CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	30/06/2021	N.A

OBJETIVO

Establecer un procedimiento que permita identificar, atender, gestionar y dar respuesta de forma oportuna a los incidentes de seguridad de la información o informática, teniendo en cuenta la normativa vigente y los estándares en seguridad definidos, con el fin de mitigar el impacto asociado a la perdida de confidencialidad, integridad y disponibilidad de la información del DADEP.

ALCANCE

Inicia con el registro de un caso en el sistema de gestión de servicios TIC. Continúa con el análisis y clasificación del caso y si se trata de un incidente de seguridad informática o de la información, luego de esto se procede a buscar la solución y finaliza con la respuesta al usuario que registró el caso y el cierre del mismo en la herramienta de gestión de servicios TIC.

DEFINICIONES Y SIGLAS

Activo: componente que tiene valor para la entidad, bienes, derechos, información y otros recursos con los que se dispone.
Clasificación: hace referencia al grado de severidad de un incidente de Seguridad de la Información.
Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
Evento de seguridad de la información: 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.
Gestor de incidentes de seguridad de la información: Corresponde al profesional de la Oficina de Sistemas, encargado de realizar el análisis, evaluación y documentación de los incidentes de seguridad de la información reportados en la entidad.
Herramienta de gestión: Corresponde a la herramienta donde se registra y documenta la información correspondiente a un incidente de seguridad de la información.
Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
Información: se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia entidad o de fuentes externas) o de la fecha de elaboración.
Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.
Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
Seguridad informática: Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.
Solicitud padre: se determina como solicitud padre, cuando un incidente puede generar varios casos sobre la misma incidencia. Está determinado por la actividad que afecte, critica o no critica, y el porcentaje de usuarios afectados.
Caso: Número consecutivo suministrado por una herramienta de gestión durante el reporte de una solicitud de servicio, para facilitar a través del mismo el seguimiento y control.

POLÍTICAS DE OPERACIÓN Y ASPECTOS GENERALES

Identificación de un incidente de seguridad de la información.
*Es todo evento o serie de eventos que tienen probabilidad significativa comprometer la operación interna y/o los servicios sociales, amenazando la triada de la información, por ejemplo: no tener acceso a la información utilizada en el desarrollo de las actividades, pérdida o robo de carpetas físicas y magnéticas con información, ataques cibernéticos por medio de correos o páginas oficiales del DADEP, correos de tipo SPAM, contenidos inusuales, entre otros.

Incidente de otro tipo

*Incidentes que se presentan a nivel tecnológico y no afectan o exponen la información de la entidad. Los incidentes que no estén relacionados con la seguridad de la información se llaman incidentes de tecnología, por ejemplo: no acceso al equipo de cómputo (porque olvidó la clave, porque el equipo esta desconectado de la red, por fallas técnicas etc.), desconfiguración de los sistemas de información o aplicaciones, el bloqueo de una contraseña o perdida de esta, etc.

Responsabilidades

Es responsabilidad de los funcionarios y contratistas reportar todos los posibles incidentes de seguridad de la información a la mesa de servicio, a través de los canales dispuestos para ello.
*Todo reporte de un posible incidente de seguridad de la información debe contener como mínimo con los siguientes datos:
•Nombre de funcionario o contratista que reporta
•Teléfono y/o extensión de contacto
•Correo electrónico
•Descripción del posible incidente

*Todo reporte de un posible incidente de seguridad de la información será valorado por la mesa de servicio, teniendo en cuenta las siguientes consideraciones al momento de realizar la asignación del caso:
•Relacionar el posible incidente con una afectación en la integridad, disponibilidad y confidencialidad de la información.
•Reunir información básica (lugar, tipo de información, datos de contacto de la persona que reporta) que llevó a determinar que es un posible incidente de seguridad de la información, información que podrá ser utilizada en la investigación y/o para empezar a contener los daños y minimizar el riesgo.

* El gestor de incidentes de seguridad de la información hará la tipificación de incidente mayor y solicitud padre, los cuales pueden ser asociados a los casos según corresponda; es posible que un incidente mayor y una solicitud padre estén asociados a un mismo caso.

Clasificación de los incidentes de seguridad de la información.

