1. OBJETIVO

Gestionar de forma oportuna los eventos e incidentes de Seguridad de la Información relacionados con la perdida de Confidencialidad, Integridad y Disponibilidad de la información de la entidad.

2. ALCANCE

Aplica para la gestión de todos los Eventos e Incidentes de Seguridad de la Información al interior de la entidad, iniciando desde el reporte hasta el cierre y finalización del incidente.

3. RESPONSABLES

Técnico Administrativo Gobierno Digital	• Desempeña un papel fundamental en la gestión y supervisión de las operaciones de soporte técnico en una organización. Sus responsabilidades varían según el tamaño y la estructura de la organización, pero aquí se presentan algunas funciones clave que suelen desempeñar. • Seguimiento de las tendencias tecnológicas y evaluación de cómo pueden afectar el soporte técnico y la infraestructura de TI de la organización. • Evaluación, selección e implementación de herramientas de gestión de soporte técnico, como sistemas de seguimiento de incidentes o soluciones de mesa de ayuda.
Lideres de Procesos	• Detectar y documentar las necesidades específicas de soporte técnico en sus procesos, ya sea en sistemas, equipos o infraestructuras, asegurando que todos los requerimientos sean conocidos por el equipo de soporte técnico.

4. DEFINICIONES / TERMINOLOGÍA

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 o de tratamiento de la información personal de la entidad.
Niveles de clasificación de la información	Nivel asignado (Confidencial, Privada, Interna o Pública) a la información en función de los requisitos legales, valor de la información, criticidad y susceptibilidad a la divulgación o modificación no autorizada.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o procesos autorizados.
Evento	La ocurrencia detectada en un estado de un sistema de información, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas (controles) o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información.

5. POLÍTICAS DE OPERACIÓN

1. Realizar la gestión de cada incidente contemplando todas las etapas de su ciclo de vida: reporte, asignación, tratamiento, respuesta y cierre.

2. El proceso de gestión de incidentes debe explicitar de manera clara y sin ambigüedades los mecanismos y métodos para realizar los reportes de incidentes de seguridad, así como también la información mínima a proporcionar; manteniendo la confidencialidad de la información suministrada por quien reporte, así como su anonimato.
3. Informar de forma completa e inmediata al responsable de seguridad de la información la existencia de un potencial incidente de seguridad informática.
4. Adoptar medidas de seguridad eficientes para proteger los activos de información.
5. Aprender de los incidentes de seguridad reportados y generar la conciencia necesaria a fin de prevenir nuevas ocurrencias cuando corresponda.

6. DESARROLLO DEL PROCEDIMIENTO

No	ACTIVIDAD (QUE)	DESCRIPCIÓN (COMO)	RESPONSABLE (QUIEN)	REGISTRO / DOCUMENTO
1	Reportar	Todos los funcionarios y terceros deben reportar cualquier evento y/o incidente de seguridad de la información, a través de los siguientes canales: - Correo institucional Línea de Atención telefónica: +57 3208585284, sea cual sea el medio por el cual se reportó el evento y/o incidente de Seguridad de la Información, deben quedar registradas en la herramienta de gestión.	Líderes de Procesos	PA-GCOM-FO-01 Oficios / Comunicaciones Correo Institucional
2	Categorizar y Registrar	La Entidad recibe el reporte del evento y/o incidente de seguridad de la Información, lo identifica, registra, clasifica y escala inmediatamente al Especialista de Seguridad Informática.	Líderes de Procesos	PA-GCOM-FO-01 Oficios / Comunicaciones Correo Institucional
3	Recolectar Información	El Técnico Administrativo Gobierno Digital debe realizar la evaluación inicial que involucra el análisis de la información descrita en el reporte e información adjuntada, si existe. Además, de ser necesario, debe establecer comunicación con el personal involucrado para así recolectar la información necesaria que permita precisar la clasificación del reporte. El reporte puede ser clasificado en: • Evento de seguridad de la información.	Técnico Administrativo Gobierno Digital	PA-GCOM-FO-07 Reporte de Incidentes de Seguridad de la Información Correo Institucional

		• Incidente de seguridad de la información. • Falsa alarma. Son catalogados incidentes de seguridad de la información los que coincidan con las siguientes causas: • Ejecución de Denegación de Servicio. • Hacking. • Ejecución de Pruebas Maliciosas o Escaneos de Red. • Contraseñas comprometidas. • Llaves de cifrado comprometidas. • Suplantación de sitios Web Phishing. • Suplantación de identidad de funcionarios. • Eavesdropping: Escuchar Secretamente y sin autorización llamadas o comunicaciones. • Introducción de código malicioso (Virus, gusanos, troyanos). • Ingeniería social. • Distribución de spam. • Acceso no autorizado a sistemas de información o redes. • Cambio de privilegios sobre sistemas de información sin autorización. • Modificación o inserción de transacciones, archivos o bases de datos sin autorización. • Descarga o envió de contenido inapropiado. • Divulgación no autorizada de información del negocio. • Piratería de software. Robo de información de negocio.		

		• Robo de información personal de clientes y/o funcionarios (ej.: Phishing). • Pérdida o hurto de equipo de cómputo. • Robo de software. • Robo de información de autenticación. • Daño o pérdida de los servicios o enlaces de comunicaciones. • Pérdida de energía. • Daño o pérdida de los equipos del Centro Alterno de Datos. Si el reporte corresponde a una falsa alarma, se debe documentar en el sistema la justificación de la decisión y posteriormente se debe cerrar y notificar a los interesados. Si el evento o incidente de seguridad de la información, atenta contra los sistemas de información o bases de datos que contienen datos personales y es catalogado como crítico entrañando un alto riesgo para los derechos y libertades de los titulares de la información se procederá sin dilación a realizar la actividad # 8 y # 9.		
4	Análisis y evaluación del impacto	El Técnico Administrativo Gobierno Digital de la Información debe determinar: • Valorar el Impacto (Confidencialidad e Integridad). • Valorar la Urgencia (Disponibilidad). Determinar de la Prioridad (Impacto Urgencia). • Afectación. Causas o Tipo de Ataque.	Técnico Administrativo Gobierno Digital	PA-GCOM-FO-07 Reporte de Incidentes de Seguridad de la Información Correo Institucional

		Adicionalmente, el especialista de Seguridad debe planear las actividades enfocadas a contener, controlar y restaurar a la normalidad las operaciones afectadas por el incidente, esto mediante las siguientes tareas, las cuales deben ser documentadas en el sistema, las acciones pueden ser: La criticidad para clasificarla en función de su impacto, y establecer el nivel de prioridad en la resolución de cada incidente de Seguridad de la Información. Se categorizan las incidencias en los siguientes términos: Crítica • Grave • Moderada • Leve Acciones de contención (Si se requieren). Acciones complementarias (Si se requieren).		
5	Aplicar acciones de contención	El Técnico Administrativo Gobierno Digital Informática si aplica, debe identificar las acciones de respuesta inmediata (Contención) con el equipo especialista del sistema de información para tratar el incidente, esto puede dar como resultado controles de Emergencia y/o controles permanentes adicionales. El plan de acción puede contener acciones como: • Activar Contingencias Desconectar Copiar/Clonar • Registrar posibles evidencias • Establecer posibles causas • Notificar a los interesados.	Técnico Administrativo Gobierno Digital Informática	PA-GCOM-FO-07 Reporte de Incidentes de Seguridad de la Información Correo Institucional

		Si la acción de Contención requiere un cambio de Emergencia, se debe activar el proceso de Gestión de Cambios de Emergencia. El Técnico Administrativo Gobierno Digital Informática gestiona la ejecución de las actividades del plan de acción enfocadas en la recuperación de la operación. Dentro de estas actividades pueden estar: • Ejecución de las acciones de restauración implantación de medidas de remediación Pruebas. • Ejecución de plan de retorno Cualquiera que sea el resultado de las acciones realizadas, se debe hacer seguimiento a las acciones por parte del Técnico Administrativo Gobierno Digital de la información verificando la documentación y evidencias registradas. Una vez finalizada las acciones de contención, el oficial de Seguridad determina si el incidente de Seguridad de la Información está bajo control.		
6	Aplicar acciones Complementarias	El Técnico Administrativo Gobierno Digital Informática con el equipo especialista del sistema de información debe identificar si se requieren actividades complementarias para tratar los incidentes de seguridad de la información, esto puede incluir la restauración del Sistema(s), Servicio(s) y/o redes de información a su estado normal. Si las acciones complementarias requieren de un cambio normal, se debe activar el proceso de Gestión de Cambios.	Técnico Administrativo Gobierno Digital	PA-GCOM-FO-07 Reporte de Incidentes de Seguridad de la Información

7	Notificar	El Técnico Administrativo Gobierno Digital Informática, almacena copia de las evidencias recopiladas, y documenta el incidente por medio del sistema que corresponda. La información que debe contener como mínimo es: • Fecha de solicitud • Persona que lo diligencia Ubicación • Descripción del incidente (descripción cronológica de los acontecimientos) Clasificación del incidente de acuerdo al procedimiento (en caso que el evento sí sea incidente) • Posibles Impactos Partes involucradas (especificar especialmente si hay terceros involucrados) • Acciones realizadas (Medidas de contención y de recuperación)	Técnico Administrativo Gobierno Digital	PA-GCOM-FO-01 Oficios / Comunicaciones
8	Reporte en el Registro Nacional de Base de Datos RNBD	En la plataforma tecnológica de la Superintendencia de Industria y Comercio reportar el incidente de seguridad dentro los (15) días hábiles siguientes al registro del incidente o evento de seguridad	Técnico Administrativo Gobierno Digital	Soporte Digital
9	Comunicación a los afectados	Una vez identificado el incidente de seguridad y cumplidas con las actividades descritas en el presente procedimiento, la Oficina de Seguridad de la Información comunicará al interesado en un lenguaje claro y sencillo la violación de seguridad, las medidas correctivas adoptadas por la organización y las recomendaciones de seguridad que deberán seguir los interesados.	Técnico Administrativo Gobierno Digital	PE-SIG-SGC-FO-13 Informe de Seguimiento

10	Documentar Lecciones Aprendidas	El Técnico Administrativo Gobierno Digital con el equipo que atendiendo el incidente es responsable de identificar las lecciones aprendidas con el objeto de evitar la reincidencia de los hechos y la eliminación de las debilidades aprovechadas por la amenaza que causó el incidente de seguridad. Así mismo, el Técnico Administrativo Gobierno Digital de la Información es responsable de identificar si aplica, controles nuevos o modificaciones a los existentes.	Técnico Administrativo Gobierno Digital	PE-SIG-SGC-FO-13 Informe de Seguimiento
11	Cerrar el incidente	Técnico Administrativo Gobierno Digital informa a la entidad para el cierre del incidente en la herramienta de gestión e informa a las personas interesadas.	Técnico Administrativo Gobierno Digital	PE-SIG-SGC-FO-13 Informe de Seguimiento

PUNTO DE CONTROL

5. Aplicar acciones de contención. PV-CI-MC-FO-06 Seguimiento Plan de Mejoramiento.

7. DOCUMENTOS DE REFERENCIA

Ley 1273 de 2009. Protección de la información y de los datos
Ley 1581 de 2012. Protección de datos personales
Decreto 1078 de 2015. Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones
Decreto 1008 de 2018. Lineamientos generales de la Política de Gobierno Digital
Plan de Seguridad y Privacidad de la Información de la Entidad, versión vigente
NTC-ISO 9001:2015. Sistema de gestión de la calidad – Requisitos
Capítulo 8.5.1. Control de la producción y de la provisión del servicio
Capítulo 8.7. Control de las salidas no conformes
Capítulo 10.2. No conformidad y acción correctiva

8. ANEXOS

PA-GCOM-PL-01 Plan de Seguridad y Privacidad de la Información
PA-GCOM-FO-01 Oficios / Comunicaciones
PA-GCOM-FO-07 Reporte de Incidentes de Seguridad de la Información
PE-SIG-SGC-FO-11 Informe de Gestión
PE-SIG-SGC-FO-13 Informe de Seguimiento
Correo Institucional
Soporte Digital

ELABORÓ	NATURALEZA DEL CAMBIO	VERSIÓN	FECHA DE APROBACIÓN

Deysi Carolina Rodríguez Molano	Procedimiento inicial	01	14/03/2023
Andrew Masami Asakura Garcia	Cambio de logo, actualización de contenido y responsables de elaboración, revisión y aprobación	02	10/01/2024
Andrew Masami Asakura Garcia	Inclusión del Logo ICONTEC / MIPG y ajuste de Pie de Página / Ajuste de contenido	03	26/08/2024
Andrew Masami Asakura Garcia	Actualización del Correo Corporativo	04	01/04/2025

ELABORÓ	REVISÓ	APROBÓ
Nombre: Andrew Masami Asakura Garcia	Nombre: Julián Alfonso Amaya Reyes	Nombre: Yeison Rokney Torres Suarez
Cargo: Profesional SIG	Cargo: Técnico Administrativo Gobierno Digital	Cargo: Gerente General
Firma:	Firma:	Firma: