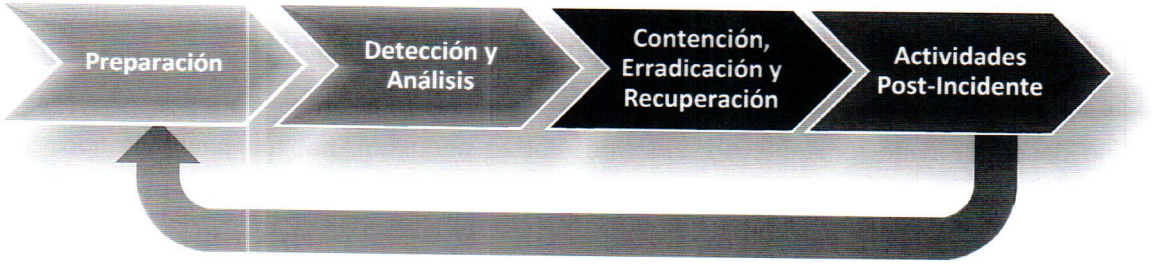

Figura 1 Ciclo de vida para la respuesta a Incidentes de seguridad de la información, según el NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos).

- Planificación y preparación para la gestión del Incidente
- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades Post-Incidente.

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial tiene como responsable en este tema al Especialista de Seguridad de la Información, o según sea el caso, generar un equipo para cumplir las funciones de un CSIRT (Equipo de atención de incidentes de seguridad en cómputo), quien define el procedimiento de atención a incidentes, bitácora de incidentes, atienden el incidente, maneja las relaciones con entes internos y externos, clasifica los incidentes y además de lo anterior, estará a cargo de:

- 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.
- Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- Anuncios de Seguridad: Debe 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).
- Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.

Este especialista debe estar enfocado principalmente, en atender los incidentes de seguridad de la información que se presenten sobre los activos soportados por la plataforma tecnológica de la entidad.

5. POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL (UAERMV)

5.1 DECLARACIÓN Y NOTIFICACIÓN DE INCIDENTES

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 Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. 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, la interrupción de los servicios, el proceso de tratamiento de incidentes y que se manejen correctamente los aspectos disciplinarios y legales que pudieran surgir durante este proceso.

Algunos ejemplos de incidentes:

- Pérdida de información que comprometa la integridad, disponibilidad y confidencialidad.
- Un acceso no autorizado.
- El robo de contraseñas.
- Prácticas de Ingeniería Social.
- La utilización de fallas en los procesos de autenticación para obtener accesos indebidos.
- El robo de información.
- El borrado de información de terceros.
- La alteración de la información de terceros.

5.2 PREPARACIÓN

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial dentro de esta etapa tiene un modelo alineado al Modelo de Seguridad y Privacidad de la Información (MPSI) definido por MinTIC, que permite a la entidad estar en capacidad de responder ante incidentes, y así mismo, velar por que los mismos pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenir la mitigación de estas, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros.

En esta etapa de preparación la cual es apoyada por el líder de tecnología, incluye las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, teniendo en cuenta:

• **Gestión de Parches de Seguridad:** la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial tiene un plan de gestión de vulnerabilidades, aplicados a Sistemas Operativos, Bases de Datos, Aplicaciones, este plan ayudará a los administradores en la identificación, adquisición, prueba e instalación de los parches, y será supervisado por el Especialista de Seguridad de la Información.

• **Aseguramiento de plataforma:** la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, debe ser asegurada correctamente. Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el Login de eventos (autenticación).

• **Seguridad en redes:** la UAERMV realiza el mantenimiento de sus equipos a cargo por medio del especialista de seguridad informática y tiene una gestión proactiva sobre cada elemento de seguridad. Las reglas configuradas en los firewalls (FW) son revisadas semanalmente. Los dispositivos FW y antivirus deben estar actualizados y con su respectiva firma al día. Todos los elementos de seguridad y de red se deben encontrar sincronizados y

sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.

• **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores y equipos de usuario) deben tener activo su antivirus y anti-malware con las firmas de actualización al día.

• **Sensibilización y entrenamiento de usuarios:** Los usuarios de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial incluidos los administradores de TI son sensibilizados una vez al año, acerca de las políticas de seguridad publicadas y existentes, relacionados con la política seguridad de la información, esta sensibilización es realizada por el Especialista de Seguridad de la Información.

5.3 PERSONAL INVOLUCRADO EN LA GESTIÓN DE INCIDENTES

El personal de escalamiento en la gestión de incidentes es el siguiente, de acuerdo a los roles establecidos para la UAERMV:

- Administrador de mesa de ayuda.
- Especialista de seguridad de la información.
- Líder de infraestructura.
- Líder procesos de tecnología.