Los incidentes de seguridad de la información se clasifican, así:

Clases de incidentes de seguridad de la información	Descripción de la acusa raíz	Ejemplo
Incidente de desastre natural	Por desastres naturales fuera del control humano.	Terremotos, erupciones volcánicas, inundaciones, huracanes, tormentas eléctricas, incendio forestal, tsunamis, derrumbes, etc.
Incidente de daño físico	Debido a acciones físicas accidentadas en las instalaciones de la entidad	Incendio, agua, ambiente nefasto (contaminación, polvo, corrosión, congelamiento), destrucción de

	de la entidad.	equipos, destrucción de medios, robo de equipos, robo de medios, etc.
Incidente de fallas de infraestructura tecnológica	Generado por fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información y los servicios sociales.	Fallas en la alimentación eléctrica, en las redes, en el aire acondicionado, fallas de hardware, etc.
Incidente de malware	Causas asociadas de programas maliciosos creados y divulgados en forma intencional.	Virus informáticos, gusanos de red, troyanos, botnet (red de robots), ataques combinados, páginas web con códigos maliciosos, sitio hosting con códigos maliciosos, etc.
Incidente de ataque técnico	Resultado de ataques a sistemas de información, a través de redes u otros medios técnicos, mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, que genera un estado anormal de los sistemas de información.	Aprovechamiento de puertas traseras, aprovechamiento de vulnerabilidades informáticas, denegación de servicios, escaneo de redes, intentos de ingreso, interferencia, etc.
Incidente relacionado con contenidos peligrosos	Por causas asociadas de propagación de contenido indeseable a través de redes de información, lo que pone en peligro la seguridad nacional, la estabilidad social y/o la seguridad y beneficios públicos.	Contenido ilegal, contenido que provoca pánico, contenido malicioso, contenido abusivo, etc.
Incidente de puesta en riesgo de la información	La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o intencional la confidencialidad, integridad y disponibilidad de la información.	Interceptación, espionaje, "chuzada" de teléfonos, divulgación, enmascaramiento, ingeniería social, phishing de redes (Suplantación de identidad), robo de datos, alteración de datos, errores de datos, etc.
Incidente de violación de reglas	Debido al uso no autorizado de recursos y violación de derechos de autor.	Uso de recursos de acceso para propósito no autorizado, por ejemplo, el uso del correo para participar en cadenas ilegales, pirámides, etc. Causada por la venta e instalación de copias de software sin licencia, u otros materiales protegidos por derechos de autor.

Tabla 1Clases de incidentes de seguridad de la información basado en la Guía Técnica 27035:2012

* Tipificación en prioridad de incidentes de la información

Para la correcta gestión, todos los incidentes de seguridad de la información deberán tipificarse en prioridad de acuerdo con su impacto y urgencia por el gestor de Incidentes de Seguridad de la Información:

Nivel de prioridad			
Impacto/Urgencia	Alta	Media	Baja
Alto	Alta	Alta	Media
Medio	Alta	Media	Baja
Bajo	Media	Baja	Baja

Tabla 2 Nivel de prioridad de los incidentes de seguridad de la información

Prioridad	Alcance	Descripción
ALTO	El incidente de seguridad puede afectar la continuidad de la prestación de los servicios sociales del DADEP.	El incidente alto tiene un impacto considerable (afectación total a la confidencialidad, disponibilidad o integridad) en la información y se considera crítica para la misión del DADEP, esto incluye información en diferentes medios y/o sistemas críticos. Estos incidentes implican una grave violación de seguridad o pueden dañar la confianza en la administración pública (pérdida de imagen institucional), o podrían afectar la seguridad física de las personas, causar una pérdida importante de recursos de la entidad.
MEDIO	El incidente de seguridad afecta a una o más dependencias	Se clasifican con este nivel aquellos eventos que puedan afectar o está afectando a los activos de información de la entidad, con una valoración considerable en la triada de la información (confidencialidad, disponibilidad o integridad), lo cual puede resultar en la pérdida directa de información para el DADEP.
BAJO	El incidente afecta a un colaborador o varios colaboradores de una dependencia.	Se clasifican con este nivel aquellos eventos que puedan ser una amenaza que afecta o está afectando a activos de información de la entidad con una valoración de impacto limitado en la triada de la información (confidencialidad, disponibilidad o integridad). Su impacto debe ser nulo o insignificante para el DADEP.

*En caso de que el incidente de seguridad de la información se considere de prioridad alta, el gestor de incidentes de seguridad de la información de la entidad deberá proponer el equipo que participará en el tratamiento del incidente y este será aprobado por el comité de Gestión Institucional del DADEP

*Cuando se presenten incidentes mayores o catastróficos no se requiere previo registro en la herramienta de gestión y debe ser tratado directamente por el gestor de incidentes de seguridad de la información quien a su vez trabajará de forma articulada con el Jefe de la Oficina de Sistemas. Esto con el fin dar un tratamiento prioritario en búsqueda de la solución del incidente.

