1. OBJETIVO

Brindar las directrices que permitan gestionar los incidentes de seguridad digital de manera oportuna, mitigando su impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de los activos de información del ICBF.

2. ALCANCE

La gestión de incidentes de seguridad digital inicia con la identificación y reporte de un evento, continua con el análisis y solución y finaliza con la notificación a los afectados.

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 digital se reportarán a la Mesa de Servicio a través de los canales de atención dispuestos para ello.

El colaborador que identifique el posible evento de seguridad digital 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 atención e investigación.

El líder de la Gestión de Incidentes de Seguridad de la Información 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 de la Información dependiendo de la clasificación por criticidad o tipo de incidente, será el encargado de notificarlo al Director de Información y Tecnología.

3.2 Una vez se reciba el reporte del posible evento de seguridad digital, la mesa de servicio debe realizar la primera categorización en la herramienta que se maneja para iniciar con la atención de éste, donde 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 digital en función a la afectación de la confidencialidad, disponibilidad e integridad de un activo de información de la entidad:

- Hubo daño o pérdida de información física o digital.
- Hubo fuga y/o robo de información física o digital.
- Hubo robo de credenciales o información mediante un ataque de ingeniería social.

- Se presentó modificación no autorizada de la información.
- Se presentó un comportamiento anormal del computador y/o sistema de información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida o robo de un activo de información.
- Hubo presencia de código malicioso “Malware”, “Ransomware”.
- Se presentó una denegación del servicio.
- Se presentó un ciberataque.
- Se presentó Fallas de Infraestructura Tecnológica que afecte la confidencialidad, disponibilidad e integridad de la información.
- Uso indebido de imagen institucional.
- Cuando se presente pérdida de confidencialidad, integridad o disponibilidad de los activos de información relacionados en la matriz de activos de la Entidad por causa de un evento o situación.

Cuando se recibe el reporte a través de la mesa de servicios o por el Líder de la Gestión de Incidentes de Seguridad de la Información y éste ha sido verificado y sus características no cumplen con las requeridas para ser clasificado como incidente, es decir, no materializa un riesgo, deberá ser tratado como un evento de seguridad digital (toda situación que represente un riesgo potencial pero que no provoca daños o riesgos para los activos y para las operaciones de la Entidad) o en su defecto como un incidente tecnológico.

3.3 Todos los eventos y/o incidentes de seguridad digital deberán estar registrados en la herramienta de gestión con la que cuente el Instituto.

3.4 Una vez clasificado el evento y/o incidente de seguridad digital, 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 digital.

Tabla 2: Urgencia

URGENCIA	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, una vez que son escalados por la mesa de servicios, de acuerdo con su valoración.

Para el caso de la atención de incidentes de seguridad digital, 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.

3.5 El equipo de respuesta que atienden incidentes de seguridad digital, estarán conformados como mínimo por el propietario y/o custodio del activo, el profesional de la Dirección de Información y Tecnología que apoya la Gestión de Incidentes de Seguridad de la Información del ICBF y demás profesionales de las Subdirecciones de Recursos Tecnológicos o Sistemas Integrados de Información que tengan a cargo activos o servicios que se vean afectados por el mismo, además del Oficial de Datos Personales de la Dirección de Planeación y Control de Gestión en el caso que la información o base de datos objeto del incidente reportado, contengan datos personales.

Para el caso de incidentes de seguridad digital 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 propietario, el profesional de la Subdirección de Recursos Tecnológicos que apoya la supervisión del Servicio de Seguridad Informática, el profesional de la Subdirección de Recursos Tecnológicos que apoya la supervisión 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 de la Información.

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 incidente de seguridad.

En caso que un incidente de seguridad digital se considere **CATASTRÓFICO**, se deberá informar al Líder del Eje de Seguridad de la Información (Director(a) de Información y Tecnología) 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.

3.6 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 o proveedor de servicio de TI conforme lo definido en la G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos.

3.7 Se deben conservar las evidencias recopiladas, con el fin de reducir la probabilidad de que éstas se modifiquen después y sean consideradas no admisibles ante un ente judicial. Dependiendo de la evidencia que se genere en el tratamiento del incidente, se determinará el lugar en dónde se conservarán, por ejemplo: las evidencias producto de un incidente de seguridad digital asociado a un ataque informático (Logs de auditoría) se almacenarán en un repositorio, el cual deberá cumplir unos requisitos mínimos de seguridad (Se determinarán de acuerdo con la clasificación de la información) para garantizar la integridad, disponibilidad y confidencialidad de ésta.

