1. OBJETIVO

Brindar las directrices que permitan gestionar los eventos e incidentes de seguridad y privacidad de la información o ciberseguridad en todo su ciclo de vida de manera oportuna, conteniendo y mitigando su impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de los activos de información del ICBF, con el fin de reducir las consecuencias causadas por estos y prevenir que no vuelvan a ocurrir.

2. ALCANCE

La gestión de incidentes de seguridad y privacidad de la información o ciberseguridad inicia con el reporte del evento de seguridad y privacidad de la información o ciberseguridad y finaliza con la revisión de las lecciones aprendidas para la mejora continua.

Aplica a nivel de la Sede de la Dirección General, Regional y Centros Zonales (CAIVAS, CESPAS, SRPA).

3. POLÍTICAS DE OPERACIÓN

3.1 Los posibles eventos de seguridad se reportarán a la Mesa de Servicio a través de los canales de atención que el instituto Colombiano de Bienestar familiar tiene dispuestos para ello.

3.2 A continuación, se relacionan las fases por las cuales pasa la gestión de incidentes de seguridad y privacidad de la información o ciberseguridad

Figura 1. Ciclo de vida gestión de incidentes de seguridad y privacidad de la información o ciberseguridad,

Fase 1. Preparación

Esta fase implica estar listo para responder a los eventos o incidentes de seguridad y privacidad de la información o ciberseguridad, se definen los roles y responsabilidades, los flujos, políticas, niveles y cualquier otro aspecto que se considere relevante para una respuesta oportuna y adecuada**.**

Fase 2. Detección e Identificación

En esta fase se descubren la ocurrencia de un evento de seguridad con el objetivo de identificar anomalías o vulnerabilidades que indiquen o evalúen si se trata de un posible incidente de seguridad y privacidad de la información o ciberseguridad

Las alertas o notificaciones de amenazas o vulnerabilidades son reportadas a través de los colaboradores, terceros, proveedores tecnológicos, mesa de servicios y los canales de recepción son el correo electrónico institucional, mesa de ayuda, línea telefónica, Microsoft Teams, entre otros)

Fase 3. Contención y Mitigación

Cuando el evento o incidente de seguridad y privacidad de la información o ciberseguridad se detecta se debe controlar a través de una respuesta inmediata para mitigar el impacto este puede causar a la Entidad.
Es importante implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del evento o incidente y así disminuir los daños a los recursos tecnológicos y la protección de la información evitando la pérdida de la confidencialidad, integridad y disponibilidad de esta.

Fase 4. Erradicación y Recuperación

Después de contener el evento o incidente de seguridad y privacidad de la información o ciberseguridad se debe realizar una erradicación de cualquier rastro dejado por el incidente eliminando la causa raíz y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual se debe restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro. La Recuperación consiste en restaurar y validar los sistemas afectados para asegurar que el incidente se ha resuelto y no existen riesgos adicionales

Fase 5. Lecciones Aprendidas y Mejora Continua

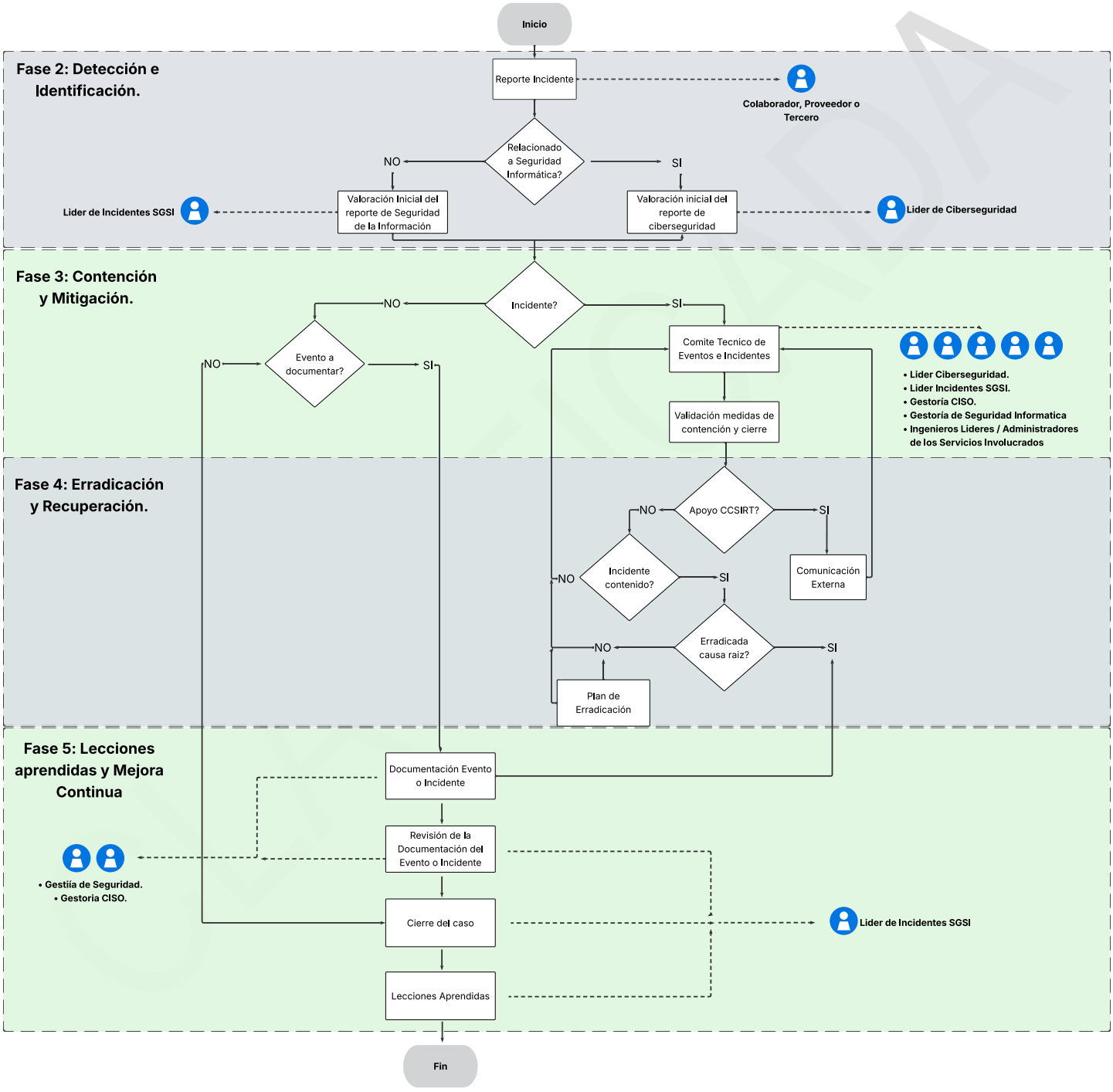
Esta fase se relaciona con la revisión y verificación POST evento o incidente de seguridad y privacidad de la información o ciberseguridad, con el fin de mejorar o fortalecer los controles.

La entidad debería mirar más allá de un solo incidente o vulnerabilidad de seguridad de la información y revisar tendencias/patrones que puedan ayudar a identificar la necesidad de cambio en los controles o en los enfoques de los diferentes vectores de ataque.

El registro adecuado de lecciones aprendidas debe incluir lo siguiente:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el evento o incidente de seguridad y privacidad de la información o ciberseguridad.
- Procedimientos documentados.
- Tomar las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un evento o incidente de seguridad y privacidad de la información o ciberseguridad similar.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los eventos o incidentes de seguridad y privacidad de la información o ciberseguridad en el futuro.

Figura 2. Esquema Gráfico Gestión de Incidentes de Seguridad y privacidad de la Información o ciberseguridad aplicando las fases anteriormente estipuladas



El colaborador que identifique el posible evento o incidente de seguridad debe enviar la mayor cantidad de evidencias (capturas de pantalla, correos electrónicos, fotografías, videos entre otros) a la Mesa de Servicios y copiar vía correo electrónico al líder de Gestión de Incidentes de Seguridad de la Información al momento de efectuar el reporte con el fin de contribuir y agilizar la investigación, con el objeto de determinar si se trata de un incidente de seguridad y privacidad de la información o ciberseguridad

3.3 El líder de la Gestión de incidentes de seguridad puede ser consultado en el micrositio del Eje que se encuentra contenido en la intranet de la entidad en el apartado **"SISTEMA INTEGRADO DE GESTION – EJE DE SEGURIDAD DE LA INFORMACION".**

El Gestor de incidentes de seguridad dependiendo de la clasificación por criticidad o tipo de incidente, será el encargado de notificarlo al Director(a) de Tecnologías de la Información.

3.4 Una vez se reciba el reporte del posible evento o Incidente de seguridad, la mesa de servicio debe realizar la primera categorización en la herramienta de gestión para iniciar con la atención de éste. Se generará un ticket / número de servicio de acuerdo con algunos de los siguientes criterios básicos los cuales determinaran si se está o no frente a un incidente de seguridad y privacidad de la información o ciberseguridad en función a la afectación de la confidencialidad, disponibilidad e integridad de un activo de información de la entidad.