* Los incidentes de seguridad de la información que no se consideren prioridad alta estarán liderados por el gestor de incidentes de seguridad de la información.

Prioridades de tratamiento de incidentes de seguridad de la información

*Se debe actuar para reducir los efectos reales y potenciales de un incidente, ya que esto puede marcar la diferencia entre un impacto menor o uno de mayor importancia, ver tabla 3. La respuesta exacta dependerá de la naturaleza del incidente al que se enfrente. No obstante, se sugieren las siguientes prioridades como punto de partida:
•Proteger la vida humana y la seguridad de las personas.
•Proteger la información reservada y confidencial.
•Proteger otra información relevante (por ejemplo, propiedad intelectual o del ámbito directivo).
•Proteger el hardware y software del DADEP.
•Minimizar la interrupción de los recursos informáticos.

*Existen varias medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno, como mínimo se debe llevar a cabo las siguientes acciones:
•Evitar que los posibles atacantes conozcan las actividades que se adelanten dentro del tratamiento.
•Comparar el impacto de dejar sin conexión los sistemas en peligro y los sistemas relacionados con el riesgo de continuar funcionando.
•Determinar los puntos de acceso usados por posibles atacantes e implementar las medidas adecuadas para evitar futuros accesos.
•Considerar la opción de volver a crear un sistema con discos duros nuevos (se deben eliminar los discos duros existentes y almacenarlos, ya que se pueden usar como prueba si se decide procesar a los posibles atacantes).
•Asegurar el cambio de las contraseñas: locales, de las cuentas de servicio y administrativas en todo el entorno.

*Las posibles acciones para adelantar son:
•**Una solución efectiva**: La gestión del incidente logró remediar los servicios o activos afectados por el incidente.
•**Una solución que relaciona un cambio:** La gestión del incidente logró remediar los servicios o activos afectados por el incidente, sin embargo, el incidente puede replicarse, siendo necesario ejecutar un cambio para evitar reincidencia.
Cualquier incidente que implique la afectación de la misionalidad de la entidad o de un proceso de manera crítica, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios tecnológicos, se debe dar una respuesta inmediata, la cual puede incluir la generación de un control de cambios para lo cual se deberá tener en cuenta las actividades del procedimiento de Gestión de Cambios de Tecnología.
La valoración del incidente de seguridad de la información se realizará por el gestor de incidentes de seguridad del DADEP para determinar las consecuencias, las cuales constituirán una prueba importante y necesaria si se decide emprender acciones legales. Entre ellos, se pueden contar los siguientes:
•Consecuencias asociadas a la pérdida de información confidencial.
•Consecuencias legales.
•Consecuencias laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
•Consecuencias en el tiempo de inactividad de los sistemas (por ejemplo, pérdida de productividad de los funcionarios y/o contratistas, sustitución del hardware, del software y de otras propiedades).
•Consecuencias relacionadas con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
•Consecuencias relacionadas con la imagen del proceso afectado por un incidente.
•Otros daños derivados, como la pérdida de la reputación o de la confianza de los beneficiarios del DADEP.

*Se utilizará la siguiente tabla para valorar las consecuencias de los incidentes de seguridad de la información en el DADEP:

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la Entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la Entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la Entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la Entidad.
5	Catastrófica	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la Entidad.

Tabla 3 Consecuencias de los incidentes de seguridad de la información

Debe tenerse en cuenta que los incidentes deben clasificarse únicamente de acuerdo con lo establecido en la anterior tabla y puede tener incumplimiento legal, sanciones, costos, pérdida de imagen o afectación de la operación de la DADEP.

PRODUCTO O SERVICIO

SALIDAS (Producto o Servicio)	DESCRIPCIÓN	GRUPOS DE VALOR OBJETIVO
- Política de SGSI - Declaración de alcance del SGSI - Plan de tratamiento de riesgos de seguridad de la información. - Informes de auditoría del SGSI - Recomendaciones de mejora para el SGSI	Documentos necesarios para gestionar inicidentes de seguridad de la información.	Comité Directivo Usuarios internos

NORMATIVIDAD Y/O DOCUMENTOS ASOCIADOS

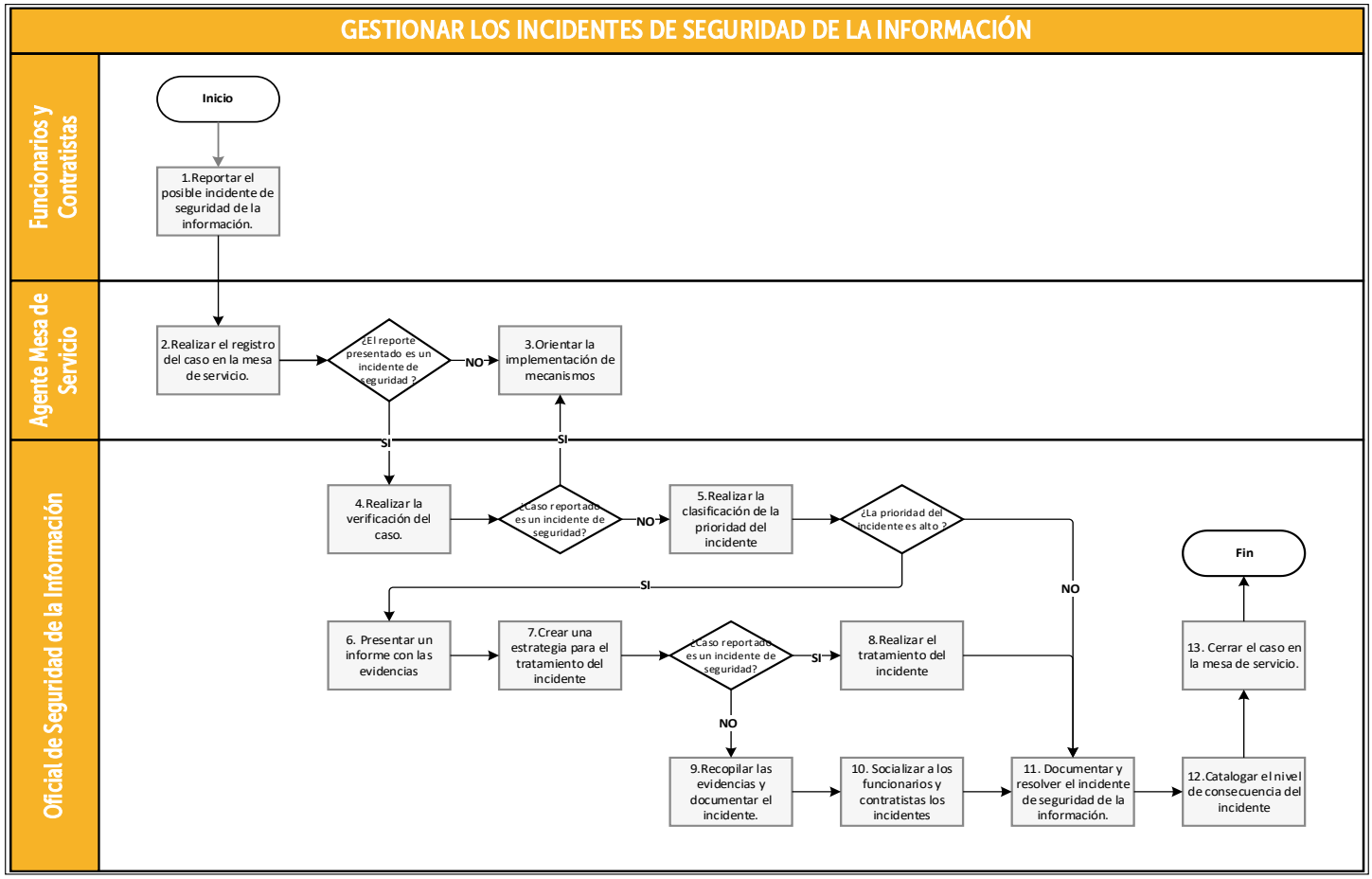
- El control de los riesgos a la seguridad de la información, riesgos laborales, aspectos ambientales se pueden consultar el siguiente vinculo: Mapa de Riesgos.
- La normativa asociada al procedimiento se puede consultar en el siguiente vinculo: Matriz de requisitos legales y normativos
- Los documentos asociados al procedimiento se pueden consultar en el siguiente vinculo: Listado Maestro de Documentos.
- Los registros asociados al procedimiento se pueden consultar en el siguiente vinculo: Listado Maestro de registros/ Cuadro de Caracterización Documental
- Las disposiciones de almacenamiento y archivo se pueden consultar en el siguiente vinculo: Tablas de Retención Documental.

ACTIVIDAD	FLUJOGRAMA	DESCRIPCIÓN ACTIVIDAD	TIEMPO	RESPONSABLE	FORMATO Y/O REGISTRO
		INICIO			
1	Ver Anexo Flujograma DSS02	Reportar a la mesa de servicio el posible incidente de seguridad de la información.		Funcionarios y contratistas	reporte del caso a través de los canales de comunicación definidos

2		Realizar el registro del caso en la mesa de servicio. ¿El reporte presentado es un incidente de seguridad ? **SI**:Realizar el escalamiento al gestor de incidentes de seguridad de la información a través de la mesa de servicios. *Continuar con la actividad 4* **NO:** Asignar caso a soporte en sitio para realizar la verificación del caso. *Continuar con la actividad 3*		Agente mesa de servicio	Registro herramienta de gestión
3		Realizar la verificación del caso y documentar en la herramienta de gestión el cierre de este. *Continuar con la actividad 13*.		Agente mesa de servicio	
4		Realizar una nueva revisión del caso y evaluar si este es un incidente de seguridad. ¿Caso reportado es un incidente de seguridad? SI: *Continuar con la actividad 5.* NO:Reasignar a la mesa de servicio. *Regresar a la actividad 3.*		Oficial de seguridad de la información	
5		Realizar la clasificación de la prioridad del incidente de acuerdo a lo definido en las tablas 1, 2 y 3 de las políticas de operación. ¿La prioridad del incidente de seguridad es alto ? SI: Continuar con la actividad 6 NO: Continuar con la actividad 11		Oficial de seguridad de la información	
6		Presentar un informe con las evidencias recopiladas y plantear posibles alternativas para la solución del incidente e informar al Jefe de la Oficina de Sistemas para convocar a los involucrados en la solución del incidente.		Oficial de seguridad de la información	Informe de evidencias
7		Crear una estrategia para el tratamiento del incidente junto con los convocados para la solucion. ¿La respuesta del incidente requiere un control de cambios ? SI: Continuar con el proceso BAI06-GestionarlosCambios. NO: Continuar con actividad 9.		Oficial de seguridad de la información	
8		*Viene del proceso BAI06-GestionarlosCambios.* Realizar el tratamiento del incidente acorde a lo establecido en el control de cambios. *Continuar con la actividad 10.*		Oficial de seguridad de la información	
9		Recopilar las evidencias y documentar el incidente.		Oficial de seguridad de la información	Informe de actividades
10		Socializar a los funcionarios y contratistas los incidentes clasificados como altos o críticos divulgando, los controles implementados para que estos tomen medidas preventivas y mitiguen riesgos de seguridad de la información.		Oficial de seguridad de la información	
11		Documentar y resolver el incidente de seguridad de la información.		Oficial de seguridad de la información	
12		Catalogar el nivel de consecuencia del incidente el cual deberá quedar documentado en la herramienta de gestión de la Entidad		Oficial de seguridad de la información	herramienta de gestión
13		Cerrar el caso en la mesa de servicio.		Oficial de seguridad de la información	herramienta de gestión
		FIN			

AUTORIZACIÓN

Elaboró:	Revisó:	Aprobó:
Guiomar Cortés Ávila Gerente de Proyectos Oficina de Sistemas	Luis Fernando Arango Vargas Profesional Universitario Oficina Asesora de Planeación	Syrus Asdrubal Pacheco Jefe Oficina de Sistemas


GESTIONAR LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
Funcionarios y Contratistas
Agente Mesa de Servicio
Oficial de Seguridad de la Información
Inicio
1.Reportar el posible incidente de seguridad de la información.
2.Realizar el registro del caso en la mesa de servicio.
¿El reporte presentado es un incidente de seguridad ?
NO
3.Orientar la implementación de mecanismos
SI
SI
4.Realizar la verificación del caso.
¿Caso reportado es un incidente de seguridad?
NO
5.Realizar la clasificación de la prioridad del incidente
¿La prioridad del incidente es alto ?
SI
NO
6. Presentar un informe con las evidencias
7.Crear una estrategia para el tratamiento del incidente
¿Caso reportado es un incidente de seguridad?
SI
8.Realizar el tratamiento del incidente
NO
9.Recopilar las evidencias y documentar el incidente.
10. Socializar a los funcionarios y contratistas los incidentes
11. Documentar y resolver el incidente de seguridad de la información.
12.Catalogar el nivel de consecuencia del incidente
13. Cerrar el caso en la mesa de servicio.
Fin