

PROCEDIMIENTO: Gestión de Incidentes de Seguridad de la Información

FECHA DE APLICACIÓN: 2023-12-05	CÓDIGO: PT.0720.29	VERSIÓN: 001	
ELABORADO POR: FABIAN EDUARDO ROJAS GALLEGO PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION CAROLA DUQUE JIMENEZ TECNICO ADMINISTRATIVO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION JUAN CARLOS CAMACHO CASTILLO PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	REVISADO POR: PAMELA KATHERINE ENRIQUEZ PAZ PROFESIONAL DE APOYO GRUPO GESTIÓN AMBIENTAL Y DE CALIDAD EDWIN RUANO GAMBOA PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	APROBADO POR: DIEGO ALEXANDER MILLAN LONDOÑO JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	

1. OBJETIVO

Determinar las actividades que se deben realizar para gestionar adecuadamente los incidentes de seguridad de la información que se puedan presentar en la Corporación Autónoma Regional del Valle del Cauca - CVC, para preservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

El procedimiento aplica cuando se presente un incidente de seguridad con los activos de información gestionados por la Oficina de Tecnologías de la Información OTI de la CVC.

3. DEFINICIONES

Las definiciones que aplican a este procedimiento pueden ser consultadas en el siguiente enlace [GLOSARIO DE TERMINOS Y DEFINICIONES OTI.](#)

4. DESARROLLO

Actividad	Responsable	Dependencia	Registro (Salida)
1. Reportar cuando se detecten eventos inusuales que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información.	Todos los Funcionarios y contratistas de la CVC	Todas las Direcciones y oficinas de la CVC	Reporte del posible incidente de seguridad
2. Analizar el evento reportado para determinar si corresponde o no, a un posible incidente de seguridad de la información. Si es un incidente de seguridad se procede a registrarlo en el formato de Reporte y Gestión de Incidentes y se continua con el procedimiento. Si no es un incidente se pasa al último numeral del presente procedimiento.	Profesional Especializado	Oficina de Tecnologías de Información	FT.0720.05 Reporte y Gestión de Incidentes de Seguridad de la Información
3. Evaluar y clasificar el incidente de seguridad, teniendo en cuenta los niveles de impacto, clasificación y priorización	Profesional Especializado	Oficina de Tecnologías de Información	FT.0720.05 Reporte y Gestión de Incidentes de Seguridad de la

del incidente.			Información
4. Implementar estrategias y acciones de respuesta inmediata que permitan contener el incidente de seguridad. Esto puede dar como resultado controles de emergencia o controles permanentes para preservar la confidencialidad, integridad y disponibilidad de la información.	Profesional Especializado	Oficina de Tecnologías de Información	FT.0720.05 Reporte y Gestión de Incidentes de Seguridad de la Información
5. Recolectar y conservar la evidencia del incidente de seguridad y reportarlo a los órganos de control o autoridades competentes para que inicien la respectiva investigación cuando sea necesario.	Profesional Especializado	Oficina de Tecnologías de Información	Evidencias del incidente y reporte a autoridades
6. Documentar las lecciones aprendidas, con el objeto de evitar la reincidencia de los hechos y eliminar las vulnerabilidades aprovechadas por la amenaza que causó el incidente de seguridad.	Profesional Especializado	Oficina de Tecnologías de Información	Base de conocimiento de incidentes de seguridad
7. Cierre y notificación del incidente de seguridad a las partes interesadas.	Profesional Especializado	Oficina de Tecnologías de Información	Notificación

NOTA 1: Para el desarrollo en detalle de las actividades del procedimiento de Gestión de Incidentes, se debe remitir al instructivo [Gestión de Incidentes de Seguridad de la Información IN.0720.06](#).

5. ANEXOS

- **Anexo 1:** [IN.0720.06 Gestión de Incidentes de Seguridad de la Información](#).
- **Anexo 2:** [FT.0720.05 Reporte y Gestión de Incidentes de Seguridad de la Información](#).

Cualquier copia impresa, electrónica o reproducción de este documento sin el sello de control de documentos se constituye en una COPIA NO CONTROLADA y se debe consultar al grupo Gestión Ambiental y Calidad de la CVC para verificar su vigencia.