1. ¿Para qué debo aplicar el documento?

El procedimiento establece el conjunto de acciones necesarias para gestionar adecuadamente los incidentes de seguridad de la información, mediante la aplicación de este procedimiento se logra implementar acciones de preparación, identificación, contención, respuesta, recuperación y mejora continua en las actividades de respuesta frente a potenciales ataques informáticos o fallas que puedan afectar a los sistemas de información de la Entidad.

2. ¿Cuál es la aplicación del documento?

Procedimiento inicia con la planificación de las actividades de preparación para la respuesta ante incidentes de seguridad, continua con la identificación, evaluación y establecimiento de la estrategia de respuesta, finaliza con las acciones de contención, recuperación de los sistemas afectados y recopilación de lecciones aprendidas para prevenir futuros incidentes de seguridad.

3. ¿Qué conceptos debo tener claros para comprender el documento?

Definiciones:

Incidente de seguridad de la información: Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un
impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad. (MINTIC)

Siglas:

COLCERT: Grupo de Respuestas a Emergencias Cibernéticas de Colombia. https://www.colcert.gov.co/800/w3-channel.html

MINTIC: Ministerio de las tecnologías de información y las comunicaciones.

4. ¿Qué leyes o normas aplican al documento?

La Normatividad que regula este procedimiento o las citas normativas que se enuncian en las actividades, están definidas en el Normograma de la UPIT, disponible para consulta en el siguiente enlace:
https://upit.gov.co/wp-content/uploads/2024/06/FO-GJ-01-Formato-Normograma-_Institucional_V2-18-06-2024-.xlsx

5. ¿Qué documentos externos requiero conocer para la ejecución?

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. MINTIC, En su versión vigente
Política de gobierno Digital MINTIC. En su versión vigente.

Taxonomía Única Incidentes Cibernéticos – TUIC, Superintendencia Financiera de Colombia. Taxonomía Única Incidentes Cibernéticos – TUIC, en su versión vigente.

Taxonomía clasificación ciberincidentes COLCERT, en su versión vigente.

6. ¿Qué documentos internos requiero en la ejecución?

La documentación interna que hace parte de este procedimiento y que se enuncian en las actividades, se encuentra definidas en el Banco de Documentos de la UPIT, en el siguiente link: https://upitgov.sharepoint.com/sites/Recursosdecomunicacionesdiseo/bancodedocumentosupit

7. ¿Qué políticas de operación debo tener en cuenta?

- Política General de la seguridad de la información UPIT. En su versión vigente.

- Todos los funcionarios, contratistas, proveedores de servicios y partes interesadas en los servicios de la UPIT deben reportar a través de la mesa de ayuda del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y Comunicaciones los eventos de seguridad de la información que puedan comprometer la confidencialidad, integridad o disponibilidad de los activos de información

- El Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones a través del responsable de seguridad de la información debe realizar la evaluación de los eventos de seguridad de la información para determinar cuáles será gestionados mediante el procedimiento de gestión de incidentes de seguridad de la información y cuales son gestionados como solicitudes de soporte.

- El coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones, apoyado por el responsable de seguridad de la información, establecen la necesidad de escalar el incidente de seguridad de la información ante equipos de respuesta de terceras partes especializados en delitos informáticos o gestión de ataques informáticos como el COLCERT, CSIRT, Fiscalía o Policía Nacional.

- La recolección de evidencias forenses de los incidentes de seguridad de la información debe ser realizada por la autoridad competente, quienes cuentan con el personal certificado en el manejo de la cadena de custodia de las evidencias, herramientas certificadas para la adecuada recolección y preservación de las evidencias forenses y los métodos legalmente aprobados para presentar las evidencias en caso de denuncia formal de delitos informáticos.
- La secretaría general de la UPIT es la dependencia encargada de formular ante la autoridad competente la denuncia de los incidentes de seguridad de la información que constituyan delitos informáticos según la legislación vigente.

8. ¿Cómo ejecuto el procedimiento?

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
1	**(FASE PLANEAR): Prevenir y planificar la respuesta ante incidentes de seguridad de la información**. Planificar campañas de sensibilización y toma de conciencia en buenas prácticas de seguridad, planificar el aseguramiento de plataformas tecnológicas siguiendo las recomendaciones de los fabricantes de equipos, planificar la instalación periódica de los parches de seguridad en sistemas operaciones y aplicaciones, planificar el aseguramiento de las redes de comunicaciones, verificando que solo estén habilitados los puertos necesarios para la prestación de servicios, planificar e implementar los controles de seguridad necesarios para prevenir	Profesional designado como responsable de Seguridad de la Información. Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones.	10 días	Plan de Seguridad y Privacidad de la Información	Aprobación del plan del Plan de Seguridad y Privacidad por parte del coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones.