De requerirse acciones disciplinarias por temas relacionados con el incidente, las áreas encargadas de realizarlas son:

Control Interno Disciplinario.

5.4 HARDWARE Y SOFTWARE

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para una correcta y eficiente gestión de incidentes debe contar con los siguientes elementos:

• Analizadores de protocolos.

• Software para recolección de evidencia.
• Kit de respuesta a incidentes.

• Software de análisis forense.

• Medios de almacenamiento.

5.5 RECURSOS PARA EL ANÁLISIS DE INCIDENTES

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial debe tener en cuenta lo siguiente, al momento de realizar el análisis del incidente:

• Listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.

• Diagrama de red para tener la ubicación rápida de los recursos existentes.

• Una Línea – Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios).

Esta información siempre debe estar actualizada para conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.

• Se debe disponer de un análisis del comportamiento de red estándar, teniendo en cuenta 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.

5.6 DETECCIÓN, EVALUACIÓN Y ANÁLISIS DE INCIDENTES

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, debe detectar, identificar y gestionar los incidentes de la siguiente manera, de acuerdo con los roles asignados en el área de Sistemas de Información y Tecnología:

• **Alertas en sistemas de seguridad FW, Fortianalyzer:** esta actividad es responsabilidad del especialista de seguridad informática.

• **NOC Caídas de enlaces y equipos críticos:** esta actividad es responsabilidad del especialista de redes.
• **Reportes de actividad de usuarios en la red:** esta actividad la hacen en conjunto el especialista de redes y el especialista de seguridad informática.

• **Software antivirus informes de gestión:** esta actividad es responsabilidad del especialista de seguridad informática.

• **Logs de servidores:** Gestionados por el especialista de servidores.

• **Logs de aplicaciones:** Gestionados por el especialista de servidores.

• **Logs de herramientas de seguridad:** Gestionado por el especialista de seguridad informática.

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial debe tener en cuenta dentro del análisis de atención a incidentes, otra serie de componentes, que van alineados con el MPSI de MinTic, como los siguientes:

• Características normales a nivel de red y de los sistemas.

• La información que permite realizar análisis al incidente debe estar centralizada en Logs de servidores, redes y aplicaciones.

• La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial debe contar con un correlacionador de eventos (sistema que almacena los logs y eventos en la red), por medio

de esta herramienta se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.

• Para un correcto análisis de un incidente debe existir una única fuente de tiempo NTP (Sincronización de Relojes), esto facilita la correlación de eventos y el análisis de información.

• Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.

5.7 NIVELES DE IMPACTO

La severidad del incidente puede ser:

• **Alto Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor, que influyen directamente en los objetivos misionales de la entidad. Se incluyen en esta categoría aquellos incidentes que afectan la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

• **Medio Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto moderado, que influyen directamente a los objetivos de un proceso determinado.

• **Bajo Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo.

La clasificación de incidentes de seguridad de la información está dada de la siguiente manera:

• **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.

• **Modificación de recursos no autorizada:** Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.

• **Uso inapropiado de recursos:** Un incidente que involucra a una persona que viola alguna de las políticas de seguridad de la información.

• **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.

• **Multicomponente:** Un incidente que involucra más de una categoría anteriormente mencionada.

• **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.

Priorización de los Incidentes y Tiempos de Respuesta:

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación), se debe determinar el nivel de prioridad de este, y de esta manera atenderlos adecuadamente según la necesidad.

Nivel de Prioridad: Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Nivel criticidad	Valor	Definición
Inferior	0.10	Sistemas no críticos, como estaciones de trabajo de usuario con funciones no críticas.
Bajo	0.25	Sistemas que apoyan a una sola dependencia o proceso de la UAERMV.
Medio	0.50	Sistemas que apoyan más de una dependencia o proceso de la UAERMV.
Alto	0.75	Sistemas pertenecientes a el área de tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1.00	Sistemas o procesos críticos.

Tabla 1: Niveles de criticidad de impacto

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Nivel criticidad	Valor	Definición
Inferior	0.10	Impacto leve en uno de los componentes de los sistemas de información o estaciones de trabajo.
Bajo	0.25	Impacto bajo en uno de los componentes de los sistemas de información o estaciones de trabajo.
Medio	0.50	Impacto moderado en uno de los componentes de los sistemas de información o estaciones de trabajo.
Alto	0.75	Impacto alto en uno de los componentes de los sistemas de información o estaciones de trabajo.
Superior	1.00	Impacto Superior en uno de los componentes de los sistemas de información o estaciones de trabajo.

Tabla 2: niveles de impacto actual o futuro

Luego de tener definidas las variables, se obtiene la prioridad mediante la siguiente fórmula:
Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)
Y los resultados obtenidos se deben comparar con la siguiente tabla para determinar la prioridad de atención:

Nivel Prioridad	Valor
Inferior	00 – 2.49
Bajo	2.50 – 3.74
Medio	3.75 – 4.99
Alto	5.00 – 7.49
Superior	7.50 – 10

Tabla 3: Nivel de prioridad del incidente

Tiempos de Respuesta, para el caso de la atención de incidentes de seguridad se han establecido unos tiempos máximos de atención de estos, teniendo en cuenta su criticidad e impacto.

Los tiempos expresados en la siguiente tabla son los definidos por la Unidad y hacen referencia al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Nivel Prioridad	Tiempo de respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 min
Alto	15 min
Superior	5 min

Tabla 4: Tiempos máximos de atención incidentes

6. INFORME DEL INCIDENTE

Una vez atendido y solucionado el incidente, se debe estructurar el informe de la siguiente manera:

- Resumen ejecutivo: ¿Qué ha pasado? De forma clara y concisa, sin terminología técnica.
- Línea de tiempo (Timeline) del incidente: Que ha sucedido paso a paso, según bitácora de incidentes.
- Datos del entorno.
- Gestión del incidente: Qué acciones se han tomado para responder al incidente.
- Análisis forense: Si se han realizado análisis forenses, resultados de los mismos (puede ir también como anexo en función de su extensión).
- Análisis de malware: Si se han realizado análisis de malware, resultados de los mismos (puede ir también como anexo en función de su extensión).
- Impacto del incidente: Determinamos (o estimamos) el impacto del incidente (datos perdidos, equipos afectados, daños causados, etc...)
- Atribución: Se debe indicar (en la medida de lo posible) quién ha podido ser el causante del incidente.
- Recomendaciones de seguridad: Qué medidas debemos tomar para que este incidente no se vuelva a repetir.
- Lecciones aprendidas: Qué se ha hecho bien, qué se ha hecho mal y qué acciones se deben tomar para hacerlo mejor en el próximo incidente.
- Anexo: Evidencias (todo aquello que por su extensión no tiene cabida en la gestión del incidente).

Teniendo en cuenta lo anterior existen tipos de informe que deben estar contemplados dentro del diligenciamiento de la bitácora y la gestión del incidente:

- Informe de detección: Se ha detectado y confirmado un incidente de seguridad. En este informe (dirigido a los responsables técnicos) se cuenta en 2 a 3 párrafos lo que se sabe hasta el momento del incidente, estimando sistemas afectados e impacto. El objetivo es iniciar la respuesta ante el incidente, dando prioridad a la rapidez sobre la exactitud.
- Informes "de batalla": Son actualizaciones del informe de detección, resumiendo las acciones tomadas por el equipo de respuesta ante incidentes. A medida que se va avanzando en la respuesta, estos informes tendrían que incrementar su exactitud (vamos sabiendo con más detalle lo sucedido).

- Informes de crisis: El objetivo es el mismo que los informes de batalla, pero la audiencia pasa a ser personal no técnico (dirección y/o legal). Prima la claridad del mensaje, y se debe de tener cuidado con lo que se dice (debe ser exacta la información)

Informes de IOC (Indicators of Compromise): Son informes destinados a compartir inteligencias con otros departamentos o entidades. En muchos casos están anonimizados (sin información del origen), y constan de 1 a2 párrafos introductorios y de un listado de IOC (Indicadores de Compromiso) para que sean comprobados por los receptores.

REVISIÓN Y APROBACIÓN:

Elaborado y/o Actualizado por	Validado por Líderes (Estratégico u Operativo) del Proceso:	Aprobado por:
JEISON MEDINA VALDEZ / GLORIA MENDEZ Contratistas / Proceso EGTI	Firma:	Firma:
Acompañamiento Asesor OAP:		
ANDREA DEL PILAR ZAMBRANO/ CHRISTIAN MEDINA Contratista/ Proceso DESI	MARCELA ROCIO MARQUEZ ARENAS (Secretaría General)	MARTHA PATRICIA AGUILAR COPETE Representante de la Alta Dirección

CONTROL DE CAMBIOS:

VERSIÓN	DESCRIPCIÓN	FECHA	APROBADO Representante de la Alta Dirección
1	Se implementa la política Gestión de incidentes de seguridad para establecer el proceder para la atención de los incidentes y su utilización como lecciones aprendidas para evitar su ocurrencia.	OCTUBRE 2019	Jefe Oficina Asesora de Planeación