3.8 Las soluciones a los incidentes de seguridad que el equipo de respuesta a incidentes y/o el profesional de la Dirección de Información y Tecnología que lidera la Gestión de Incidentes de Seguridad de la Información, consideren que deben postularse a la base de datos de conocimiento, se documentarán de acuerdo con lo establecido en el "P10.GTI Procedimiento Gestión del Conocimiento Tecnológico".

3.9 En algunos casos la solución del incidente puede ser dada desde la contención de éste, pero en otros requiere la recuperación o restauración del servicio a su estado normal de operación.

3.10 Los incidentes de seguridad digital 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.

3.11 En caso de que se presente un incidente de seguridad digital 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 a través del F2.P5.GTI Formato Reporte Incidentes Bases de Datos Personales Superintendencia de Industria y Comercio.

3.12 En caso de que se presente un incidente de Seguridad Digital cuya contención o solución este fuera del alcance de los especialistas ICBF en cumplimiento al Decreto 338 de 2022, el Director general y/o el Líder del **SGSI** o a quien este delegue 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/

3.13 En caso de haber realizado el análisis del 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 de Información y Tecnología como líder del Sistema de Gestión de Seguridad de la Información **SGSI** con el fin que se activen los planes de contingencia.

3.14 El profesional de la Dirección de Información y Tecnología que apoya 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 de la Dirección de Información y Tecnología que apoyan las gestiones de Activos de Información y Riesgos de seguridad y privacidad de la información, seguridad digital 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.

3.15 El profesional de la Dirección de Información y Tecnología que apoya la Gestión de Incidentes de Seguridad de la Información informará las lecciones aprendidas al profesional de la Dirección de Información y Tecnología que apoya la Gestión de Cambio y Cultura con el fin de fortalecer e interiorizar mediante diferentes estrategias y generar conciencia en los colaboradores.

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

4. DESCRIPCIÓN DE ACTIVIDADES

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		Inicio		
1 P.C	Reportar evento de Seguridad Digital identificado.	Reportar el posible evento de seguridad digital 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. Colaboradores del ICBF. Analista SOC del proveedor de servicios TI	Correo electrónico Llamada telefónica Tiquete generado en el módulo de autoservicio de la herramienta de gestión de servicios.
2	Registrar evento de Seguridad y privacidad de la información	Realizar la categorización y registro del posible incidente de seguridad digital Aplicar Política de operación 3.2 ¿Es un posible incidente de seguridad digital? 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.	Analista de mesa de Servicio	Herramienta de gestión de servicios
3	Escalar el evento o incidentes para su análisis y clasificación.	Realizar el escalamiento al Profesional de la Dirección de Información y Tecnología que apoya la gestión de	Analista del operador de la mesa de Servicio	Herramienta de gestión de servicios

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		Incidentes de Seguridad de la Información para su análisis y clasificación.		
4 P.C	Gestionar el evento y/o incidente de seguridad digital.	Analizar y clasificar si el evento es o no, un posible incidente de seguridad digital de acuerdo con las políticas de operación 3.3 y 3.4 ¿Es realmente un incidente de seguridad digital? SÍ: Pasa a la actividad 5. NO: Si se declara un evento de seguridad digital 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, activando el P8.GTI Procedimiento de gestión de incidentes de tecnología de la información y finaliza el procedimiento.	Profesional de la Dirección de Información y Tecnología 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 digital.	Informar a los implicados para la solución del incidente de seguridad digital y conformar el equipo, según la política de operación 3.5.	Director de Información y Tecnología. Profesional de la Dirección de Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información. Analista SOC del proveedor de servicios TI	Correo electrónico, memorando, verbal o con posterior documentación.
6 P.C	Analizar el incidente de seguridad digital.	El equipo de respuesta a incidentes de seguridad digital 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 Información y Tecnología de la Sede Dirección General designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG.	Correo electrónico o video llamada F1.P5.GTI Formato Informe Incidente de Seguridad Digital

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
			Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	
7 P.C	Contener incidente de seguridad digital	El equipo de respuesta a incidentes de seguridad digital realizará todas aquellas tareas necesarias con el fin de contener el incidente y así minimizar su impacto. ¿Se logró contener el incidente de seguridad digital? 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 la Dirección de Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	Correo electrónico o video llamada F1.P5.GTI Formato Informe Incidente de Seguridad Digital
8 P.C	Erradicar la causa raíz del incidente de seguridad digital.	El equipo de respuesta a incidentes de 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 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 de la Dirección de Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	Herramienta de gestión de servicios F1.P5.GTI Formato Informe Incidente de Seguridad Digital