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	incidentes, mantener contacto con grupos de interés en materia de seguridad digital y autoridades responsables de seguridad de la información (ColCERT, MINTIC, Centro Cibernético policial), Planificar los análisis de vulnerabilidades sobre la plataforma tecnológica, planificar la ejecución y pruebas de copias de respaldo de la información, planificar y ejecutar simulacros de respuesta ante incidentes informáticos.				
2	**(FASE HACER): Proteger la infraestructura tecnológica y detectar incidentes de seguridad de la información – Monitorizar eventos de seguridad de la información** Se deben monitorizar las alertas y reportes generados por las herramientas de seguridad (Firewall, WAF, consola de antivirus, consola de administración Azure), se deben evaluar los reportes de eventos de seguridad compartidos por grupos técnicos como ColCERT, MINTIC y grupos especializados en seguridad informática, se debe monitorizar el comportamiento de equipos, sistemas de	Profesional designado como responsable de Seguridad de la Información Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones (TICS).	1 hora	Informes de pruebas de análisis de vulnerabilidades, reportes de seguridad de entidades externas, tiquetes de mesa de ayuda	Seguimiento al plan de seguridad de la información en el plan de acción anual.

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	información y plataformas tecnológicas. Se deben analizar los reportes de eventos de seguridad registrados por los usuarios en la mesa de ayuda de UPIT				
3	**(FASE HACER): Proteger la infraestructura tecnológica y detectar incidentes de seguridad de la información - Registrar incidentes de seguridad - Análisis** Los eventos de seguridad de la información, solicitudes de servicios realizadas por los usuarios, resultados de pruebas de análisis de vulnerabilidades y los reportes de entidades independientes se deben analizar para determinar la necesidad de realizar diagnósticos detallados y crear tiquetes de incidentes de seguridad de la información en la mesa de ayuda UPIT.	Profesional designado como responsable de Seguridad de la Información Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones.	2 horas	Tiquete de mesa de ayuda	Asignación del tiquete de mesa de ayuda al profesional responsable de seguridad de la información.
4	**(FASE HACER): Proteger la infraestructura tecnológica y detectar incidentes de seguridad de la información- Evaluación - Clasificar incidentes de seguridad de la información.** Los eventos de seguridad de la información que sean	Profesional designado como responsable de Seguridad de la Información Grupo Interno de Trabajo de Gestión de Tecnologías de Información y	1 hora	Tiquete de mesa de ayuda con detalles de la categoría del incidente	Verificar si los síntomas y detalles del incidente reportado confirman la categoría asignada en el tiquete de mesa de ayuda.

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	calificados como incidentes de seguridad de la información (Ver Taxonomía Única Incidentes Cibernéticos Superfinanciera – TUIC, Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información de MINTIC y Guía para la gestión de incidentes de seguridad d la información en el tratamiento de datos personales de la Superintendencia de industria y comercio), deben ser evaluados de acuerdo con los criterios definidos en la política de gestión de incidentes de seguridad de la información de la UPIT. Priorizar el incidente de seguridad de la información de acuerdo con los lineamientos de gestión de incidentes de seguridad de la UPIT	Comunicaciones.			
5	**(FASE HACER): Notificar los incidentes de seguridad de la información.** Notificar a las partes interesadas internas de la ocurrencia de incidentes de seguridad	Profesional designado como responsable de Seguridad de la Información Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones.	1 hora	Tiquete de mesa de ayuda con detalles de la categoría del incidente, correos electrónicos, mensajes de alerta	Confirmación por mensaje de texto, mensaje de voz o presencialmente la materialización de incidente de seguridad de la información, autorización del encargado del grupo interno de trabajo gestión de tecnologías de información las comunicaciones para activar las

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
					acciones de respuesta al incidente.
6	**(FASE HACER): Responder a los incidentes de seguridad de la información – Definir estrategia de respuesta** Definir una estrategia de atención y respuesta ante los incidentes de seguridad, notificar a las áreas afectadas las acciones iniciales de tratamiento del incidente de seguridad, coordinar al personal técnico y administrativo requerido para la atención del incidente, notificar a la alta dirección los resultados del diagnóstico y evaluación del incidente.	Profesional designado como responsable de Seguridad de la Información Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones.	1 hora	Tiquete de mesa de ayuda con detalles de la estrategia de respuesta inicial propuesta para responder ante el incidente de seguridad	Autorización del encargado del grupo interno de trabajo gestión de tecnologías de información las comunicaciones para activar las acciones preliminares de respuesta al incidente.
7	**(FASE HACER): Responder a los incidentes de seguridad de la información- contención -** Aislar los componentes afectados por el incidente para prevenir extensión a otros compontes,	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información Grupo Interno de Trabajo de Gestión de Tecnologías de Información y Comunicaciones.	2 hora	Registros electrónicos en los componentes tecnológicos con detalles del aislamiento de máquina, tiquetes de servicio a proveedores externos solicitando bloqueo de tráfico	Autorización del coordinador del grupo interno de trabajo gestión de tecnologías de información las comunicaciones para aislar, suspender o bloquear componentes o servicios TIC.

