Objetivo:

Identificar, investigar y tratar desviaciones a las Políticas de Seguridad y Privacidad de la Información y a la de tratamiento de datos personales, para evitar recurrencias de incidentes en el uso de la información a través del análisis de causas y consecuencias en el ciclo de vida del incidente.

Alcance:

Trata cualquier desviación/incidente a las Políticas de Seguridad y Privacidad de la Información y a la de tratamiento de datos personales, cubriendo el ciclo de vida del incidente en el uso de la información, que va desde su detección hasta su cierre, pasando por las etapas de asignación, contención, investigación, junto con la respectiva documentación y evidencias generadas en el ciclo.

Términos y definiciones:

1. **BASE DE DATOS:** Conjunto organizado de datos personales que sea objeto de tratamiento por parte de la EAAB-ESP.
2. **CICLO DE VIDA DE UN INCIDENTE:** El curso normal de etapas que lleva a que un evento que viole las Políticas de Seguridad y Privacidad de la información y Tratamiento de datos personales sea identificado, contenido, investigado, resuelto y cerrado.
3. **CONTENER INCIDENTE:** Suspender e Impedir que siga afectando la desviación.
4. **DATO PERSONAL:** Información vinculada o que pueda asociarse a una o varias personas naturales, determinadas o determinables.
5. **EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Cualquier suceso observable que denota una situación de riesgo o amenaza que puede afectar la información en su integridad, o confidencialidad o disponibilidad.
6. **GRUPO DE SEGURIDAD DE LA INFORMACIÓN GSI :** Personas que proveen un conjunto de Servicios que presta informática, que incluye: Mesa de ayuda, SOC, Grupo de Control de vulnerabilidades, Administradores de Infraestructura informática, Grupo de Seguridad de la Información – GSI; responsables por el diseño, desarrollo, implantación y verificación de las Políticas de Seguridad y Privacidad, y la de Tratamiento de Datos Personales, y que hacen parte de la "Segunda Línea de Defensa" según MIPG.
7. **HERRAMIENTA GRC**: Software licenciado por la EAAB, en donde se gestionan los elementos de Gobierno, Riesgo y Cumplimiento que impactan la operación de la Empresa.
8. **INCIDENTE DE SEGURIDAD:** Eventos de violación de la Política de Seguridad y Privacidad de la información o de Tratamiento de Datos Personales, como la pérdida, robo y/o acceso no autorizado o indebido a los datos personales -DP- que son objeto de tratamiento
9. **INCIDENTE DE SEGURIDAD NO CLASIFICADO:** Incidentes que no involucren la identificación de activos de información expresamente clasificados y que no develen la presencia de vulnerabilidades cuya revelación pongan en riesgo la postura de seguridad de la información de la Empresa.
10. **LINEAS DE DEFENSA:** Modelo de responsabilidades en la protección de la información según el MIPG. Ver Manual Operativo Sistema de Gestión Versión 2 de agosto 2018 Página 88 www.funcionpublica.gov.co

    PRIMERA LÍNEA: Líderes y responsables de proceso, Facilitadores SIG y Colaboradores de la Empresa.
    SEGUNDA LÍNEA: Dirección Gestión de Calidad y Procesos y Líderes de los sistemas de gestión.
    TERCERA LÍNEA: Oficina de control interno.
11. **MESA DE AYUDA:** Centro de Servicio de la Dirección Servicios de Informática- 7777.
12. **RESPONSABLE O DETERMINADOR DE INFORMACIÓN:** Es el funcionario de nivel directivo de la EAAB ESP que en razón de su cargo o función es responsable del proceso que origina o custodia la información y por ende de su protección.
13. **USUARIO DE LA INFORMACIÓN:** Persona natural o jurídica que usa la información de la EAAB-ESP.