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
9 P.C	Solucionar el incidente de seguridad digital.	El equipo de respuesta a incidentes de seguridad digital 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 Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	Herramienta de gestión de servicios
10	Documentar las evidencias del incidente de seguridad digital	Recopilar y organizar las evidencias producto de la investigación del incidente de seguridad digital 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 Digital	Profesional de la Dirección de Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales F1.P5.GTI Formato Informe Incidente de Seguridad Digital Herramienta de gestión de servicios.
11	Proteger las evidencias.	Guardar la información recolectada según la Política de operación 3.6 La actividad la ejecuta el profesional que apoya la gestión de incidentes de Seguridad Digital	Profesional de la Dirección de Información y Tecnología 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
			Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	
12	Documentar incidentes de seguridad digital	Documentar el incidente de seguridad digital presentado según las políticas de operación 3.10. y/o 3.11.	Profesional de la Dirección de Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Profesional del Grupo de Planeación y Sistemas de la Regional. Profesional de la Subdirección de Sistemas Integrados de Información de la SDG. Especialista, Profesional o Técnico del proveedor de servicios de TI. Profesional del Grupo de Planeación y Sistemas de la Regional	F1.P5.GTI Formato Informe Incidente de Seguridad Digital Registro en el aplicativo de la SIC (Si el incidente está relacionado con datos personales)
13 P.C	Informar incidente de seguridad Digital 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.	Director de la Dirección de Información y Tecnología designado para la Gestión de Incidentes de	F1.P5.GTI Formato Informe Incidente de Seguridad Digital

No	Nombre de la Actividad	Descripción de la actividad	Responsable	Registro
		¿Es requerido enviar reporte del incidente de seguridad a entes de control o autoridades competentes? Si: enviar reporte del posible incidente de seguridad digital según Política de Operación 3.12 y pasar a la actividad 14. No: Pasa a la actividad 14.	Seguridad de la Información. Profesional de la Dirección de Información y Tecnología de la SDG.	F1.G5.GTI Formato Acta de Recolección de Evidencias Digitales
14	Revisar respuesta a Incidentes de Seguridad Digital	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 Información y Tecnología de la SDG designado para la Gestión de Incidentes Seguridad de la Información. Profesional de la Subdirección de Recursos Tecnológicos de la SDG Gestor de seguridad informática del proveedor de servicios de TI Oficial de seguridad de la información del proveedor de servicios de TI	F1.P10.GTI Formato Postulación Conocimiento Tecnológico
15	Notificar a los afectados	Informar o notificar a los afectados sobre incidentes que afecten la confidencialidad o integridad 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 Información y Tecnología de la SDG designado para la Gestión de Incidentes de Seguridad de la Información.	Herramienta gestión de servicios
		Fin		

P.C.: Punto de Control

5. RESULTADO FINAL

Incidente de seguridad digital 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 Digital:** un 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 seguridad digital:** 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
- **Seguridad digital:** es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas.
- **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.
- **SRT:** Subdirección de Recursos Tecnológicos adscrita a la Dirección de Información y Tecnología.
- **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

- Decreto 338 de 2022
- GTC-ISO/IEC 27035
- NTC-ISO/IEC 27001
- ISO/IEC 27032
- ISO/IEC 27000
- Documento CONPES 3854
- NIST SP 800-53
- 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
F1.P5.GTI	Formato Informe Incidente de Seguridad Digital
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

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
10/05/2023	P5.GTI V8	Se ajusta la descripción en el objetivo y alcance. Se adiciona la política de operación 3.6, y se ajusta la numeración de las demás políticas. Se ajusta el contenido de las políticas de operación 3.2, 3.4, 3.5, 3.7, 3.8, 3.10, 3.12, 3.14, 3.15 y 3.16. Se ajustan las actividades 1, 2, 4, 5, 6, 7, 8, 9, 11, 12, 13 y 14 descritas en el numeral “4. DESCRIPCIÓN DE ACTIVIDADES., dado que se incorpora el concepto de seguridad digital, se ajusta el nombre de informe de seguridad digital y se elimina en las que aplicaba el acta de reunión. En el numeral 6. DEFINICIONES se agregan las definiciones de “Incidente de seguridad digital” y “Ciberseguridad”, así mismo se ajusta la definición de “Seguridad Digital”. Se ajusta el nombre del Procedimiento Gestión de Incidentes de Seguridad de la Información por el Procedimiento Gestión de Incidentes de Seguridad Digital.

Fecha	Versión	Descripción del Cambio
		Se ajusta el nombre del formato “F1.P5.GTI Formato Informe Incidente de Seguridad de la Información¨ por el F1.P5.GTI Formato Informe Incidente de Seguridad Digital”. Se adiciona en el numeral “7. DOCUMENTOS DE REFERENCIA” el Decreto 338 de 2022 “Por el cual se adiciona el Título 21 a la Parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”.
23/12/2020	P5.GTI V7	Se actualiza nombre del procedimiento de “Procedimiento Gestión de Incidentes de Seguridad de la Información” a "Procedimiento gestión de incidentes de seguridad digital" Se actualiza definición de incidente de seguridad digital y privacidad en las definiciones del procedimiento. Se ajusta título del concepto a plan de continuidad del negocio acorde a sus siglas en inglés BCP. Se elimina 5482_G21 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Relacionarlo en el control de cambios. 1. Objetivo: Se adopta el término seguridad digital y privacidad reemplazando el uso de seguridad de la información, seguridad informática y ciberseguridad acorde con la política de gobierno digital. Se incluye el uso del concepto de evento de seguridad el cual es el primer estado de una situación que posterior a su evaluación si cumple con las condiciones de un incidente de seguridad digital y privacidad pasa a ser clasificada como tal. 3.1 se actualizan los canales para reporte de incidentes de seguridad de la información y se complementa el párrafo con: "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 atención e investigación." 3.2 Se complementa el párrafo con: •Cuando se presente indisponibilidad de los activos de información relacionados en la matriz de activos de información de la entidad por causa de evento un evento o situación que afecte su funcionamiento o acceso. Cuando se recibe el reporte a través de la mesa de ayuda o por el líder de gestión de incidentes de seguridad de la información y éste ha sido verificado y sus características no cumplen con las requeridas para ser clasificado como incidente, es decir, no materializa un riesgo, deberá ser tratado como un evento de seguridad digital. Entendiendo por evento de seguridad digital, toda situación que represente un riesgo potencial pero que no provoca daños o riesgos para los activos y para las operaciones de seguridad digital. 3.3 Se cambia incidentes de seguridad de la información por evento y/o incidentes de seguridad digital. 3.4 Se cambia incidentes de seguridad de la información por evento y/o incidentes de seguridad digital. Se agrega en tabla 1 una tabla de Impacto Afectación Económica Reputacional Se cambia la palabra evento por incidente de seguridad digital. 3.5 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital.

Fecha	Versión	Descripción del Cambio
		Para el caso de los incidentes de seguridad informática, cambia por Para el caso de incidentes de seguridad digital y privacidad que afecten la disponibilidad de un servicio, servidor, base de datos y/o aplicación Se elimina la palabra “y/o custodio del activo” En el equipo de respuesta se agrega al líder de gestión de incidentes de seguridad de la información. 3.6 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital. 3.7 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital. 3.10 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital. 3.11 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital. 3.12 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital, se ajusta el párrafo “**,** los Especialistas encargados de los servicios de tecnología involucrados y al director de Información y Tecnología como líder del Sistema de Gestión de Seguridad de la Información”. 3.13 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital y privacidad y se complementa el párrafo con ". 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 evento y/o incidente y sí es el caso se deberá registrar en la matriz de riesgos del proceso o regional afectado.". se agrega al párrafo “privacidad de la información. seguridad digital y privacidad y continuidad del negocio **.** 3.14 Se cambia incidentes de seguridad de la información por incidentes de seguridad digital. 4. Descripción de actividades Actividad 1 cambia incidente de seguridad de la información por incidente de seguridad digital Actividad 2 cambia incidente de seguridad de la información por incidente de seguridad digital Actividad 3 Se ajusta y se incluye evento “y/o incidente de seguridad digital” 5. Resultado Final 6.DEFINICIONES se actualiza el concepto de evento acorde a la actualización de la ISO27000:2018 Se ajusta Evento de seguridad de la información por Evento de seguridad digital Se ajusta Incidente de Seguridad Informática por Incidente de Seguridad Digital Se elimina Incidente Digital Plan de Continuidad de la Operación cambia por Plan de Continuidad del Negocio 7. DOCUMENTOS DE REFERENCIA Se elimina 5482_G21 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.
28/01/2020	P5.GTI V6	Se actualizó la siguiente información: • Objetivo • Alcance • La política de operación 3.1, sobre los canales para reportar incidentes de seguridad de la información. • La política de operación 3.4 Clasificación del Incidente • La política de operación 3.5 Equipos de respuesta

Fecha	Versión	Descripción del Cambio
		• La política de operación 3.7 Gestión de Conocimiento. • La política de operación 3.10 Registro Base de Datos. • La política de operación 3.11 Reporte a entes externos. • La política de operación 3.12. Activar planes de contingencia. • La política de operación 3.15 notificar a los usuarios. • En el punto 4 descripción de actividades, en aquellas en donde se menciona el término: incidente de seguridad, se completó con la denominación: de la información • Actividad 13 – Informar entes externos • DOCUMENTOS DE REFERENCIA
27/11/2018	P5.GTI V5	• En el alcance se cambia el texto: “posible incidente”, por “evento”. • Se actualizan las políticas de operación: 3.2, 3.3, 3.4, 3.5, 3.9, 3.10 y 3.12. • Se incluyeron las políticas 3.13, 3.14 y 3.15. • En las actividades 6, 7, 8, 9, 10, 11 y 12, se adicionó como parte de los responsables al: Especialista, Profesional o Técnico del proveedor de servicios de TI. • Se incluyó la actividad 15 en el flujo de actividades. • Se incluyeron las definiciones de: evento, evento de seguridad de la información y se ajustó la definición de incidente de seguridad de la información. Se incluyó la ISO/IEC 27000 en el numeral 7 documento de referencia.
12/07/2018	P5.GTI V4	Se actualizó la siguiente información: • El objetivo del procedimiento de Gestión de Incidentes de Seguridad de la Información. • El alcance del procedimiento de Gestión de Incidentes de Seguridad de la Información. • La política de operación 3.2, sobre los criterios básicos. • La política de operación 3.4, en lo referente al impacto y la urgencia. • La política de operación 3.5, para el caso de incidentes que se consideren catastróficos. • La política de operación 3.10, sobre el reporte de incidentes sobre Base de Datos a la SIC. • Se incluyo la política de operación 3.11, en la cual se mencionan las entidades a las cuales se debe reportar un posible incidente de seguridad de la información. • Se incluyo la política de operación 3.12, sobre cuando informar al Líder de gestión de Continuidad. • Se actualizaron las actividades 6 y 13. • Se incluyeron definiciones nuevas relacionadas con incidentes digitales y continuidad de la operación. • Se actualizaron los documentos de referencia. • Se eliminaron las actividades 15 y 16, por el ajuste realizado a la política de operación 3.10. • Se actualizan las definiciones. Se realiza ajuste en los responsables de las actividades, de acuerdo con las orientaciones brindadas por la Subdirección de Mejoramiento Organizacional para el Levantamiento de Cargas.
15/03/2018	P5.GTI V3	• Se actualizó la dependencia del responsable de Incidentes de Seguridad de la Información. • Se incluyó al Oficial de Datos en la política de operación 3.5. • Se incluyó la política 3.10 para realizar el reporte a la Superintendencia. • Se agrega el Formato reporte incidentes Bases de Datos Personales Superintendencia de Industria y Comercio. • Se incluyeron definiciones relacionadas con Datos Personales. • Se incluyeron las actividades No. 15 y 16 relacionadas con el reporte y registro de incidentes que afectan las Bases de Datos Personales ante la SIC. Se elimina el Anexo No. 1 – Criterios gestiones SGSI, ya que se ingresan estos datos en la Matriz de escalamiento de la herramienta de Gestión de servicios.
16/01/2018	P5.GTI V2	Se actualiza rotulado de información de acuerdo con lo dispuesto en la Guía para la rotulación de la información.

Fecha	Versión	Descripción del Cambio
16/11/2016	P5.GTI V1	• Se complementó el punto número 1 objetivo. • Se complementó el punto número 2 alcance. • En el punto 3 políticas de operación, se redujeron de 17 políticas a 9 políticas optimizando el procedimiento. • En el punto 4 descripciones de las actividades, se pasó de 36 actividades a 14 actividades optimizando el procedimiento. • El punto 6 definiciones, se eliminan algunas definiciones y se agregan nuevas definiciones. • El punto 7 documentos de referencia, se eliminan algunos documentos y se agregan nuevos documentos. • El punto 8 relación de formatos, de agregan formatos. Y en el punto 9 anexos, se agrega un anexo.
16/11/2016	P5.GTI V1	Se migra al nuevo formato establecido como resultado del rediseño del Modelo de Procesos, lo que implica cambio de código (PR7.MPEV.P1).