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
8	**(FASE HACER): Responder a los incidentes de seguridad de la información. Evaluar Suspensión de servicios** Determinar la necesidad de suspender servicios, coordinar las comunicaciones a partes externas afectadas por el incidente, ¿Se requiere autorizar suspender servicios (¿sitio web, sistemas de información, otros? Si ir a: 9 No ir a:10	Coordinador de grupo interno de trabajo Gestión de tecnología de información y comunicaciones	2 horas	Correo electrónico de autorización de suspensión de servicios TIC	Autorización del nivel directivo de la UPIT para suspender servicios TIC para prevenir propagación de incidente de seguridad o daños irreparables sobre la confidencialidad, integridad o disponibilidad de los activos de información
9	**(FASE HACER): Responder a los incidentes de seguridad de la información. Contención-Suspender servicios** Suspender servicios informáticos afectados, apagar máquinas, suspender servicios de comunicaciones hasta lograr la recuperación de los sistemas afectados	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	2 hora	Registro en ticket de mesa de ayuda indicando día y hora de suspensión de servicios	Verificación de suspensión de servicios o apagado de máquinas afectadas.
10	**(FASE HACER): Responder a los incidentes de seguridad de la información. CONTENCIÓN- Evaluar solicitud de apoyo externo** Determinar la necesidad de solicitar apoyo externo de proveedores o grupos especializados en materia de seguridad digital	Profesional designado como responsable de Seguridad de la Información Profesionales responsables del grupo interno de trabajo gestión de tecnología de información y	2 horas	Informe de estado de incidente en mesa de ayuda, correos al coordinador del grupo interno de trabajo gestión de TIC con detalles del apoyo requerido	Verificar tipo de apoyo solicitado, parte interesada a la cual se solicita el apoyo, condiciones para recibir el apoyo externo

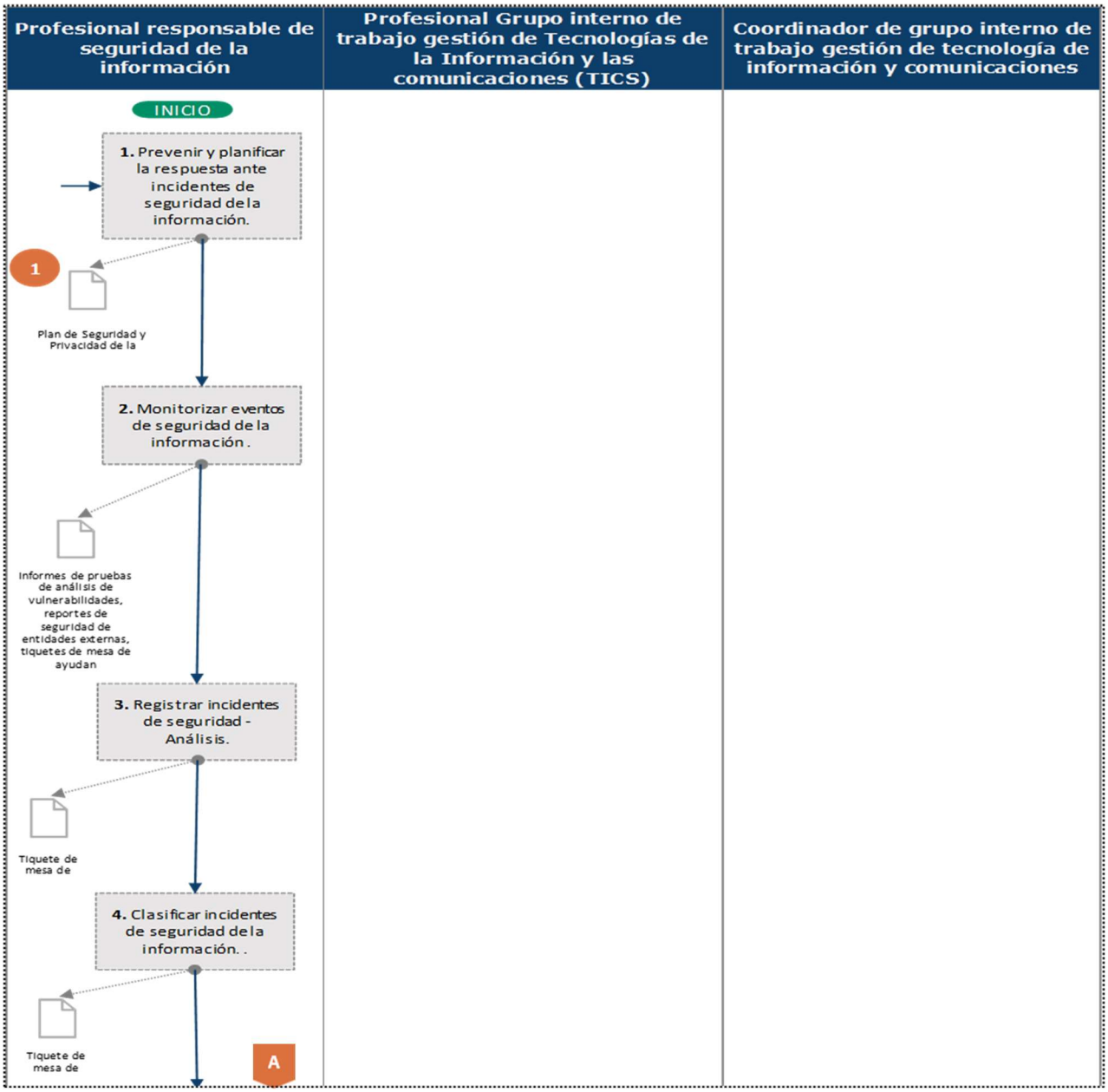
No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	¿Se requiere apoyo externo de grupos especializados? Si ir a: 11 No ir a:12	comunicaciones.			
11	**(FASE HACER): Responder a los incidentes de seguridad de la información. CONTENCIÓN-Apoyo externo** Notificar a la parte externa especializada, la necesidad de apoyo para realizar la contención del incidente de seguridad: ISP proveedor de Internet para bloquear tráfico anómalo Proveedores para recibir apoyo técnico especializado sobre la plataforma a cargo del proveedor ColCERT para identificar acciones de contención y respuesta técnica	Profesional designado como responsable de Seguridad de la Información Grupo de trabajo interno TIC. Profesionales responsables del grupo interno de trabajo gestión de tecnología de información y comunicaciones	2 horas	Comunicaciones escritas o telefónicas, tiquetes o registros en herramientas de registro de eventos ante terceras partes de apoyo en eventos de seguridad de la información. (Colcert. MINTIC, proveedores)	Verificar los detalles del registro de solicitud de apoyo técnico en materia de seguridad informática a terceras partes
12	**(FASE HACER): Responder a los incidentes de seguridad de la información- ERRADICACIÓN.** Eliminar las causas que generan el incidente de seguridad de la información. Eliminar malware de los equipos afectados. Activar filtros y protecciones contra tráfico malicioso. Desactivar software malicioso, desactivación de cuentas de cuentas de usuario con anomalías, cerrar vulnerabilidades, cambio de claves, ajuste de reglas de equipos de	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	1 hora a 72 horas	Registro en ticket de mesa de ayuda de las acciones erradicación aplicadas	Revisión de información registrada en mesa de ayuda y evaluaciones del estado de disponibilidad de los servicios informáticos: servicios afectados y servicios no afectados.