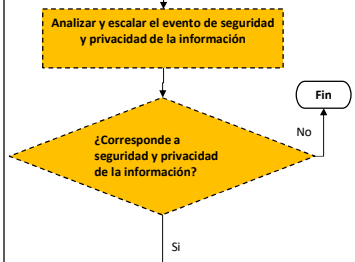
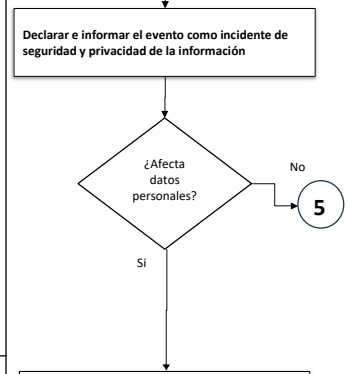
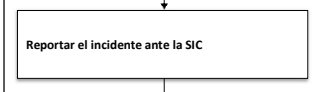
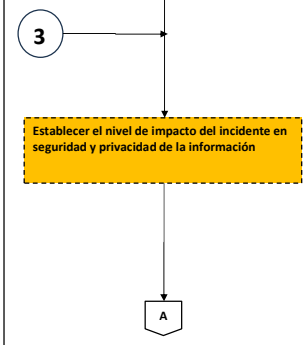
Políticas de Operación:

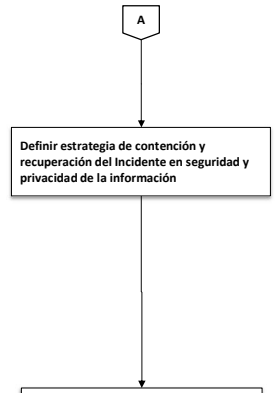
1. El Responsable o Determinador de la información afectada -"primera línea de defensa", es el encargado de gestionar los incidentes de Seguridad o de Privacidad de su información durante el ciclo de vida.
2. El responsable o Determinador de la información afectada "primera línea de defensa" es el encargado de la gestión de los riesgos que pueden afectar su información por medio de la aplicación de controles preventivos en los planes de mejora que traten los riesgos a niveles aceptables.
3. Cada Usuario de la Información en la Empresa debe acatar las condiciones de uso de la información, reportar los eventos que identifique, relacionados con seguridad y privacidad de la información física o electrónica al Responsable o Determinador de la información y a la mesa de ayuda/ Dirección Servicios de Informática línea 7777.
4. Cada Usuario de la Información en la Empresa debe participar en la contención del incidente que está afectando la información que tiene a su cargo, y debe estar pendiente durante el ciclo completo del incidente hasta su cierre.
5. Si el evento afecta documentos físicos, o las instalaciones locativas de la Empresa, o personas, se debe reportar a la Dirección de Seguridad -Vigilancia, responsable por la atención de ésta clase de incidentes.
6. Cada incidente de seguridad de la información debe tener un identificador único durante su ciclo de vida.
7. Un incidente de seguridad de la información permanece en estado "no cerrado" hasta tanto no se cumpla con su notificación, correcta contención, investigación, documentación, y sea aprobado por el GSI.
8. Los incidentes en seguridad de la información que no sean notificados a la mesa de ayuda no serán reconocidos como tal.
9. Los eventos reportados se registran como posibles incidentes que han afectado la información, o su acceso, o su privacidad, durante su gestión se podrá concluir, si son realmente incidentes de seguridad o privacidad. Se debe mantener registro de la gestión y el escalamiento
10. El GSI tiene la responsabilidad de clasificar y registrar los eventos reportados como incidentes, de asignarlo y de controlar su gestión hasta su cierre final; solicitando a las partes involucradas un reporte de la gestión realizada.
11. Los incidentes clasificados con impacto "alto", el grupo asignado debe trabajar de manera inmediata en la contención, restablecimiento del servicio y en la investigación, cuidando siempre la integridad y confidencialidad de la información recolectada con sus evidencias.
12. Los incidentes de seguridad que involucren expedientes se deben atender ateniéndose a lo dispuesto por la normatividad del Archivo General de la Nación
13. En los casos diferentes a los de expedientes, la reconstrucción de la información debe ser analizada en función de los beneficios o de la necesidad de la información para el funcionamiento de la empresa, teniendo en cuenta una relación costo/beneficio para la empresa.
14. Si el incidente de seguridad afecta datos personales debe ser reportado en el módulo del Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio habilitado para tal efecto, dentro de los 15 días a partir del momento en que se identifique el incidente.
15. Los incidentes de seguridad digital identificados y catalogados como Muy Grave y Grave que no sean tipificados como clasificados se reportan al CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital), para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno.
    Los incidentes catalogados como Menos Grave y Menor que no sean clasificados, deben ser comunicados al CSIRT Gobierno en el formulario establecido por el CSIRT una vez sean gestionados, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

