1. OBJETIVO

Gestionar oportunamente los incidentes de seguridad de la información que afecten la confidencialidad, integridad o disponibilidad de los activos de información de la DIAN, para dar una respuesta efectiva que incluya acciones de preparación, identificación, contención, erradicación, recuperación y análisis post-incidente.

2. ALCANCE

Inicia con la detección o reporte de eventos de seguridad de la información y finaliza con el cierre del incidente.

3. CONDICIONES GENERALES

3.1 Generalidades

Todos los servidores públicos y contratistas deben reportar los eventos de seguridad de la información a los enlaces de seguridad de la información o delegados, designados en las dependencias del nivel central y del nivel seccional.

3.2 Tipificación de eventos de seguridad de la información

El enlace de seguridad de la información o delegado debe catalogar el evento presentado, en alguna de las siguientes categorías:

Tipo de evento	Descripción
Acceso no autorizado	Intento de acceso lógico o físico a datos, sistemas de información, aplicaciones o recursos tecnológicos sin la debida autorización.
Alerta sin impacto	Evento que no tiene consecuencias reales ni representa una amenaza significativa para la DIAN.
Archivo sospechoso	Detección o identificación de un archivo o un código que presenta comportamiento sospechoso.
Afectación en el tratamiento de datos personales	Presunta pérdida de confidencialidad, integridad o disponibilidad de los datos personales.
Copia no autorizada de información	Detección de transferencia o copia de datos sin la debida autorización.
Correo sospechoso/malicioso	Recepción de correos con enlaces o archivos adjuntos que podrían contener una amenaza cibernética.
Errores humanos	Acciones no intencionadas de los usuarios que pueden comprometer la seguridad de información de los activos de la DIAN.

Tipo de evento	Descripción
Escaneo de vulnerabilidades	Identificación de fallos o debilidades en software o hardware que podrían comprometer la seguridad de la infraestructura tecnológica de la DIAN.
Extravío de recurso físico con información institucional	Pérdida o extravío de dispositivos físicos institucionales que contienen información de la DIAN.
Incumplimiento de acuerdos de nivel de servicio	Incumplimiento de un acuerdo de nivel de servicio por parte de un área de la entidad o un tercero.
Incumplimiento de Políticas de Seguridad de la Información	Incumplimiento u omisión del MN-IIT-0072 Manual de políticas y lineamientos de seguridad de la información de la DIAN.
Incumplimiento normativo	Incumplimiento u omisión de normativas internas, lineamientos institucionales o regulaciones externas aplicables a la DIAN.
Intento de modificación de datos	Detección de intento no autorizado de alterar información o modificar configuraciones en un sistema o servicio informático.
Intermitencia o lentitud del servicio	Degradación parcial del servicio o sistema de información sin pérdida total de disponibilidad.
Multicomponente	Hace referencia a un evento de seguridad de la información que involucra más de una categoría de eventos.
Perdida o fuga de Información	Sospecha o alerta de eliminación, robo o divulgación no autorizada de información o de datos.
Phishing	Intento de engaño que busca obtener credenciales, datos personales o información sensible mediante comunicaciones fraudulentas que simulan provenir de fuentes legítimas o confiables.
Suplantación de la DIAN	Identificación de sitios o servicios falsos que imitan a la DIAN o sus funciones.
Uso inapropiado de los recursos	Evento en el que un usuario realiza acciones que incumplen las políticas y directrices establecidas por la DIAN para el uso adecuado de sus recursos tecnológicos.
Otro	Hace referencia a cualquier otro tipo de evento que no se encuentre dentro de las definiciones de eventos anteriormente expuestas o identificadas por la DIAN.

3.3 Tipificación de incidentes de seguridad de la información

Con esta información, los servidores públicos de la OSI, responsables de la gestión de incidentes de seguridad de la información debe catalogar el incidente identificado, en alguna de las siguientes categorías:

Tipo de incidente	Descripción
Acceso no autorizado	Corresponde a situaciones en las que una persona, proceso o sistema accede de forma lógica o física a información, sistemas, aplicaciones o activos de información, sin contar con la autorización formal requerida.
Amenazas internas	Abuso de privilegios, negligencia o acciones maliciosas realizadas por usuarios legítimos con acceso autorizado a los activos de información de la DIAN.
Despliegue inseguro de sistemas	Implementación de sistemas, servicios o aplicaciones sin la validación de controles de seguridad mínimos o sin pruebas de calidad adecuadas.
Errores o fallas de terceros	Fallos o acciones indebidas de contratistas o proveedores con acceso autorizado a infraestructura o servicios de TI de la DIAN.
Explotación de vulnerabilidades	Aprovechamiento de fallos o debilidades en el software, hardware o configuraciones para comprometer la seguridad de la infraestructura tecnológica de la DIAN.
Incumplimiento normativo	Incumplimiento de los lineamientos definidos en el MN-IIT-0072 Manual de políticas de seguridad de la información, o de las normativas vigentes relacionadas con la seguridad y privacidad de la información de la DIAN.
Ingeniería social	Manipulaciones utilizadas para engañar personas y obtener acceso, credenciales, información confidencial o reservada, o inducir acciones en enlaces maliciosos o descargar malware
Interrupción o indisponibilidad del servicio	Situaciones que provocan la interrupción o pérdida total de disponibilidad de un sistema, servicio o activo de información.