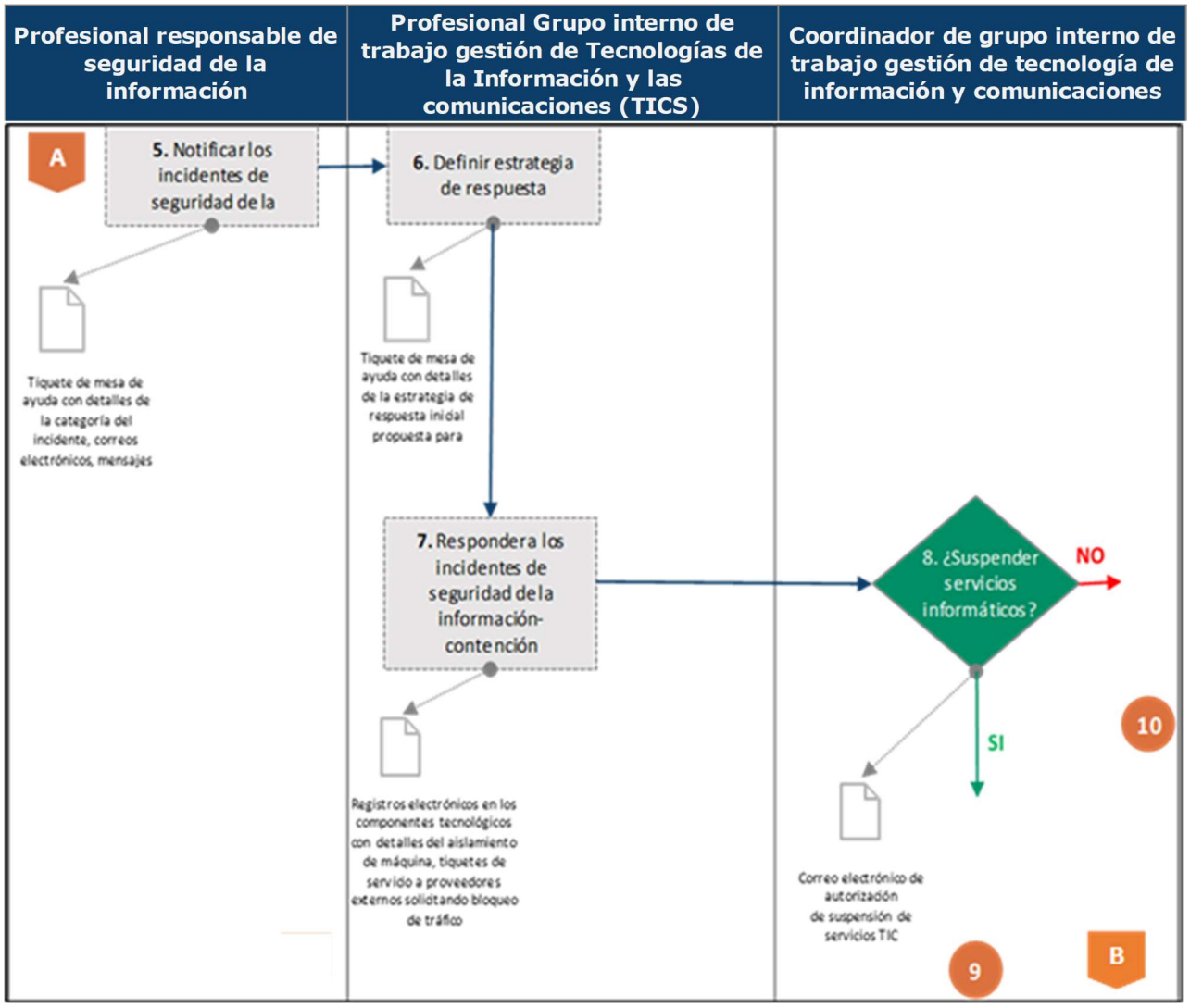
No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	seguridad (firewall, waf, IDS)				
13	**(FASE HACER): Responder a los incidentes de seguridad de la información- Evaluar necesidad de apoyo externo para recuperación**. Evaluar la necesidad de apoyo externo para recuperar los sistemas afectados, **¿Se requiere apoyo externo de grupos especializados?** **Si ir a: 14** **No ir a:15**	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	1 hora a 72 horas	Registro en ticket de mesa de ayuda de las acciones erradicación aplicadas	Revisión de información de solicitud de apoyo externo.
14	**(FASE HACER): Responder a los incidentes de seguridad de la información – recuperación notificar partes externas.** Notificar a las partes interesadas el estado de recuperación de los componentes afectados, reportar a los grupos de seguridad de MINTIC/ColCERT el estado de restablecimiento de los servicios o componentes afectados	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	1 hora a 72 horas	Registro en ticket de mesa de ayuda de las acciones de recuperación de servicios, aplicaciones y sistemas afectados.	Verificar que las acciones de recuperación documentadas en los tiquetes de mesa de ayuda.
15	**(FASE HACER): Responder a los incidentes de seguridad de la información- RECUPERACION**. Restablecimiento de los servicios afectados, reinstalar equipos, recuperación de información afectada, reconfigurar los servicios	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de	1 hora a 72 horas	Registro en ticket de mesa de ayuda de las acciones de recuperación de servicios, aplicaciones y sistemas afectados.	Verificar que los servicios, aplicaciones y sistemas se han recuperado.