Documentos de soporte

CÓDIGO	NOMBRE	Actividades	ENTIDAD
MPFT0204I01	Valoración y definición del nivel de Impacto de los Incidentes en Seguridad de la Información	5	EAAB
MPFT0204I02	Incidentes de seguridad de la información asociados a datos personales	3, 4	EAAB
MPFT0219P	Investigación y Análisis Forense	5	EAAB
MPFA0605P	Investigaciones por pérdidas o daño de activos y/o elementos	2	EAAB
MPEE0301P	Administración de riesgos y oportunidades	3, 11	EAAB
MPEE0301F05	Reporte de eventos de riesgos	3	EAAB
MPEE0502P	Mejoramiento continuo	11	EAAB
MPEE0502F02	Plan de mejoramiento	11	EAAB

Actividades

#	Nombre de la actividad	Descripción	Registro	Responsable
1		Identifica y reporta a la mesa de ayuda los eventos de seguridad o privacidad de la información que son una posible desviación a las Políticas de Seguridad y Privacidad de la Información (física o digital) o de Tratamiento de Datos Personales, acorde con la Políticas Operacional 1 y 8.	Número de reporte	Colaboradores de la EAAB
2		Una vez el Coordinador de Seguridad de la Información tiene reportado el caso, examina el evento para determinar si corresponde a una violación a las Políticas de Seguridad y Privacidad de la Información o Datos personales o si involucra instalaciones físicas de la Empresa, o personas. Cuando el evento incluya personas o instalaciones físicas, traslada el caso mediante correo electrónico al Determinador de la información con copia a la Dirección de Seguridad / Vigilancia quien tiene competencia para su atención e investigación según el procedimiento MPFA0605P "Investigaciones por pérdidas o daño de activos y/o elementos" (Política Operacional 5) y finaliza este procedimiento. En caso de ser de seguridad y privacidad de la información, continua con la actividad No. 3	Correo de notificación al Determinador copia opcional a Vigilancia	Profesional Especializado Nivel 20 Gerencia de Tecnología Dirección Servicios de Informática (Coordinador de Seguridad de la Información)
3		En caso que el evento sea un incidente en seguridad y/o privacidad de la información, el Coordinador de Seguridad de la información le comunica al responsable /determinador de la información afectada que se declara como incidente de seguridad y privacidad de la información (Políticas Operacional 1 y 3) y reporta mediante correo electrónico la materialización del riesgo en el formato de "Reporte de eventos de riesgos" - MPEE0301F05 a la Dirección de Gestión de Calidad y Procesos, de acuerdo con el procedimiento MPEE0301P de "Administración de riesgos y oportunidades" A su vez, registra en la herramienta GRC (Archer) el evento reconocido como incidente de seguridad de la información, asignando un identificador (Política Operacional 6). Si el incidente de seguridad de la información afectó datos personales que están siendo tratados por la EAAB-ESP, se debe informar del caso a la Dirección de Servicios de Informática en su rol de Oficial de Protección de Datos Personales mediante correo electrónico, de acuerdo con el instructivo MPFT0204I02 Incidentes de seguridad de la información asociados a datos personales	Correo de notificación al Determinador Registro en la herramienta GRC del seguimiento del incidente. Correo de notificación a Oficial de Datos Personales	Profesional Especializado Nivel 20 Gerencia de Tecnología Dirección Servicios de Informática (Coordinador de Seguridad de la Información)
4		Si el incidente de seguridad afecta datos personales el Director de Servicios de Informática en su rol de Oficial de Protección de Datos Personales reporta en el módulo del Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio habilitado para tal efecto, dentro de los 15 días siguientes, contados a partir del momento en que se identifique el incidente con base en la información registrada en la herramienta GRC (Archer) conforme a los lineamientos o el instructivo MPFT0204I02 Incidentes de seguridad de la información asociados a datos personales.	Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio	Director Nivel 8 Gerencia de Tecnología Dirección Servicios de Informática (Oficial de Protección de Datos Personales)
5		El Coordinador de Seguridad de la Información analiza el incidente, lo clasifica y establece su impacto siguiendo el instructivo MPFT0204I01 "Valoración y definición del nivel de Impacto de los Incidentes en Seguridad de la Información", con el fin de determinar el nivel de impacto y afectaciones del incidente y, si se requiere inicia el procedimiento MPFT0219P de Investigación y Análisis forense Se registran en Archer los resultados del análisis con sus soportes, la valoración del impacto, y asigna el responsable de la gestión del incidente. Una vez identificado el incidente de seguridad de la información y no es clasificado se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno. Los incidentes catalogados por el responsable de seguridad de la información como Menos Grave y Menor y no son clasificados, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos, acorde con la Política de Operación Número 15.	Registro del Incidente en la herramienta GRC de Acueducto (Archer) actualizado con el nivel de impacto, responsable asignado para la gestión y soportes. Notificación de correo de asignación de responsable para la gestión del incidente Reporte o comunicación al CSIRT Gobierno (si aplica)	Profesional Especializado Nivel 20 Gerencia de Tecnología Dirección Servicios de Informática (Coordinador de Seguridad de la Información)