Tipo de incidente	Descripción
Malware	Infección mediante software o código malicioso que compromete la seguridad de los sistemas de información, ciberactivos y/o los datos institucionales.
Modificación no autorizada	Alteraciones no autorizadas realizadas por personas, procesos o sistemas, que comprometen la integridad de la información o afectan el funcionamiento de sistemas, servicios o activos de la DIAN.
Multicomponente	Hace referencia a un incidente de seguridad de la información que involucra dos o más de las categorías previamente definidas
Otros	Incidente que no se ajustan a las categorías existentes o identificadas por la DIAN
Pérdida o fuga de información	Pérdida, divulgación o fuga no autorizada de información confidencial o reservada.
Pérdida o robo de activos fisicos	Extravío o robo de dispositivos institucionales que contienen información confidencial de la DIAN.
Uso Inapropiado de recursos	Uso indebido de recursos tecnológicos, físicos o de información institucional, en contravención de las políticas y lineamientos establecidos por la DIAN.
Violación en la seguridad de datos personales	Perdida de confidencialidad o integridad de los datos personales tratados por la DIAN

3.4 Valoración de los incidentes de seguridad de la información

Con el fin de permitir una gestión adecuada de los incidentes de seguridad de la información, es necesario determinar su nivel de prioridad. Esta priorización permitirá atenderlos oportunamente según su criticidad. Para ello, se definen una serie de variables que servirán como base para su evaluación en la herramienta de gestión.

Impacto actual: cantidad de daño que ha provocado el incidente en el momento de ser detectado.
Impacto futuro: cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Nivel de impacto	Descripción
Superior	Impacto alto en uno o más componentes de más de un sistema de información.
Alto	Impacto moderado en uno o más componentes de más de un sistema de información.
Medio	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Inferior	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.

Criticidad: depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Nivel de criticidad	Descripción
Superior	• Los activos afectados son clasificados como críticos en la entidad. • Los riesgos materializados corresponden a riesgos catastróficos o altos. • Se presentó afectación sobre datos personales confidenciales, reservados o de niños, niñas y adolescentes.
Alto	• Los activos afectados son clasificados con criticidad alta en la entidad. • Los riesgos materializados corresponden a riesgos altos. • Se presentó afectación sobre datos personales privados.
Medio	• Los activos afectados son clasificados como moderados en la entidad. • Los riesgos materializados corresponden a riesgos medios. • Se presentó afectación sobre datos personales semiprivados.
Bajo	• Los activos afectados son clasificados como bajos en la entidad. • Los riesgos materializados corresponden a riesgos bajos. • Se presentó afectación sobre datos personales públicos.
Inferior	• Sistemas no críticos

Fuente: Oficina de Seguridad de la Información

Prioridad: con base en la valoración del impacto y la criticidad, se determina la prioridad y el tiempo de atención correspondiente para el incidente identificado.

Nivel de prioridad	Tiempo de atención
Superior	1 hora
Alto	2 horas
Medio	4 horas
Bajo	8 horas
Inferior	16 horas

Fuente: Oficina de Seguridad de la Información

3.5 Contacto con autoridades

A continuación, se presentan los criterios que deben aplicarse para realizar el contacto con las autoridades correspondientes, en caso de que sea necesario reportar un incidente según su naturaleza:

Entidad	Cuando	Quien	Medios de reporte
ColCERT	El incidente está catalogado como Superior y Alto.	Servidores Públicos, responsables de la gestión de incidentes de seguridad de la información	Reportar a través del correo electrónico contacto@colcert.gov.co, adjuntando un informe técnico que describa el incidente. El ColCERT se encargará de gestionar el apoyo de entidades como la fiscalía, el Centro Cibernético Policial u otras autoridades competentes, cuando la atención del caso así lo requiera.
	El incidente está catalogado como Medio y Bajo.		Reporte de incidentes de seguridad digital, gestionados por las entidades. https://www.colcert.gov.co/800/w3-article-198656.html#formulario_iform_ReporteIncidentes_1
Superintendencia de Industria y	Cuando se identifica un incidente que compromete la confidencialidad, integridad y/o	Oficial de protección de datos	Registrar el incidente en la plataforma tecnológica de la Superintendencia de Industria y Comercio y

Entidad	Cuando	Quien	Medios de reporte
Comercio (SIC)	disponibilidad de los datos personales.	personales o delegado	reportarlo dentro de los quince (15) días hábiles siguientes a su identificación. https://www.sic.gov.co/tema/proteccion-de-datos-personales

3.6 Acciones mínimas de contención

Las acciones de contención deben ser evaluadas y consensuadas entre las partes involucradas. No obstante, se plantean algunas alternativas que podrán ser ejecutadas conforme a la tipificación del incidente, previa realización de un análisis que considere las posibles consecuencias de su implementación.