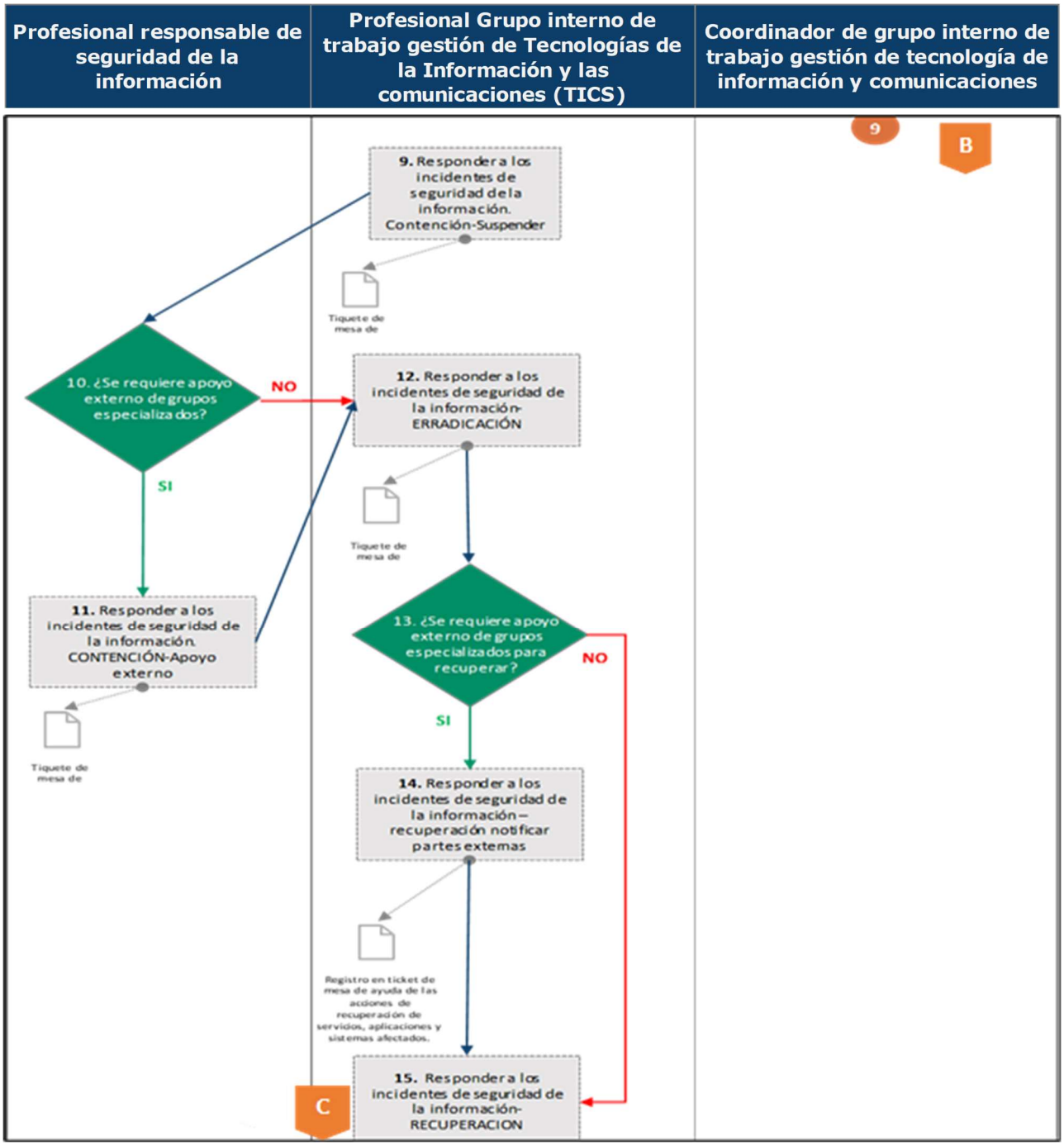
No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	afectados para resolver problemas de seguridad.	activos de información			
16	**(FASE HACER): Responder a los incidentes de seguridad de la información- Evaluar Notificación a organismos de control.** Determinar la necesidad de reportar a organismos de control del estado final del incidente de seguridad: Superintendencia de Industria y Comercio (incidentes de datos personales), MINTIC (incidentes de seguridad de la información no relacionados con datos personales) **Se debe notificar a entidades externas la resolución final de incidente de seguridad** **Si ir al paso: 17** **No ir al paso: 18**	Coordinador del grupo interno de trabajo gestión de tecnologías de información y comunicaciones	24 horas	Notificaciones, correos o comunicaciones externas	Confirmar la decisión de notificar a entes de control
17	**(FASE HACER): Responder a los incidentes de seguridad de la información- Notificar a entes de control** Notificar a las partes externas interesadas la resolución del incidente de seguridad usando los canales de comunicación o formatos definidos por la respectiva parte interesada	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	5 días	Notificaciones, correos o comunicaciones externas	Verificar que la parte externa recibe la notificación.

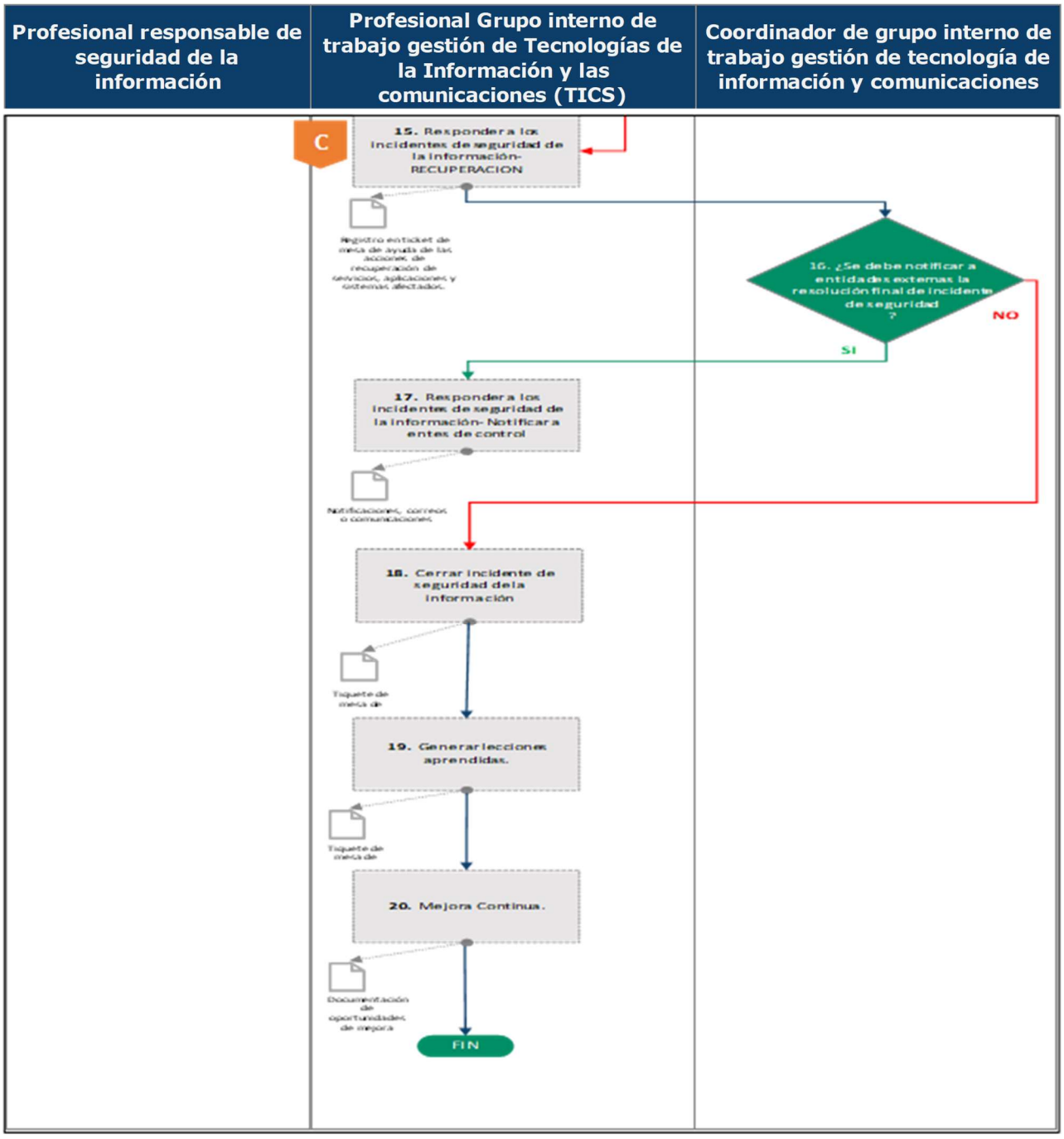
No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
18	**(FASE HACER): Cerrar incidente de seguridad de la información:** Documentar en el sistema de mesa de ayuda los resultados finales del tratamiento de incidentes de seguridad de la información,	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	1 día	Tiquete de mesa de ayuda	Verificar que la documentación del tiquete de mesa de ayuda este completa.
19	**(FASE VERIFICAR): Generar lecciones aprendidas.** preparar reportes finales de afectaciones, causas y acciones pendientes sobre el cierre del incidente de seguridad, preparar la documentación para la identificación de la causa raíz del incidente de seguridad y lecciones aprendidas. Actualizar la matriz de riesgos, actualizar la documentación de controles de seguridad, determinar acciones preventivas para futuros eventos.	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de activos de información	2 días	Tiquete de mesa de ayuda	Verificar que la documentación de lecciones aprendidas permita identificar las oportunidades de mejora para prevenir futuros incidentes.
20	**(FASE MEJORA CONTINUA):** Aplicar el procedimiento de mejora continua del sistema integrado de gestión de la UPIT para documentar al plan de mejoramiento de controles, procedimientos, capacidades y otros aspectos necesarios para prevenir la materialización de nuevos	Profesionales del grupo interno de trabajo gestión de tecnologías de información y comunicaciones responsables de la administración de	2 días	Documentación de oportunidades de mejora	Verificar el registro de la oportunidad de mejora con el grupo interno de trabajo Planeación

