



CONTROL DE CAMBIOS

| VERSIÓN | FECHA      | DESCRIPCIÓN DE LA MODIFICACIÓN |
|---------|------------|--------------------------------|
| 1       | 30/05/2023 | Nuevo procedimiento.           |

OBJETIVO

Supervisar la infraestructura para detectar eventos relacionados con la seguridad usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

ALCANCE

Inicia con el registro de los eventos relacionados con la seguridad de la información, continua con la caracterización de los eventos según su impacto y termina con el monitoreo de los tiques de incidentes de seguridad potenciales.

DEFINICIONES Y SIGLAS

Definiciones:

**Incidente de seguridad:** Es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información.

**Vulnerabilidad:** Debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.

Siglas:

**OTIC:** Oficina de Tecnologías de la Información y las Comunicaciones

POLÍTICAS DE OPERACIÓN Y ASPECTOS GENERALES

- Las actividades que son punto de control, serán señaladas dentro del Flujoograma con la figura de cuadrado y la sigla punto de control (P.C.) dentro de ella.
- Cuando en las actividades se presenten incumplimiento de requisitos de norma o de los clientes y/o usuarios, deberán implementarse el procedimiento denominado "Acciones correctivas, preventivas y de mejora".
- Cuando dentro del procedimiento se incluyan acciones de divulgación o comunicación estas deberán realizarse en el marco del Plan de comunicaciones del Departamento y deberá tener en cuenta los procedimientos y protocolos establecidos.

PRODUCTO O SERVICIO

| SALIDAS (Producto o Servicio)   | DESCRIPCIÓN  | GRUPOS DE VALOR OBJETIVO              |
|---|--|---------------------------------------|
| 1. Políticas operativas específicas de seguridad y privacidad de la información | 1. Establecer los lineamientos que permiten proteger y salvar guardar la confidencialidad, la integridad y disponibilidad de los activos de información de la Entidad. | Comité Directivo<br>Usuarios internos |

NORMATIVIDAD Y/O DOCUMENTOS ASOCIADOS

- El control de los riesgos a la seguridad de la información, riesgos laborales, aspectos ambientales se pueden consultar en el Mapa de Riesgos Institucional.
- La normativa asociada al procedimiento se puede consultar en la Matriz de requisitos legales y normativos - Normograma del Proceso.
- Los documentos asociados al procedimiento se pueden consultar en el Listado Maestro de Documentos.
- Los registros asociados al procedimiento se pueden consultar en el Listado Maestro de registros.
- Las disposiciones de almacenamiento y archivo se pueden consultar en las Tablas de Retención Documental.

| ACTIVIDAD | FLUJOGRAMA           | DESCRIPCIÓN ACTIVIDAD  | TIEMPO                       | RESPONSABLE   | FORMATO Y/O REGISTRO                            |
|-----------|----------------------|--|------------------------------|---|---|
|           |                      | INICIO.  |                              |   |   |
| 1         | Anexo 1- Flujoograma | Registrar los eventos relacionados con la seguridad, reportados por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. | Cuando se presente el evento | Mesa de servicios y servidor asignado de la seguridad de la información | <a href="#">Formato Unico de Sistemas</a>       |
| 2         |                      | Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta conmensurada.              | Cuando se presente el evento | Mesa de servicios y servidor asignado de la seguridad de la información |   |
| 3         |                      | Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.   | Cuando se presente el evento | Mesa de servicios y servidor asignado de la seguridad de la información | <a href="#">Sistema de Gestión de Servicios</a> |
| 5         |                      | FIN.   |                              |   |   |

AUTORIZACIÓN




|  |   |   |
|--|---|---|
| <p><b>ELABORÓ:</b></p>  <p><b>Nombres y Apellidos:</b> Carlos de la Ossa y Leydi Támara Rodríguez<br/><b>Cargo:</b> Contratista OTIC y Contratista OTIC</p> | <p><b>REVISÓ:</b></p>  <p><b>Nombres y Apellidos:</b> Syrus Asdrúbal Pacheco.<br/><b>Cargo:</b> Jefe de la OTIC.</p> | <p><b>APROBÓ:</b></p>  <p><b>Nombres y Apellidos:</b> Syrus Asdrúbal Pacheco.<br/><b>Cargo:</b> Jefe de la OTIC.</p> |
|--|---|---|



DIAGRAMA DE FLUJO  
PROCESO: GESTIÓN DE LA TECNOLOGÍA Y LA INFORMACIÓN  
PROCEDIMIENTO: GESTIONAR SERVICIOS DE SEGURIDAD

Mesa servicios  
y Servidor  
asignado de la  
seguridad de la  
información