Tipo de incidente	Acciones de contención inmediatas
Acceso no autorizado	• Cierre de sesiones activas. • Solicitar el cambio de contraseñas. • Bloquear las cuentas de usuarios afectadas.
Amenazas internas	• Revisar registros de actividad de los usuarios identificados. • Cambiar credenciales de acceso a los sistemas o servicios afectados. • Aislar a los usuarios identificados si es necesario.
Despliegue inseguro de sistemas	• Aplicar controles de seguridad adecuados. • Revisar configuraciones de seguridad de los sistemas implementados. • Validar los servicios y aplicaciones desplegadas.
Errores o fallas de terceros	• Aislar los servicios afectados hasta resolución del incidente. • Identificar la causa del error o falla. • Notificar a los proveedores o contratistas sobre el incidente.
Explotación de vulnerabilidades	• Aislar el sistema o servicio afectado. • Aplicar parches de seguridad inmediatamente si están disponibles.

Tipo de incidente	Acciones de contención inmediatas
	• Evaluar posibles riesgos adicionales.
Incumplimiento normativo	• Detener las actividades no autorizadas o que violen las normativas. • Notificar a los responsables de la política o normativa violada. • Revisar y reforzar controles del MN-IIT-0072 Manual de políticas y lineamientos de seguridad y de la información.
Ingeniería social	• Alertar a los servidores públicos y/o ciudadanía sobre la amenaza. • Bloquear enlaces maliciosos o correos sospechosos. • Realizar un análisis de la información comprometida.
Interrupción o indisponibilidad del servicio	• Validar el estado de los servicios y sistemas de información. • Identificar las causas de la interrupción o indisponibilidad. • Aplicar procedimientos de recuperación para restaurar el servicio.
Malware	• Aislar los dispositivos infectados. • Realizar un análisis de malware en profundidad. • Desinfectar o restaurar los dispositivos desde copias de seguridad seguras.
Modificación no autorizada	• Bloquear los accesos a los recursos modificados. • Restaurar los datos o configuraciones alteradas a partir de copias de seguridad.
Otros	• Determinar la naturaleza específica del incidente. • Definir acciones de contención según el impacto detectado. • Todas aquellas tareas definidas por los servidores públicos de la OSI, responsables de la gestión de incidentes de seguridad de la información que deban ejecutarse para evitar la propagación del incidente.

Tipo de incidente	Acciones de contención inmediatas
	• Todas aquellas tareas que determine el procedimiento PR-IIT-0454 Disponibilidad de la operación tecnológica.
Pérdida o fuga de información	• Identificar el impacto de la pérdida o fuga de información. • Bloquear accesos externos o sistemas afectados. • Notificar al dueño o propietario del activo de información.
Pérdida o robo de activos fisicos	• Informar a los responsables del activo. • Bloquear accesos asociados a los dispositivos perdidos. • Monitorear actividad inusual relacionada con los recursos perdidos.
Uso Inapropiado de recursos	• Aislamiento físico o lógico de los activos afectados. • Detener el uso indebido de los recursos. • Notificar a los responsables de los recursos involucrados.
Violación en la seguridad de datos personales	• Notificar al Oficial de protección de datos personales o delegado. • Aislar y proteger los datos comprometidos. • Iniciar análisis de la afectación y posibles riesgos de exposición.

3.7 Datos personales

Si dentro de la descripción de este procedimiento o de alguno de sus documentos relacionados se manejan datos personales, se deben implementar los instrumentos, lineamientos y parámetros establecidos en la política de tratamiento de datos personales de la DIAN, el manual de protección de datos personales, en especial lo referente al principio de privacidad por diseño y por defecto y demás normativa interna y/o externa referente al tema; son datos sensibles tener en cuenta lo establecido en el Manual de protección de Datos y en Anexo 1 del mismo

4. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	clasificación documento
Manual	MN-IIT-0072	Manual de políticas y lineamientos de seguridad de la información	Digital	interno
Procedimiento	PR-IIT-0458	Gestión de incidentes	Digital	interno
Procedimiento	PR-IIT-0454	Disponibilidad de la operación tecnológica	Digital	interno
Procedimiento	PR-CAC-0043	Peticiones, quejas, sugerencias, reclamos, felicitaciones y denuncias	Digital	interno
Protocolo	OD-PEC-0003	Protocolo de Manejo de Incidentes e Identificación de Crisis	Digital	Interno

5. DEFINICIONES Y SIGLAS

- **ColCERT**: Grupo de Respuesta a Emergencias Cibernéticas de Colombia - Organismo nacional encargado de coordinar las acciones de prevención, respuesta y gestión ante incidentes de ciberseguridad en Colombia. Fuente: UAE DIAN - Oficina de Seguridad de la Información

- **Crisis:** materialización de un incidente que se sale de control y afecta negativamente a las personas, a la prestación de servicios, a la tecnología, a la información o a la reputación institucional. Fuente: UAE DIAN. Subdirección de Procesos.

- **DGIT:** Dirección de Gestión de Innovación y Tecnología.

- **Evento de seguridad de la información**: cualquier ocurrencia o detección de una situación anómala que podría impactar la confidencialidad, integridad o disponibilidad de la información, en contravención de las políticas, normas o procedimientos de seguridad de la información de la DIAN. Fuente: UAE DIAN - Oficina de Seguridad de la Información

- **Incidente de seguridad de la información:** evento o serie de eventos de seguridad de la información que tienen una alta probabilidad de impactar negativamente los activos de información y amenazar las operaciones de negocio de la entidad.
  Fuente: UAE DIAN - Oficina de Seguridad de la Información.

- **Incidente de seguridad en el tratamiento de datos personales:** evento o serie de eventos de seguridad de la información que tienen una alta probabilidad de impactar negativamente la gestión o tratamiento de datos personales por parte de la entidad. Fuente: UAE DIAN. Oficina de Seguridad de la Información

- **OSI:** Oficina de Seguridad de la Información.

- **SI:** Seguridad de la Información
- **SIC:** Superintendencia de Industria y Comercio - supervisa el cumplimiento de la Ley 1581 de 2012 y su normativa relacionada, garantizando los derechos de los titulares de datos.
- **SOC:** Centro de Operaciones de Seguridad.

6. DIAGRAMA DE FLUJO

6.1 Entradas

No de actividad	Proveedores	Entradas	Requisitos
1	Servidores públicos, Centro de Operaciones de Seguridad (SOC) y contratistas DIAN	Reporte de Eventos de Seguridad de la información	Reportar en la herramienta de gestión disponible al enlace de seguridad de la información, en caso de presentarse alguno de los siguientes eventos de seguridad de la información: • Correos falsos o sospechoso masivos que lleguen al buzón corporativo de la entidad. • Mal funcionamiento del software y hardware de la entidad. • Afectación a datos personales resguardados por la entidad. • Incumplimiento del manual de políticas y lineamientos de seguridad y privacidad de la información o directrices. • Errores humanos que afecten la seguridad de la información de la entidad. • Incumplimiento de las expectativas de integridad, confidencialidad o disponibilidad de la información. • Cambios no controlados en los sistemas de la entidad. • Infracciones de acceso. • Vandalismo o disturbios sociales que afecten la seguridad de la información de la entidad. • Desastres naturales que afecten la seguridad de la información de la entidad. • Vulnerabilidades de hardware y software de la entidad.
1	Ciudadanos	Peticiones, quejas, sugerencias, reclamos, felicitaciones y denuncias *(A)	Recibido a través del procedimiento PR-CAC-0043 Peticiones, quejas, sugerencias, reclamos, felicitaciones y denuncias. Deben contener la siguiente información: • Número de radicado para el caso de las PQRS. • La designación de la dependencia de la Dirección de Impuestos y Aduanas Nacionales a la cual se dirige.

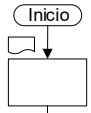
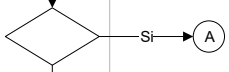
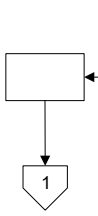
No de actividad	Proveedores	Entradas	Requisitos
			• Los nombres y apellidos completos del solicitante y de su representante y o apoderado, sí es el caso, con indicación de su documento de identidad, dirección electrónica o física donde recibirá correspondencia y teléfono de contacto. • El objeto de la petición. • Las razones en las que fundamenta su petición. • La relación de los requisitos exigidos por la Ley y de los documentos que desee presentar para iniciar el trámite. • La firma del peticionario cuando fuere el caso.
1	Entes externos	Reporte de eventos o incidentes	Entidades externas como el Ministerio de Tecnologías de la Información y las Comunicaciones a través del ColCERT puede identificar vulnerabilidades o incidentes que afecten los activos de la organización. El detalle de esta información depende en gran medida de cómo se identifiquen las debilidades sobre la organización, por lo general se espera recibir la identificación del activo potencialmente afectado y las debilidades encontradas, así como fecha y hora del hallazgo.

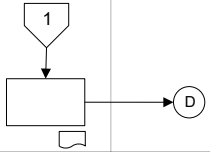
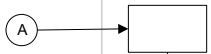
*A (Activo de información)

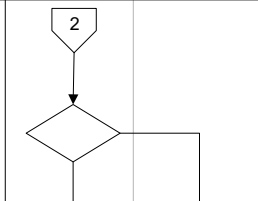
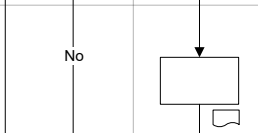
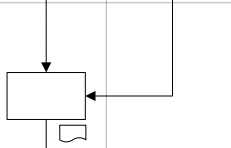
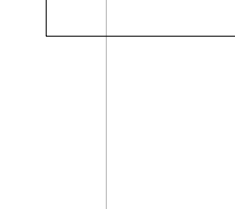
6.2 Descripción de Actividades

Los símbolos definidos para los flujogramas de la DIAN son los siguientes:

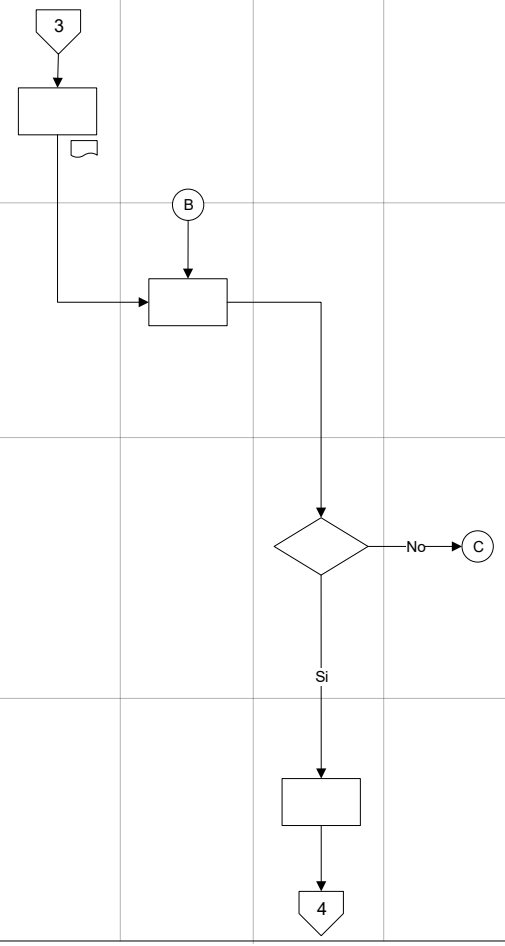
Simbolo	Descripción	Simbolo	Descripción
	INDICA LA SECUENCIA DEL FLUJOGRAMA.		INDICA QUE EL FLUJOGRAMA TIENE VARIAS OPCIONES DE SECUENCIA (máximo 3).
	INDICA LAS ACTIVIDADES REALIZADAS MANUALMENTE.		INDICA LAS ACTIVIDADES REALIZADAS AUTOMÁTICAMENTE.
	INDICA QUE LA ACTIVIDAD ESTA GENERANDO UNA SALIDA A OTRO PROCEDIMIENTO, SUBPROCESO, PROCESO O CLIENTE EXTERNO.		INDICA EL INICIO O EL FIN DEL FLUJOGRAMA.
	INDICA QUE EN LA ACTIVIDAD PRESENTA UNA ENTRADA GENERADA POR OTRO PROCEDIMIENTO, SUBPROCESO, PROCESO O CLIENTE EXTERNO.		INDICA LA CONEXIÓN ENTRE ACTIVIDADES UTILIZANDO CARACTERES ALFABETICOS.
	INDICA QUE UN PROCEDIMIENTO, SUBPROCESO O PROCESO SUMINISTRA O RECIBE INSUMOS.		INDICA LA CONEXIÓN ENTRE PÁGINAS UTILIZANDO CARACTERES NUMÉRICOS.

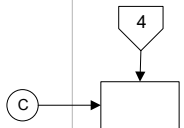
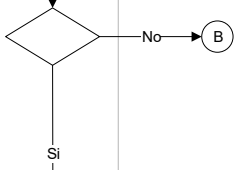
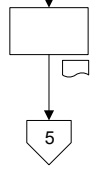
ACTIVIDAD	RESPONSABLE DE			DEPENDENCIA	REGISTROS
	Servidor Público DIAN	Enlace de SI / Responsable de Incidentes SI	Incidentes de seguridad de la Información		
1.Identificar y reportar evento de seguridad de la información. Los eventos de seguridad pueden ser detectados por funcionarios, ciudadanos (PQRS) o por el equipo de monitoreo de Infraestructura Tecnológica. Ante la detección de una situación anómala o sospechosa, los funcionarios deben reportarla por correo electrónico al Enlace de Seguridad de la Información o al delegado designado. Se reporta el incidente teniendo en cuenta los requisitos establecidos en el numeral 6.1 y la tipificación de eventos presentados en el numeral 3.2.				Todas las dependencias	Correo electrónico PQRS
2. Registrar caso en herramienta Se debe crear un nuevo caso en la herramienta destinada para la gestión de eventos e incidentes de seguridad de la información, incluyendo la siguiente información: Tipo de evento: Seleccionar la categoría correspondiente según las opciones disponibles en la herramienta. Descripción del evento: Explicar de forma clara y concisa la situación presentada. Fecha y hora del reporte: Registrar el momento en que se reportó el evento. Evidencias adjuntas: Incluir capturas de pantalla, correos electrónicos u otros elementos que respalden el reporte.				Todas las dependencias	Registro en Herramienta de Gestión
3. ¿El evento debe escalarse a un incidente de seguridad de la información? Una vez registrado el evento, Los responsables de atender Incidentes de Seguridad de la Información lo analizará para determinar si debe ser escalado como un incidente, o si debe continuar su tratamiento y cierre como un evento. Si el evento corresponde a un incidente de seguridad de la información, continúa con la Actividad 6. De los contrario, si el evento no cumple con las características o parámetros para ser clasificado como incidente, se debe continuar con la Actividad 4.				Oficina de Seguridad de la información	Registro en Herramienta de Gestión
4. Realizar tratamiento del evento Durante el tratamiento del evento, se deben documentar en la herramienta de gestión todas las acciones realizadas, asegurando su trazabilidad. Este tratamiento incluye las siguientes etapas: **Análisis.** Son las acciones o actividades iniciales que permiten obtener una visión clara del hecho, con el fin de tomar decisiones informadas sobre su tratamiento. **Verificación.** Son las acciones o actividades realizadas para confirmar si se trata de un comportamiento anómalo real o simplemente de un falso positivo. **Acciones Correctivas Menores.** Son acciones, medidas o actividades simples que se aplican para corregir el evento y prevenir su recurrencia.				Todas las dependencias	Registro en Herramienta de Gestión

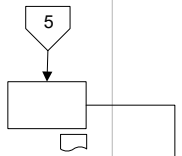
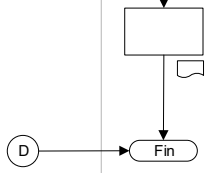
ACTIVIDAD	RESPONSABLE DE: Enlace de SI / Responsable de Incidentes SI	RESPONSABLE DE: Incidentes de seguridad de la Información	DEPENDENCIA	REGISTROS
5. Realizar Cierre del Evento Una vez finalizado el tratamiento del evento y ejecutadas las acciones correspondientes, se procede con su cierre formal en la herramienta de gestión. Finaliza el procedimiento.			Todas las dependencias	Registro en Herramienta de Gestión
6. Registrar Incidente de Seguridad de la Información Cuando un evento es escalado a incidente de seguridad de la información, se realiza un análisis inicial para obtener una comprensión general de lo ocurrido. Es necesario registrar en la herramienta de gestión la siguiente información: **Tipo de incidente.** Seleccionar la categoría correspondiente, según las opciones definidas en la herramienta. **Descripción de la situación.** Se debe incluir un resumen claro y preciso del incidente, con los hechos conocidos hasta el momento. **Responsable.** Persona de la Oficina de Seguridad de la Información encargada de liderar la gestión del incidente. **Fecha de ocurrencia.** Momento en que se produjo el incidente. **Fecha de registro del incidente.** Fecha en la que el incidente fue identificado y oficialmente escalado. **Activos de información afectados.** Activos de información impactados por el incidente. **Riesgos materializados.** Riesgos que se materialización como consecuencia del incidente. **Afectación a datos personales.** Se indica si se vieron comprometidos datos personales. **Equipo de trabajo asignado.** Relación de las personas involucradas en la atención y tratamiento del incidente. **Información adicional.** Cualquier otro dato relevante para la comprensión o tratamiento del incidente.			Oficina de Seguridad de la Información	Registro en Herramienta de Gestión
7. Valorar incidente de seguridad de la información Con el fin de permitir una gestión adecuada de los incidentes de seguridad de la información, es necesario determinar su nivel de prioridad. Esta priorización permitirá atenderlos oportunamente según su criticidad. Para ello, se definen una serie de variables que servirán como base para su evaluación en la herramienta de gestión. **Impacto Actual.** Cantidad de daño que ha provocado el incidente en el momento de ser detectado. **Impacto Futuro.** Cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado. **Nivel de criticidad.** Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados. **Prioridad.** Con base en la valoración del impacto y la criticidad, se determina la prioridad y el tiempo de atención correspondiente para el incidente identificado. Ver numeral 3.4.			Oficina de Seguridad de la información	Registro en Herramienta de Gestión

ACTIVIDAD	RESPONSABLE DE			DEPENDENCIA	REGISTROS
	Incidentes de seguridad de la Información	Jefe de Oficina de Seguridad de la Información	Oficial de protección de datos personales o delegado		
8. ¿Debe escalarse el incidente de seguridad de la información y activarse el Protocolo de Manejo de Crisis? Se debe analizar si el incidente de seguridad de la información afecta negativamente la continuidad de las operaciones de la Entidad y si cumple con los criterios establecidos para la activación de la mesa de de crisis, conforme a los numerales 6.3 y 6.4 del documento OD-PEC-0003 Protocolo de manejo de incidentes e identificación de crisis. Si el incidente cumple con las características para ser escalado como una crisis, se debe continuar con la Actividad 9. Si el incidente no cumple con las características o parámetros para ser escalado como una crisis, se debe continuar con la Actividad 10.				Oficina de Seguridad de la información	Registro en Herramienta de Gestión
9. Escalar el incidente a la mesa de crisis El Jefe de la Oficina de Seguridad de la Información solicita la convocatoria de la Mesa de Crisis conforme a los lineamientos establecidos en el numeral 6.8 del Protocolo de manejo de incidentes e identificación de crisis. - OD-PEC-0003.				Oficina de Seguridad de la información	Registro en Herramienta de Gestión
10. Reporte de Incidente de Seguridad de la Información al ColCERT De acuerdo con la normativa vigente, los responsables de Gestión de Incidentes de Seguridad de la Información de la OSI debe reportar los incidentes clasificados con niveles de criticidad superior, alto, medio y bajo, utilizando la plataforma dispuesta por el MinTIC para tal fin. Véase numeral 3.5 Contacto con autoridades.				Oficina de Seguridad de la información	Registro en Herramienta de Gestión
11. ¿Incidente relacionado con tratamiento de datos personales? Valida con el Grupo de Gestión de Incidentes de Seguridad, si se identifica que el incidente esta relacionado con la afectación de datos personales bajo la responsabilidad de la DIAN. Si el incidente cumple con las características para registrarse en la Plataforma tecnológica de la Superintendencia de Industria y Comercio, se debe notificar al Oficial de Protección de Datos Personales o su delegado. Continuar con la Actividad 12. Si el incidente no cumple con las características para registrarse en la Plataforma tecnológica de la Superintendencia de Industria y Comercio, continuar con la Actividad 13.				Oficina de Seguridad de la información	Registro en Herramienta de Gestión

ACTIVIDAD	RESPONSABLE DE			DEPENDENCIA	REGISTROS
	Oficial de protección de datos personales o delegado	Enlace SI / DGIT / OSI	Incidentes de seguridad de la Información		
12. Reportar incidente a la Superintendencia de Industria y Comercio Si el incidente relacionado con la afectación de datos personales, el Oficial de Protección de Datos Personales o su delegado, debe informar a la Superintendencia de Industria y Comercio (SIC) dentro de un plazo máximo de 15 días hábiles, utilizando la plataforma de la SIC dispuesta para tal fin. Ver numeral 3.5.				Oficina de Seguridad de la información	Plataforma de SIC - Registro Nacional de Bases de Datos.
13. Ejecutar Acciones de contención del incidente El objetivo de estas actividades es implementar medidas para evitar la propagación del incidente, minimizando el riesgo de destrucción de evidencia. Todas las acciones deben registrarse en la herramienta de gestión asignada por la Oficina de Seguridad de la Información. El enlace de Seguridad de la Información, su delegado o el responsable designado será quien registre las actividades, de acuerdo con el procedimiento PR-IIT-0458 de Gestión de Incidentes, cuando el procedimiento sea aplicable.				Todas las Dependencias Oficina de Seguridad de la información Dirección de Gestión de Innovación y Tecnología	Registro en Herramienta de Gestión
14. ¿Es requerida la recolección de evidencia digital en dispositivos electrónicos de la DIAN? Se evalúa la necesidad de recolectar evidencia digital relacionada con el incidente en algún dispositivo electrónico de la DIAN. Si el incidente cumple con las características necesarias para la recolección de evidencia digital, se debe proceder con la Actividad 15. Si el incidente no cumple con las características para la recolección de evidencia digital, se debe continuar con la Actividad 16.				Oficina de Seguridad de la información	Registro en Herramienta de Gestión
15. Realizar tratamiento de evidencia digital en dispositivos electrónicos de la DIAN La Oficina de Seguridad de la Información llevará a cabo las actividades correspondientes al manejo de evidencia digital en los dispositivos electrónicos de la DIAN, de acuerdo con el marco de referencia del Modelo de Seguridad y Privacidad de la Información, Guía 13 - Evidencia Digital, y los estándares internacionales ISO/IEC 27037:2012 e ISO/IEC 27042:2015. Toda la gestión relacionada debe ser debidamente registrada en las herramientas designadas para tal fin.				Oficina de Seguridad de la información	Herramienta de Gestión Herramientas de Informática forense



ACTIVIDAD	RESPONSABLE	DEPENDENCIA	REGISTROS
	Enlace SI / DGIT / OSI		
16. Ejecutar acciones de erradicación del incidente El objetivo de estas actividades es implementar medidas correctivas, de mitigación, remediación o eliminación de vulnerabilidades, fallos o deficiencias que hayan causado el incidente de seguridad de la información en los activos de la DIAN. Todas las acciones deben registrarse en la herramienta de gestión asignada por la Oficina de Seguridad de la Información. El enlace de Seguridad de la Información, su delegado o el responsable designado será quien registre las actividades, de acuerdo con el procedimiento PR-IIT-0458 de Gestión de Incidentes, cuando el procedimiento sea aplicable.		Todas las Dependencias Oficina de Seguridad de la información Dirección de Gestión de Innovación y Tecnología	Registro en la Herramienta de Gestión
17. Ejecutar acciones de recuperación del incidente El objetivo de estas actividades es restaurar los sistemas afectados a su funcionamiento normal, asegurando que se realicen en un entorno controlado y libre de cualquier amenaza remanente. Las acciones de recuperación deben llevarse a cabo con el fin de restablecer la integridad, confidencialidad y disponibilidad de los activos de información de la DIAN. Todas las acciones de recuperación deben ser registradas en la herramienta de gestión asignada por la Oficina de Seguridad de la Información. El enlace de Seguridad de la Información, su delegado o el responsable designado será quien registre las actividades, conforme al procedimiento PR-IIT-0458 de Gestión de Incidentes, cuando el procedimiento sea aplicable.		Todas las Dependencias Oficina de Seguridad de la información Dirección de Gestión de Innovación y Tecnología	Registro en la Herramienta de Gestión
18. ¿Se solucionó el incidente de seguridad de la información? Una vez finalizadas todas las actividades de recuperación, la Oficina de Seguridad de la Información, en conjunto con el dueño del activo de información afectado y/o el equipo técnico de la Dirección de Gestion de Innovación y Tecnología que atendió el incidente, evaluará la solución implementada. Si el incidente cumple con los criterios para considerarlo solucionado, se debe continuar con la Actividad 19. Si el incidente no cumple con los criterios para considerarlo solucionado, se debe regresar a la Actividad 13.		Todas las Dependencias Oficina de Seguridad de la información Dirección de Gestión de Innovación y Tecnología	Registro en la Herramienta de Gestión
19. Registrar las lecciones aprendidas y alimentar la base de conocimiento La Oficina de Seguridad de la Información, en conjunto con el dueño del activo de información afectado y/o el equipo técnico de la Dirección de Gestion de Innovación y Tecnología que atendió el incidente, deberá documentar en la herramienta destinada para tal fin la identificación de las lecciones aprendidas, con el objetivo de reducir el riesgo de reincidencia de incidentes similares. Las lecciones aprendidas deben ser comunicadas al dueño del activo afectado, al equipo técnico de la Dirección de Gestión de Innovación y Tecnología, o a la Oficina de Seguridad de la Información, de acuerdo con la naturaleza del incidente.		Todas las Dependencias Oficina de Seguridad de la información Dirección de Gestión de Innovación y Tecnología	Registro en la Herramienta de Gestión

ACTIVIDAD	RESPONSABLE		DEPENDENCIA	REGISTROS
	Enlace SI / DGIT / OSI	Grupo de incidentes de seguridad de la Información		
20. Definir acciones de mejora La Oficina de Seguridad de la Información, junto con el dueño del activo afectado y/o el equipo técnico que atendió el incidente, deberá identificar e implementar acciones de mejora basadas en las lecciones aprendidas, conforme a los principios de mejora continua y normatividad de la DIAN. Las acciones de mejora derivadas de la identificación de las lecciones aprendidas deben ser comunicadas al dueño del activo de información afectado, al equipo técnico de la Dirección de Gestión de Innovación y Tecnología, o a la Oficina de Seguridad de la Información, dependiendo las acciones propuestas en la acción de mejora.			Todas las Dependencias Oficina de Seguridad de la información Dirección de Gestión de Innovación y Tecnología	Registro en la Herramienta de Gestión
21. Cerrar el incidente de seguridad de la información El Grupo de Gestion de incidentes de seguridad de la información, una vez verificada la solución del incidente, la documentación de las lecciones aprendidas, procederá a cerrar formalmente el incidente en la herramienta de gestión, informando sobre las acciones realizadas al enlace de seguridad de la información. Finaliza el procedimiento.			Oficina de Seguridad de la información	Registro en la Herramienta de Gestión

6.4 Salidas

No de actividad	Salidas	Clientes	Requisitos
5	Reporte de cierre del evento	Servidores públicos DIAN, Ciudadanos, entes externos.	• Solicitud debidamente registrada en la herramienta de gestión. • Informar acciones tomadas.
9	Incidente escalado	Mesa de Crisis	Registrar en el formato FT-PEC-2843 Reporte de incidentes: ▪ La identificación clara y concreta del incidente. ▪ Breve recuento de las acciones registradas en la herramienta de gestión, que no fueron suficientes para mitigar el incidente o sus efectos negativos. ▪ La valoración del incidente, en los factores de afectación de acuerdo con el protocolo OD-PEC-0003.
10	Reporte de incidente	ColCERT	Según numeral 3.5 Contacto con autoridades: • Correo electrónico dirigido a contacto@colcert.gov.co • Registro en la página web del ColCERT.
12	Reporte de incidente	Superintendencia de Industria y Comercio	• Incidente relacionado con la afectación de datos personales. • Registro en el portal web https://rnbd.sic.gov.co/sisi/login el incidente de seguridad con datos personales.
19	Lecciones aprendidas	Oficina de Seguridad de la Información	• Registro en la herramienta de gestión de las actividades que facilitaron o dificultaron la atención del incidente de seguridad de la información.
20	Acciones de mejora	Oficina de Seguridad de la Información	• Registro en la herramienta de gestión las actividades asociadas a la mejora de controles y/o actualizaciones a los riesgos de seguridad de la información.
21	Cierre del incidente	Servidores públicos DIAN	• Notificación indicando que el incidente fue gestionado y cerrado. • Informar sobre acciones tomadas.

7. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	09/05/2025		Versión inicial	Información pública

Elaboró:	Jhon Félix Rivera Gutiérrez Oscar Alberto Casallas Gómez **Elaboración técnica**	Gestor IV Gestor II	Oficina de Seguridad de la Información
	Tito Alejandro Menjura Murcia **Elaboración metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Francisco Andrés Daza Cardona	Jefe de Oficina	Oficina de Seguridad de la Información
Aprobó:	Francisco Andrés Daza Cardona	Jefe de Oficina	Oficina de Seguridad de la Información