Recibido el reporte a través de la mesa de servicios o por el Líder de la Gestión de Incidentes de Seguridad, y una vez verificado que las características no cumplen con los requisitos para ser clasificado como incidente de seguridad y privacidad de la información o de ciberseguridad —es decir, que no materializa un riesgo—, deberá ser tratado como un evento de seguridad o Incidente tecnológico, en caso de que corresponda.

3.5 Todos los eventos y/o incidentes de seguridad y privacidad de la información o ciberseguridad, deberán estar registrados en la herramienta de gestión con la que cuente el Instituto.

3.6 Una vez clasificado el evento o incidente de seguridad y privacidad de la información o ciberseguridad, deberá ser categorizado de acuerdo con su impacto y urgencia en la herramienta de gestión con la que cuenta el Instituto.

Tabla 1. Impacto vs Valoración

Impacto	Afectación Económica	Reputacional
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.

Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.

IMPACTO	Descripción	Valoración
Catastrófico	**Extremadamente Dañino:** Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad a nivel de: • Pérdidas económicas Superiores a 500 SMLMV. • Afectación de la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país. • Sanciones de Contraloría, Procuraduría y Fiscalía. • Daños totales de la infraestructura de la entidad.	**ALTO**
Mayor	**Dañino:** Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad: • Pérdidas Económicas entre 100 y 500 SMLMV. • Afectación de la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal. • Sanciones de Contraloría, Procuraduría y Fiscalía. • Daños totales de la infraestructura de la entidad.	
Moderado	**Moderado:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. • Pérdidas económicas entre 50 y 100 SMLMV. • Afectación de la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos. Sanciones a nivel de oficina jurídica o control interno. • Daños parciales de la infraestructura de la entidad. • Llamados de atención a nivel organizacional	**MEDIO**
Menor	**Menor:** Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad: • Pérdidas económicas entre 10 y 50 SMLMV. • Afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores. • Sanciones a nivel procesos. • Daños pequeños de la infraestructura de la entidad • Llamados de atención a nivel proceso	**BAJA**
Leve	**Ligeramente Dañino:** Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad: • Pérdidas económicas menores a 10 SMLMV. • Afectación imagen de algún área de la organización • Sanciones a nivel grupo. • Daños pequeños de la infraestructura de la entidad. • Llamados de atención a nivel grupo	

En la **Tabla 1** se muestra el Impacto vs Valoración, se entiende como las consecuencias que puede ocasionar en la organización la materialización de un incidente de seguridad y privacidad de la información o ciberseguridad

Tabla 2 .Nivel de Severidad

NIVEL DE SEVERIDAD	Descripción
Alto	El incidente de seguridad de digital debe atenderse de forma inmediata (0 - 120) minutos
Medio	El incidente de seguridad de digital debe atenderse de forma inmediata (0 - 240) minutos
Bajo	El incidente de seguridad de digital debe atenderse de forma inmediata (0 - 1440) minutos

En la **Tabla 2** se muestran los tiempos sugeridos para iniciar la atención del evento y/o incidente de seguridad y privacidad de la información o ciberseguridad, una vez que son escalados por la mesa de servicios, de acuerdo con su valoración y criticidad.

Para el caso de la atención de incidentes de seguridad y privacidad de la información o ciberseguridad, se han establecido unos tiempos máximos con el fin de gestionarlos adecuadamente de acuerdo con su criticidad e impacto. En la Tabla 2, se establece un acercamiento los tiempos máximos en que deben ser atendidos los incidentes y no al tiempo en el cual el incidente debe ser solucionado, atendiendo esto último a que la solución de estos puede variar dependiendo de la situación.

3.7 El equipo de respuesta que atienden los eventos o incidentes de seguridad y privacidad de la información o ciberseguridad, estarán conformados como mínimo por el propietario y/o custodio del activo, el profesional de la Dirección de Tecnologías de la Información que apoya la Gestión de incidentes de seguridad de la información ICBF, los profesionales del servicio de perimetral o aquellos que tengan a cargo activos o servicios que se vean afectados por el mismo, y si se trata de un tema de privacidad de datos personales participará el Oficial de Datos Personales de la Dirección de Planeación y Control de Gestión.

Para el caso de eventos o incidentes de seguridad y privacidad de la información o ciberseguridad que afecten la disponibilidad, integridad o confidencialidad de un servicio, servidor, base de datos y/o aplicación, el equipo de respuesta estará conformado por el el apoyo a la supervisión del Servicio de Seguridad Informática, el profesional del servicio afectado, el Especialista de TI del proveedor de servicios de TI del servicio afectado, el Gestor Seguridad Informática del proveedor de servicios de TI y el Oficial de Seguridad de la Información del proveedor de servicios de TI y el líder de la Gestión de incidentes de seguridad y privacidad de la información o ciberseguridad

Los equipos que se conformen podrán solicitar información o la participación de colaboradores de otros procesos, especialistas y/u operadores estratégicos requeridos para la atención del evento o incidente de seguridad y privacidad de la información o ciberseguridad.

En caso que un incidente de seguridad y privacidad de la información o ciberseguridad, se considere **CATASTRÓFICO**, se deberá informar al Líder del Eje de Seguridad de la Información (Director(a) de y Tecnologías de la Información) la ocurrencia de dicho incidente, quien deberá informar a la alta gerencia (Dirección y Secretaría General) con el fin de que se analicen los recursos financieros, humanos y tecnológicos correspondientes a la atención de la emergencia, al igual evaluar las alternativas para la contención, erradicación y solución del incidente, a través de la activación del Plan de Continuidad de la Operación del ICBF.

3.8 La recolección de las evidencias se realizará en primera instancia por un agente de soporte en sitio con apoyo del Gestor de incidentes de seguridad de la información, líder de perimetral o proveedor de servicio de TI conforme lo definido en la G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos.

3.9 Las evidencias recopiladas durante la gestión de incidentes de seguridad y privacidad de la información o ciberseguridad deberán preservarse de manera que se garantice su integridad, autenticidad, disponibilidad y confidencialidad, con el fin de evitar su alteración y asegurar su validez y admisibilidad ante instancias disciplinarias, administrativas o judiciales. El almacenamiento de las evidencias se determinará según su naturaleza y clasificación de la información. Por ejemplo, las evidencias derivadas de incidentes asociados a ataques informáticos, tales como registros de auditoría (logs), deberán almacenarse en un repositorio seguro que cumpla con requisitos mínimos de seguridad, incluyendo controles de acceso, trazabilidad, mecanismos de protección contra modificaciones no autorizadas y respaldo periódico. De igual manera se deberá garantizarse la adecuada cadena de custodia, documentando la recolección, traslado, almacenamiento, acceso y disposición final de la evidencia, conforme a los procedimientos internos establecidos.

3.10 En algunos casos la solución del evento o incidente de seguridad y privacidad de la información o ciberseguridad puede ser brindada desde la contención de éste, pero en otros casos requiere la recuperación o restauración del servicio a su estado normal de operación.

3.11 Los incidentes de seguridad y privacidad de la información o ciberseguridad con impacto Mayor o Catastróficos, deben ser documentados en la herramienta de gestión y adicionalmente debe generarse un informe de éste donde se evidencie las actividades realizadas de contención y solución.

3.12 En caso de que se presente un incidente de seguridad y privacidad de la información o ciberseguridad relacionado con base de datos con Datos o información sensible, deberá ser reportado a la Superintendencia de Industria y Comercio, por el Oficial de Datos Personales con previa autorización del Director(a) de Tecnologías de la Información a través del Formato Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio.

3.13 En caso de que se presente un incidente de seguridad y privacidad de la información, o ciberseguridad cuya contención o solución este fuera del alcance de los especialistas DTI del ICBF en cumplimiento al Decreto 338 de 2022, el Director(a) general y o a quien este delegue de la DTI, lo reportará a los entes externos que correspondan. A continuación, se mencionan los canales para reportar los incidentes:

- CSIRT Gobierno: Equipo de Respuesta a Incidentes de MINTIC csirtgob@mintic.gov.co
- COLCERT: Centro de respuesta a emergencias cibernéticas malware@colcert.gov.co
- Centro Cibernético de la Policía: Equipo de respuesta a incidentes y delitos informáticos https://caivirtual.policia.gov.co/

3.14 En caso de haber realizado el análisis de un incidente y su solución supera los tiempos objetivos de recuperación de los servicios tecnológicos, se informará a, los especialistas encargados de los servicios de tecnología involucrados y al Director(a) de Tecnologías de la Información con el fin que se activen los planes de contingencia, continuidad de la operación o continuidad de la operación tecnológica.

3.15 El profesional de la Dirección de Tecnologías de la Información que lidera la Gestión de Incidentes de Seguridad de la Información convocará una mesa de trabajo donde se dará a conocer los incidentes presentados a los profesionales que apoyan las gestiones de Activos de Información y Riesgos de seguridad y privacidad de la información, ciberseguridad y continuidad del negocio seguridad de la información, con el fin de realizar los ajustes necesarios en cada una de sus gestiones. Para el caso de la Gestión de Riesgos, se debe revisar en conjunto con la gestión de incidentes si se trata de un nuevo riesgo el cual se ha materializado por medio del incidente y si es el caso, se deberá registrar en la matriz de riesgos del proceso o regional afectado. En el marco de la gestión de activos de información, se deberá revisar y, de ser necesario, actualizar la clasificación y el nivel de criticidad del activo. En caso de que el activo no se encuentre previamente identificado, deberá incorporarse formalmente en la matriz o inventario de activos de información, asegurando su adecuada valoración, asignación de responsable y definición de controles correspondientes.