No.	Descripción de la Actividad	Responsable (cargo y área)	Duración	Registro	Acción de control
	incidentes de seguridad de la información originados en la causa raíz identificada.	activos de información			
	Fin del procedimiento				


Profesional responsable de seguridad de la información
Profesional Grupo interno de trabajo gestión de Tecnologías de la Información y las comunicaciones (TICS)
Coordinador de grupo interno de trabajo gestión de tecnología de información y comunicaciones
INICIO
1. Prevenir y planificar la respuesta ante incidentes de seguridad de la información.
1
Plan de Seguridad y Privacidad de la
2. Monitorizar eventos de seguridad de la información .
Informes de pruebas de análisis de vulnerabilidades, reportes de seguridad de entidades externas, tiquetes de mesa de ayudan
3. Registrar incidentes de seguridad - Análisis.
Tiquete de mesa de
4. Clasificar incidentes de seguridad de la información. .
Tiquete de mesa de
A


Profesional responsable de seguridad de la información
Profesional Grupo interno de trabajo gestión de Tecnologías de la Información y las comunicaciones (TICS)
Coordinador de grupo interno de trabajo gestión de tecnología de información y comunicaciones
A
5. Notificar los incidentes de seguridad de la
Tiquete de mesa de ayuda con detalles de la categoría del incidente, correos electrónicos, mensajes
6. Definir estrategia de respuesta
Tiquete de mesa de ayuda con detalles de la estrategia de respuesta inicial propuesta para
7. Respondera los incidentes de seguridad de la información- contención
Registros electrónicos en los componentes tecnológicos con detalles del aislamiento de máquina, tiquetes de servicio a proveedores externos solicitando bloqueo de tráfico
8. ¿Suspender servicios informáticos?
NO
SI
10
Correo electrónico de autorización de suspensión de servicios TIC
9
B


Profesional responsable de seguridad de la información
Profesional Grupo interno de trabajo gestión de Tecnologías de la Información y las comunicaciones (TICS)
Coordinador de grupo interno de trabajo gestión de tecnología de información y comunicaciones
9
B
9. Responder a los incidentes de seguridad de la información. Contención-Suspender
Tiquete de mesa de
10. ¿Se requiere apoyo externo de grupos especializados?
NO
SI
12. Responder a los incidentes de seguridad de la información- ERRADICACIÓN
Tiquete de mesa de
11. Responder a los incidentes de seguridad de la información. CONTENCIÓN-Apoyo externo
Tiquete de mesa de
13. ¿Se requiere apoyo externo de grupos especializados para recuperar?
NO
SI
14. Responder a los incidentes de seguridad de la información – recuperación notificar partes externas
Registro en ticket de mesa de ayuda de las acciones de recuperación de servicios, aplicaciones y sistemas afectados.
C
15. Responder a los incidentes de seguridad de la información- RECUPERACION


Profesional responsable de seguridad de la información
Profesional Grupo interno de trabajo gestión de Tecnologías de la Información y las comunicaciones (TICS)
Coordinador de grupo interno de trabajo gestión de tecnología de información y comunicaciones
C
15. Responder a los incidentes de seguridad de la información- RECUPERACION
Registro en ticket de mesa de ayuda de las acciones de recuperación de servicios, aplicaciones y sistemas afectados.
16. ¿Se debe notificar a entidades externas la resolución final de incidente de seguridad ?
NO
SI
17. Responder a los incidentes de seguridad de la información- Notificar a entes de control
Notificaciones, correos o comunicaciones
18. Cerrar incidente de seguridad de la información
Tiquete de mesa de
19. Generar lecciones aprendidas.
Tiquete de mesa de
20. Mejora Continua.
Documentación de oportunidades de mejora
FIN

9. ¿Qué producto o servicio se genera de este procedimiento?

Producto / Servicio Generado	Descripción del Producto / Servicio
Prevención y tratamiento de incidentes de seguridad de información.	El procedimiento genera las acciones necesarias para prevenir la materialización de incidentes de seguridad de la información que afecten la confidencialidad, integridad o disponibilidad de la información institucional, genera el conjunto de lecciones aprendidas que permiten mejorar las capacidades de la UPIT para gestionar la seguridad de la información y fortalecer sus controles de seguridad de la información.

10. Control de documentos

Versión Generada	Fecha	Descripción del Cambio o Modificación
1	30/08/2024	Versión Inicial

Elaboró	Revisó	Aprobó
Ing. Juan Carlos Alarcón S. Contratista Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.	**Ing. Bismark Buenaños** Coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones. **Ing. Jhon Alexander Gómez Arévalo** Contratista Grupo Interno de Trabajo de Planeación	**Bismark Buenaños** Coordinador del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones.