1 OBJETIVO

Establecer un procedimiento formal para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad de la información, con el fin de minimizar el impacto sobre los activos de información y operaciones de la entidad y cumplir con las normativas y requerimientos legales vigentes.

2 ALCANCE

El presente procedimiento es aplicable a todos los activos de información de la entidad y los procesos responsables de los mismos.

Asimismo, se aplica a incidentes de seguridad digital de diversa índole, tales como:

- Ataques cibernéticos (phishing, malware, ransomware, etc.).
- Accesos no autorizados o violaciones de la seguridad.
- Pérdida o exposición accidental de datos.
- Fallos o vulnerabilidades en sistemas y aplicaciones que puedan comprometer la confidencialidad, integridad o disponibilidad de la información.

3 RESPONSABLE

El (la) responsable de garantizar el cumplimiento y del monitoreo de este procedimiento, es el Subsecretario de Sistemas de Información y será responsabilidad de los líderes de proceso y de todos los funcionarios y terceros que tengan a su cargo activos de información, reportar los incidentes relacionados con seguridad de la información.

4. MARCO LEGAL

▪ Ley 594 de 2000.Por medio de la cual se expide la Ley General de Archivos.

▪ Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

▪ Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

▪Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones -TIC-Se crea la agencia Nacional de espectro y se dictan otras disposiciones.

▪ Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

▪ Ley 1474 de 2011.Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

▪ Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales

▪ Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

▪ Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

▪ Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

▪ Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

▪ Decreto 1078 de 2015.Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

▪ Resolución 1519 de 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

▪ Decreto 767 de 2022, Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Decreto municipal 0496 de 2022, por el cual se deroga el decreto 0714 de 2016 y se adopta la política para el tratamiento de datos personales en el municipio de Pasto.

- Resolución 00500 de marzo de 2021 – MINTIC, Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

5. DEFINICIONES

Amenaza: Cualquier circunstancia o evento potencial que pueda explotar una vulnerabilidad y causar daño a los sistemas, datos o procesos de la organización.

Brecha de seguridad: Violación o incumplimiento de las medidas de seguridad que resulta en el acceso no autorizado a datos o sistemas, exponiendo información sensible a riesgos.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Por disposición del Gobierno Nacional, mediante la Resolución Número 473 de 17 de febrero del 2022, el Mintic adicionó al artículo 1. de la Resolución 002108 del 2020, el Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT, bajo el Viceministerio de Transformación Digital, para continuar articulando y coordinando a nivel nacional los aspectos de ciberseguridad a todos los sectores públicos y privados del país.

Contención: Acciones inmediatas destinadas a limitar la propagación y el impacto del incidente, evitando que se extienda o cause daños adicionales.

Erradicación: Eliminación de la causa raíz del incidente, removiendo componentes maliciosos o comprometidos para prevenir su recurrencia.

Evento de seguridad: Cualquier ocurrencia observable en el entorno de TI que puede tener relevancia para la seguridad, ya sea maliciosa o no, y que debe ser monitoreada para identificar posibles incidentes.

GLPI: Software libre para gestión de mesa de ayuda relacionada con temas de tecnologías, proviene de la sigla de Gestión Libre de Parque Informático.

Incidente de seguridad de la información: Evento o serie de eventos no deseados o inesperados que afectan la confidencialidad, integridad y/o disponibilidad de la información, y que pueden comprometer los activos de la organización.

Lecciones aprendidas: Análisis posterior a la resolución del incidente que permite identificar fortalezas, debilidades y oportunidades de mejora en los procesos y controles de seguridad, para prevenir futuros incidentes.

Notificación de incidentes: Proceso mediante el cual se informa de manera oportuna a las partes internas y, en su caso, a organismos externos o autoridades pertinentes sobre la ocurrencia de un incidente.

Plan de respuesta a incidentes: Conjunto de procedimientos, roles y responsabilidades definidos para detectar, analizar, contener, erradicar y recuperarse de incidentes de seguridad de la información.

Recuperación: Conjunto de medidas y procesos que permiten restaurar los sistemas y servicios a su funcionamiento normal tras un incidente, asegurando que se han mitigado los riesgos asociados.

Registro de incidentes: Documentación detallada de cada incidente, que incluye la fecha, hora, descripción, acciones tomadas, impacto, responsables y lecciones aprendidas, con el objetivo de facilitar el análisis y la mejora continua.

Riesgo: La probabilidad de que una amenaza explote una vulnerabilidad y el impacto que dicho evento tendría sobre la organización. Se evalúa considerando tanto la probabilidad como el impacto potencial.

Vulnerabilidad: Debilidad o falla en los sistemas, procesos o controles de seguridad que puede ser aprovechada por una amenaza para comprometer la seguridad de la información.

6. GENERALIDADES/POLITICAS DE OPERACIÓN

Este procedimiento se realiza bajo las siguientes consideraciones:

Los reportes de incidentes de seguridad de la información se deben realizar al correo electrónico soportesistemas@pasto.gov.co o en caso de afectación al correo institucional de forma telefónica a la Subsecretaría de Sistemas de

Información o directamente con el subsecretario de Sistemas de Información, en todo caso deberá quedar registro inicial del reporte del incidente.

Los reportes de incidentes de seguridad de la información deberán incluir cualquier activo de información identificado en los procesos.

Cuando la afectación sea a un activo de información que no sea digital se podrá involucrar a otras áreas relacionadas con la naturaleza de los activos.

Cuando la afectación del incidente involucre activos de naturaleza digital, se deberá remitir el respectivo reporte a COLCER, cuando se trate de incidentes muy graves o graves se trabajará las tareas de contención y recuperación con el apoyo de este organismo.

Dependiendo de la gravedad del incidente se deberá establecer acciones para prevenir el incidente, así mismo, dependiendo de la gravedad se podrán hacer recomendaciones por parte de la Subsecretaría de Sistemas de Información para ajustar la matriz y plan de acción de riesgos de seguridad de la información, siempre y cuando la dependencia ya cuente con dicho documento.

7. CONTENIDO

TAREA	PUNTO CRITICO DE CONTROL	RESPONSABLE	DOCUMENTO /REGISTRO
1. Detección, reporte y registro del incidente de seguridad de la información	Identificar y registrar de inmediato los incidentes de seguridad de la información detectados o reportados	Funcionarios o terceros Secretaria ejecutiva de la SSI	Registro en software mesa de servicio GLPI
2. Clasificación y Priorización	Evaluar la gravedad, impacto y urgencia del incidente para asignar prioridades de respuesta.	Encargado de gestión de incidentes de SI	Registro en software mesa de servicio GLPI
3. Asignación al personal técnico y colaboración con otras áreas de ser necesario	Dependiendo de tipo de afectación se asigna el personal idóneo para atender el caso, si es requerido se busca apoyo con otras áreas involucradas	Subsecretario de Sistemas de Información	Registro en software mesa de servicio GLPI Oficios

TAREA	PUNTO CRITICO DE CONTROL	RESPONSABLE	DOCUMENTO /REGISTRO
4. Realizar acciones de contención, erradicación y recuperación	En coordinación con la dependencia afectada, el personal asignado y el responsable de gestión de incidentes	Personal técnico asignado al caso	Registro en software mesa de servicio GLPI
5. Reporte de incidentes de nivel menos graves y menores a COLCERT relacionados con activos digitales	Los casos pueden ser de nivel menos graves y menores	Responsable de gestión de incidentes	Portal web COLCERT
6. Reporte de incidentes de nivel muy grave o grave relacionados con activos digitales	Los casos pueden ser de nivel muy grave o grave	Responsable de gestión de incidentes	Formato reporte de incidentes de seguridad de la información COLCERT
7. Establecer compromisos de mejora	Implementar acciones de mejora para prevenir futuros casos	Responsable de gestión de incidentes	Acta mesa de trabajo u oficio

8. CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA

Elaborado por:	Revisado por:	Aprobado por:
EDUARDO ANDRÉS HERNANDEZ ZAMBRANO Contratista	EDWIN FERNANDO GAITA DÍAZ Técnico Administrativo	DARIO FERNANDO ALFARO FIGUEROA Líder proceso de seguridad y privacidad de la información