#	Nombre de la actividad	Descripción	Registro	Responsable
6		Según el nivel de impacto del incidente, se definen las estrategias de contención y recuperación del incidente a implementar, para lo cual, se recomienda tener en cuenta: i. Daño potencial de activos de información por causa del evento o incidente teniendo en cuenta la criticidad del activo. ii. Datos personales afectados. iii. Infraestructura crítica afectada. iv. Preservación de la evidencia. v. Tiempo y recursos internos y externos necesarios para la estrategia. vi. Efectividad de la estrategia. vii. Duración estimada de las medidas a tomar. viii. Características de las posibles fuentes de ataque. ix. Activación del Procedimiento de recuperación de desastres (si existe) x. Tiempo (Hábil y no hábil) para llevar a cabo la solución. xi. Recurso humano necesario para implementar la solución. Este recurso está tanto a nivel técnico como operativo. xii. Implicaciones reputacionales, económicas y legales. xiii. Definir y notificar a responsables para llevar a cabo la estrategia de solución.	Registro en la herramienta GRC de Acueducto (Archer) con las acciones definidas para la contención y recuperación	Profesional nivel 22-21-20 Gerencia de Tecnología Dirección Servicios de Informática (Responsable asignado para la gestión del incidente)
7		El responsable asignado para la gestión del incidente aplica las medidas para detener el incidente acorde con su impacto, evita que siga afectando la información y los elementos involucrados; y toma evidencias de la plataforma afectada, en coordinación con la Dirección de Seguridad; actualizando la información del incidente con las acciones de contención implementadas, sus resultados, las evidencias y las lecciones aprendidas de acuerdo con la herramienta definida para tal fin (Política Operacional 4).	Registro en la herramienta GRC de Acueducto (Archer) de las acciones de contención.	Profesional nivel 22-21-20 Gerencia de Tecnología Dirección Servicios de Informática (Responsable asignado para la gestión del incidente)
8		El responsable asignado para la gestión del incidente recupera los servicios afectados por el incidente y los pone en operación; actualizando la información del incidente con las acciones de recuperación, el reinicio de los servicios afectados y las lecciones aprendidas; considerando las política de operación 12 y 13 en la herramienta definida para tal fin.	Registro en la herramienta GRC de Acueducto (Archer) de las acciones de recuperación y el reinicio de los servicios.	Profesional nivel 22-21-20 Gerencia de Tecnología Dirección Servicios de Informática (Responsable asignado para la gestión del incidente)
9		Analiza las causas del incidente de seguridad y privacidad de la información determinadas inicialmente, en el que se incluye la elaboración de hipótesis de las causas, la investigación, la documentación de los resultados y lecciones aprendidas para la gestión de los riesgos materializados y la prevención de la repetición del incidente y realice los ajustes correspondientes (si aplica). En el caso de afectación de datos personales continua con la actividad No. 10, de lo contrario sigue a la actividad No. 11	Registro en la herramienta GRC de Acueducto (Archer) de las investigaciones realizadas con sus resultados y evidencias.	Profesional nivel 22-21-20 Gerencia de Tecnología Dirección Servicios de Informática (Responsable asignado para la gestión del incidente)
10		El responsable/ determinador de la información de la base de datos asociada al incidente, comunicará a los Titulares de la Información que hayan sido afectados con el fin de brindarles la oportunidad para que puedan adoptar las medidas necesarias para protegerse de las consecuencias de este evento. Si el incidente afectó completamente los datos personales de la base de datos se publicará un aviso en la página web de la entidad. Si afectó datos personales de manera parcial se comunicará a los afectados respectivos mediante correo electrónico.	Aviso en la página web Comunicación por correo electrónico	Director Nivel 8 Jefe de Oficina Gerente Corporativo (Responsable/Determinador de la Información)
11		Con base en las lecciones aprendidas en la contención, recuperación de los servicios y de las investigaciones realizadas, el responsable de la información en conjunto con el Coordinador de Seguridad de la Información formula los planes de mejora para los riesgos materializados con el incidente, con el fin de prevenir y evitar su recurrencia; acorde con la política de operación 2. El coordinador de seguridad de la información actualiza la información del incidente con sus respectivas evidencias en la herramienta de Archer. La gestión de los planes de mejora se realizan de acuerdo con el procedimiento MPEE0502P de "Mejoramiento continuo" Los riesgos materializados se deben actualizar con respecto a la probabilidad de ocurrencia, por efecto de su materialización de acuerdo con el procedimiento MPEE0301P "Administración de riesgos y oportunidades"	MPEE0502F02 "Plan de mejoramiento" .Registro en la herramienta GRC de Acueducto (Archer) de los riesgos actualizados con los planes de mejoramiento.	Director Nivel 8 Jefe de Oficina Gerente Corporativo (Responsable/Determinador de la Información) Profesional Especializado Nivel 20 Gerencia de Tecnología Dirección Servicios de Informática (Coordinador de Seguridad de la Información)
12		Cierra el incidente, verificando las acciones previas y en especial la capitalización de las lecciones aprendidas en su ciclo de vida.	Registro de cierre del incidente en la herramienta GRC de Acueducto (Archer)	Profesional Especializado Nivel 20 Gerencia de Tecnología Dirección Servicios de Informática (Coordinador de Seguridad de la Información)

Control de cambios

FECHA	DESCRIPCIÓN Y JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
11/01/2024	Se realizó ajuste en el objetivo, alcance, políticas de operación, y actividades de acuerdo con el nuevo formato de procedimiento. Se incluyeron nuevas actividades asociadas a datos personales y se vincularon los instructivos para valoración del impacto de incidentes de seguridad y de incidentes de seguridad de la información asociados a datos personales. Se ajusta el código del procedimiento MPCS0202P Mejoramiento continuo y su respectivo formato al código MPEE0502P, por la migración al mapa versión 6	3
12/12/2019	Se realizan ajustes al documento	2

Control de revisión y aprobación

Elaboración	Revisión	Aprobación
IVAN ERNESTO GUERRA MATIZ Dirección Servicios de Informática Gerencia de Tecnología ALVARO PINZON MORALES Profesional Especializado Nivel 20 Dirección Servicios de Informática Gerencia de Tecnología	HEYDI ELENA ESPITIA SALAS Profesional Especializado Nivel 22 Dirección Servicios de Informática Gerencia de Tecnología	ADRIANA DEL PILAR GUERRA MARTINEZ Directora Dirección Servicios de Informática Gerencia de Tecnología
10/10/2023	10/10/2023	11/01/2024