3.16 El profesional de la Dirección de Tecnologías de la Información que apoya la Gestión de incidentes de seguridad de la información informará las lecciones aprendidas al profesional que apoya la Gestión de Cambio y Cultura con el fin de fortalecer e interiorizar mediante diferentes estrategias y generar conciencia en los colaboradores.

3.17 La Entidad divulga a los colaboradores de las diferentes medidas de protección, buenas prácticas y recomendaciones que deben adoptar con relación a la seguridad, ciberseguridad y privacidad de la información.

3.18 Una vez se materialice un incidente de seguridad y privacidad de la información o ciberseguridad se deberá reportar a las gestiones de riesgos y de activos de información para que se incluya en

la matriz de riesgos de ICBF y se incluya o se recalifique el activo de información y/o del proveedor, así como también se proceda a revisar el activo de información en su clasificación y nivel de criticidad

3.19 El F3.P25.GTI Formato Matriz Registro de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad es el instrumento para la consolidación, control y trazabilidad de los eventos y/o incidentes de seguridad de la información identificados en la Entidad, en cumplimiento de los controles establecidos en la ISO/IEC 27001:2022, en especial aquellos relacionados con la gestión de incidentes de seguridad de la información. En esta matriz se deberá registrar cada evento e incidente, fortaleciendo el inventario institucional de incidentes y facilitando su análisis, tratamiento y seguimiento, conforme a los lineamientos definidos por MinTIC para la gestión de incidentes y ciberseguridad en el sector público. Todos los registros deberán estar debidamente documentados y almacenados en la ruta oficial definida para la custodia de esta información, garantizando su integridad, confidencialidad, disponibilidad y disponibilidad como evidencia para entes de control o auditorías internas y externas.

4. DESCRIPCIÓN DE ACTIVIDADES

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		Inicio		
1	Reportar evento de Seguridad y privacidad de la información o ciberseguridad	Reportar el posible evento de Seguridad y privacidad de la información o ciberseguridad según Política de operación 3.1 ¿El reporte es realizado por un analista del SOC del proveedor de servicios de TI a través del P11.GTI Procedimiento de gestión de eventos y alertas? SI: Pasa a la actividad 5. NO: Pasa a la actividad 2.	Directores, subdirectores, Jefes de Oficina, Asesores, Profesionales, Técnicos y Asistenciales de la Sede de la Dirección General, Regional y Centro Zonal Profesional de la Dirección de Tecnologías de la Información	Correo electrónico Llamada telefónica Ticket generado en el módulo de autoservicio de la herramienta de gestión de servicios
2	Registrar evento de Seguridad y privacidad de la información o ciberseguridad	Realizar la categorización y registro del posible incidente de seguridad y privacidad de la información o ciberseguridad. Aplicar Política de operación 3.2 ¿Es un posible incidente de seguridad y privacidad de la información o ciberseguridad?	Profesional de la Dirección de Tecnologías de la Información	Herramienta de gestión de servicios

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		SÍ: pasa a la actividad 3. NO: activar el P8.GTI Procedimiento de gestión de incidentes de tecnologías de la información y finalizar el procedimiento.		
3	Escalar el evento o incidente para su análisis y clasificación	Realizar el escalamiento al Profesional de la DTI que apoya la gestión de incidentes de seguridad y privacidad de la información o ciberseguridad para su análisis y clasificación.	Profesional de la Dirección de Tecnologías de la Información	Herramienta de gestión de servicios
4	Gestionar el evento y/o incidente de seguridad y privacidad de la información o ciberseguridad	Analizar y clasificar si el evento es o no, un posible incidente de seguridad y privacidad de la información o ciberseguridad de acuerdo con las políticas de operación 3.3 y 3.4 ¿Es realmente un incidente de privacidad de la información o ciberseguridad? SÍ: Pasa a la actividad 5. NO: Si se declara un evento de seguridad se generará el reporte y se finalizará el procedimiento. Para los que no se declaren como incidente o evento, se devuelve a la mesa de servicio para su reasignación y recategorización,	Profesional de la Dirección de Tecnologías de la Información de la SDG designado para la Gestión de Incidentes de Seguridad de la Información	Herramienta de gestión de servicios
5	Seleccionar los equipos de respuesta a incidentes de seguridad y privacidad de la información o ciberseguridad	Informar a los implicados para la solución del incidente y conformar el equipo, según la política de operación 3.5.	Director(a) de Tecnologías de la Información. Profesional de la Dirección de Tecnologías de la Información de la SDG designado para la Gestión de incidentes de seguridad Profesional de la Dirección de Tecnologías de la Información de Seguridad y Ciberseguridad	Correo electrónico, memorando, verbal o con posterior documentación

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
6	Analizar, detectar e identificar el incidente de seguridad y privacidad de la información o ciberseguridad	El equipo de respuesta a incidentes de seguridad y privacidad de la información, o ciberseguridad realizará el análisis pertinente con el fin de identificar la causa o causas que dieron origen al incidente y determina si se informa al gestor de Continuidad del Negocio. ¿Se informa al Líder de la Gestión de Continuidad del Negocio? Si: Se aplica la política de operación 3.5.y pasa a la actividad 7. No: pasa a la actividad 7	Profesional de la Dirección de Tecnologías de la Información de la Sede Dirección General designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de la Información de Sistemas de Información Profesional del Grupo de Planeación y Tecnología de la Regional	Correo electrónico o video llamada F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad
7	Contener y mitigar el incidente de seguridad y privacidad de la información o ciberseguridad	El equipo de respuesta a incidentes de seguridad y privacidad de la información o ciberseguridad realizará todas aquellas tareas necesarias con el fin de contener el incidente y así minimizar su impacto. ¿Se logró contener y mitigar el incidente de seguridad y privacidad de la información o ciberseguridad? Si: pasa a la actividad 8 No: pasa a la actividad 6 y si la contención del incidente esta fuera del alcance del ICBF se da cumplimiento a la política de operación 3.12.	Profesional de Tecnologías de la información SDG designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de la Información de Sistemas de Información de la SDG Profesional del Grupo de Planeación y Tecnología de la Regional	Correo electrónico o video llamada F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad
8	Erradicar la causa raíz del incidente de seguridad y privacidad de la información o ciberseguridad	El equipo de respuesta a incidentes de seguridad y privacidad de la información o ciberseguridad o seguridad digital realizará todas aquellas tareas necesarias con el fin de erradicar la causa raíz detectada. ¿Se logró erradicar la causa raíz? Si: pasa a la actividad 9	Profesional de Tecnologías de la SDG designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de Sistemas de Información	Herramienta de gestión de servicios F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		No: pasa a la actividad 6 y si la erradicación de la causa raíz del incidente esta fuera del alcance del ICBF se da cumplimiento a la política de operación 3.12.	Profesional del Grupo de Planeación y Tecnología de la Regional	
9	Solucionar y recuperar el incidente de seguridad y privacidad de la información o ciberseguridad	El equipo de respuesta a incidentes de seguridad y privacidad de la información o ciberseguridad realizará todas aquellas tareas necesarias con el fin de solucionarlo. Ver política de operación 3.8 ¿Se logró solucionar el incidente? Si: pasa a la actividad 10. No: activar el P7.GTI Procedimiento de Gestión de Problemas de Tecnología y finaliza procedimiento.	Profesional de la Dirección de Tecnologías de la información de la SDG designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información del Servicio de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de la Información de Sistemas de Información Profesional del Grupo de Planeación y Tecnología de la Regional	Herramienta de gestión de servicios
10	Documentar las evidencias del incidente de seguridad y privacidad de la información o ciberseguridad	Recopilar y organizar las evidencias producto de la investigación del incidente siguiendo los lineamientos estipulados en la Guía de Recolección de Evidencias de Elementos Informáticos G5.GTI. En la actividad participa el profesional que apoya la gestión de incidentes de seguridad y privacidad de la información o ciberseguridad.	Profesional de la Dirección de Tecnologías de la información SDG designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información del Servicio de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de la Información de Sistemas Ide Información Profesional del Grupo de Planeación y Tecnología de la Regional	F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad F3.P25.GTI Formato Matriz Registro de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad Herramienta de gestión de servicios
11	Proteger las evidencias	Guardar la información recolectada según la Política de operación 3.6	Profesional de la Dirección de Tecnologías de la Información de la SDG designado para la Gestión de Incidentes de Seguridad de la Información	F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		La actividad la ejecuta el profesional que apoya la gestión de incidentes de seguridad y privacidad de la información o ciberseguridad	Profesional de la Dirección de Tecnologías de la Información del Servicio de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de Sistemas de Información Profesional del Grupo de Planeación y Tecnología de la Regional	
12	Documentar incidentes y/o eventos de seguridad y privacidad de la información o ciberseguridad	Documentar el evento o incidente de seguridad y privacidad de la información o ciberseguridad presentado según las políticas de operación 3.10. y/o 3.11.	Profesional de la Dirección de Tecnologías de la Información de la SDG designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información del Servicio de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de Sistemas de Información Profesional del Grupo de Planeación y Tecnología de la Regional	F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad F3.P25.GTI Formato Matriz Registro de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad Registro en el aplicativo de la SIC (Si el incidente está relacionado con datos personales)
13	Informar incidente de seguridad y privacidad de la información o ciberseguridad a entes de control o autoridades competentes.	Con base a la evidencia y documentación generada, se evaluará si la situación presentada se debe informar a entes de control o autoridades competentes. ¿Es requerido enviar reporte del incidente de seguridad y privacidad de la información o ciberseguridad a entes de control o autoridades competentes?	Director(a) de Tecnologías de la Información designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Dirección de Tecnologías de la Información de la SDG.	F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		Si: enviar reporte del posible incidente de seguridad y privacidad de la información o ciberseguridad, según Política de Operación 3.12 y pasar a la actividad 14. No: Pasa a la actividad 14.		
14	Revisar respuesta a incidente de seguridad y privacidad de la información o ciberseguridad	Se realiza una revisión de la respuesta y solución dada al incidente de seguridad de acuerdo con los lineamientos establecidos en la política de operación 3.7.	Profesional de la Dirección de y Tecnologías de la SDG designado para la Gestión de Incidentes Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información del Servicio de Seguridad y Ciberseguridad	F1.P10.GTI Formato Postulación Conocimiento Tecnológico
15	Notificar a los afectados	Informar o notificar a los afectados sobre incidentes que afecten la confidencialidad, integridad o disponibilidad de su información, así como de las medidas adoptadas para la remediación del incidente colocando como adjunto al caso generado en la herramienta de gestión de incidentes de la entidad.	Profesional de la Dirección de Tecnologías de la información de la SDG designado para la Gestión de Incidentes de Seguridad de la Información	Herramienta gestión de servicios
16	Revisar las lecciones aprendidas para la mejora continua	Realizar una revisión de los controles de seguridad POST incidente de seguridad y privacidad de la información o ciberseguridad.	Profesional de la Dirección de Tecnologías de la información de la SDG designado para la Gestión de Incidentes de Seguridad de la Información Profesional de la Dirección de Tecnologías de la Información del Servicio de Seguridad y Ciberseguridad Profesional de la Dirección de Tecnologías de Sistemas de Información Profesional del Grupo de Planeación y Tecnología de la Regional	F1.P25.GTI Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad
		Fin		

P.C.: Punto de Control

5. RESULTADO FINAL

Incidente de seguridad y privacidad de la información o ciberseguridad atendido, tratado y documentado.

6. DEFINICIONES

- **Activo Crítico:** son aquellos elementos o componentes que hacen parte de la infraestructura crítica.
- **Activo de Información:** se denomina activo a aquello que tiene valor para la organización y por lo tanto debe protegerse.
- **Analista de Mesa de Servicio:** recibe la información de los Colaboradores del ICBF, registra los casos en la herramienta de mesa de servicio y es el primer contacto para la gestión de los incidentes de seguridad de la información.
- **Ataque Informático:** conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.
- **Bases de Datos:** conjunto organizado de datos personales que sea objeto de tratamiento. Para el caso del ICBF, son bases de datos toda la información que repose en Sistemas de Información Oficiales y que sean objeto de la Política de Tratamiento de Datos Personales ICBF.
- **CCOC:** comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.
- **Ciberataque:** es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que ataquen a sistemas de información como lo son infraestructuras, redes computacionales, o bases de datos que están albergadas en servidores remotos. Estas maniobras son realizadas por medio de actos maliciosos usualmente originados de fuentes anónimas y direcciones que no pueden ser rastreadas.
- **Ciberespacio:** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias.
- **Ciberincidente:** cualquier acto malicioso o evento sospechoso que: comprometa, o intente comprometer la Seguridad del perímetro electrónico, la Seguridad del primero físico o un activo crítico.
- **Ciberseguridad:** según ISACA es el proceso de proteger activos de información por medio del tratamiento de amenazas para información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

- **Código Malicioso:** conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.
- **COLCERT:** por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado Colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.
- **Contención de un Incidente:** son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.
- **CSIRT:** por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
- **Dato Personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales, tales como nombre, apellido, cédula, edad, color de ojos, estatura, fotografía o video de la persona, entre otros. Estos datos se pueden clasificar como dato público, sensible y semiprivado.
- **Dato Público:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al nombre, estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato Semiprivado:** datos que son de carácter privado, este tipo de datos sólo le interesan al titular y a un grupo determinado de personas. (Ej. Datos financieros, crediticios).
- **Datos Sensibles:** son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud, a la vida sexual, videos, fotografías, datos biométricos (huella dactilar, iris del ojo, pulsaciones cardiacas entre otros).
- **Denegación del Servicio:** conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema o servicio informático.
- **Entorno Digital:** ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas

tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

- **Entorno Digital Abierto:** entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).
- **Equipo de Respuesta a Incidentes:** conformado por Colaboradores del ICBF y/o terceros asociados (operadores estratégicos) que cuentan con las habilidades y competencias para tratar los incidentes de seguridad de la información durante el ciclo de vida de éstos.
- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2009].
- **Evento de seguridad**: es cualquier ocurrencia observable que sea relevante para la seguridad de la información. Esto puede incluir intentos de ataques o fallos que descubren vulnerabilidades de seguridad existentes. [ISO/IEC 27000:2018].
- **Incidente de Seguridad Informática:** una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas del estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.
- **Incidente de ciberseguridad:** ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable**.**
- **Infraestructura Crítica (IC)**: son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.
- **NITS:** es el proceso de proteger información a través de la prevención, detección y respuesta hacia ataques.
- **Oficial de Datos:** en el ICBF es la Dirección de Planeación y Control de Gestión
- **Oficial de Seguridad de la Información:** designación dada a una persona para cumplir con los temas relacionados frente a la seguridad de la información.
- **Phishing**: es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.
- **Plan de Continuidad de la Negocio (BCP. Business Continuity Plan):** actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- **Ransomware:** piezas de código desarrolladas por atacantes informáticos para secuestrar información de los equipos infectados a través de técnicas criptográficas y posteriormente solicitar el pago de rescate para la recuperación de información.
- **RNBD:** por sus siglas Registro Nacional de Bases de datos

- **Servicio Esencial:** el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. Adaptación Ley 8/2011-Gobierno de España.
- **SIC:** por sus siglas Superintendencia de Industria Comercio.
- **SOC:** Centro de Operaciones de Seguridad donde se monitorea el estado de la seguridad informática a través de la gestión temprana de alertas y eventos.
- **Suplantación de Identidad:** todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.
- **SDG:** Sede de la Dirección General.
- **Vulnerabilidad:** es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

7. DOCUMENTOS DE REFERENCIA

- Resolución 3248 del 2 de Julio de 2025 “Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Ciberseguridad y Continuidad de la Operación”, o la norma que la modifique, sustituya o derogue.
- Resolución 11980 del 30 de diciembre de 2019 “Por la cual se adopta el modelo de Planeación y Sistema Integrado de Gestión del ICBF “.
- Resolución 6659 del 15 de diciembre de 2020 “Por la cual se modifica el modelo de Planeación y sistema Integrado de Gestión del ICBF “.
- Decreto 1430 del 24 de diciembre de 2025 “Por la cual se modifica la estructura del Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras“.
- G3.MI Guía de Gestión de Riesgos y Peligros
- Resolución 02277 de 2025 “Por medio de la cual el Ministerio TIC actualiza el Modelo de Seguridad y Privacidad de la Información”
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital”
- CONPES 4144 de 2025: Política Nacional de Inteligencia Artificial
- Norma ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.
- G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos
- G3.MI Guía Gestión de Riesgos
- P3.GTI Procedimiento Gestión de Cambios de Emergencia de Tecnologías de la Información
- P4.GTI Procedimiento Gestión de Cambios de Tecnologías de la Información
- P10.GTI Procedimiento Gestión del Conocimiento Tecnológico
- P11.GTI Procedimiento de Gestión de Eventos y Alertas
- G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos

8. RELACIÓN DE FORMATOS

CÓDIGO	NOMBRE DEL FORMATO
F9.P1.MI	Formato Acta de Reunión o Comité
F1.G5.GTI	Formato Acta de Recolección de Evidencias Digitales
F1.P10.GTI	Formato Postulación Conocimiento Tecnológico
F1.P25.GTI	Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad
F2.P25.GTI	Formato Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio
F3.P25.GTI	Formato Matriz Registro de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
27/12/2024	V1	Se cambia el nombre de Dirección de Información y Tecnología por Dirección de Tecnologías de la Información conforme al Decreto 1430 del 24 de diciembre de 2025 de estructura SDG del ICBF. Se ajusta la gráfica Esquema Gráfico Gestión de Incidentes de Seguridad y privacidad de la Información o ciberseguridad. Se incluye en el ítem 3.19 el Formato Matriz Registro de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad, con el fin de llevar un documento controlado del inventario de registros de incidentes y/o eventos de seguridad. Se ajusta el item documentos de referencia. Se incluye en el ítem 8. relación de formatos, el Formato Matriz Registro de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad.