# GUÍA PARA EL ANÁLISIS DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
# TE-DR-008


**Ministerio de Comercio, Industria y Turismo**
**Gobierno de Información y Estadística**
**Junio - 2026**

## TABLA DE CONTENIDO

## 1. OBJETIVO

Establecer los lineamientos para identificar y categorizar los eventos e incidentes relacionados con la seguridad y privacidad de la información, implementando las acciones orientadas a dar respuesta a los eventos e incidentes con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información del Ministerio.

## 2. ALCANCE

Inicia con la identificación y tipificación del evento o incidentes como de ciberseguridad o de seguridad y privacidad de la información o requerimiento; continúa con la valoración y finaliza con el escalamiento para implementación de las acciones de tratamiento respectivas. Aplica a los requerimientos de usuario registrados en la Mesa de Ayuda.

## 3. DEFINICIONES

**Activos Tecnológicos:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

**Código Malicioso:** más conocido como Malware (Malware por su procedencia del inglés Malicious Software) son piezas de programación mal intencionadas con el fin de obtener, destruir o utilizar información y funcionalidades de los equipos infectados sin consentimiento del propietario. Estas piezas de programación son conocidas como virus, gusanos, caballos de Troya troyano, ramsonware y phishing y otros, los cuales mutan y evolucionan continuamente.

**Confidencialidad:** Propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Propiedad de la información que hace que no esté disponible o que sea revelada a individuos no autorizados, entidades o procesos. Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

**Control:** i) Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. ii) Medida que está modificando el riesgo (2.68) [SOURCE: ISO Guide 73:2009] Nota 1: Los Controles incluidos en cualquier proceso, política, dispositivo, practica, u otras acciones la cual modifica el riesgo. Nota 2: Los Controles puede no siempre intentar ejercer o asumir un efecto modificador.

**Controles compensatorios:** controles físicos, lógicos y administrativos para la protección de los datos, procesados y/o almacenados. La mayoría de las veces estos controles se pueden implementar sin mayores complicaciones en la infraestructura existente y apoyan la disminución de la magnitud de los riesgos identificados.

**Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. [Fuente: ISO 27000]

**Evento de Seguridad de la Información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [GTC-ISO/IEC 27035]

**Exploit:** Programa informático malicioso que aprovecha una vulnerabilidad para realizar acciones no autorizadas por el usuario.

**Gusano:** es código malintencionado de auto propagación que se puede distribuir automáticamente de un equipo a otro a través de las conexiones de red. Un gusano puede producir daños como el consumo de recursos del sistema local o de la red que posiblemente provoquen un ataque de denegación de servicio. Algunos gusanos se pueden ejecutar y propagar sin la intervención del usuario, mientras que otros necesitan que el usuario ejecute el código de gusano directamente para poder propagarse. Los gusanos también pueden suministrar una carga además de la replicación.

**Incidente de Seguridad de la Información:** (Inglés: Information security incident). Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. [SO/IEC 27000:2017]

**Mesa De Servicio:** Es una unidad funcional dedicada a gestionar una variedad de eventos sobre el servicio. La mesa es un punto único de contacto para los usuarios de los servicios de TI. Maneja los incidentes y eventos sobre servicio a través del uso de herramientas especializadas para dejar registro y administrarlos.

**Requerimientos:** Un requerimiento es una descripción de una condición o capacidad que debe cumplir un sistema, ya sea derivada de una necesidad de usuario identificada, o bien, estipulada en un contrato, estándar, especificación u otro documento formalmente impuesto al inicio del proceso.

**Spyware:** Programa creado para recopilar información sobre las actividades realizadas por un usuario y distribuirla a agencias de publicidad u otras organizaciones interesadas.

**Troyano:** Término usado para designar a un malware que permite la administración remota de una computadora, de forma oculta y sin el consentimiento de su propietario, por parte de un usuario no autorizado.

**Virus Informático:** Es un programa o un segmento de código creado con el objetivo de causar daños en los computadores, el cual puede ocasionar graves consecuencias para el computador que lo almacena.

**Vulnerabilidad:** Error de software que usa un intruso para violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia de los sistemas de información y las comunicaciones, de sus datos y aplicaciones a un sistema de información de forma manual o mediante el uso de exploits.

## 4. CONDICIONES GENERALES

La presente Guía orienta la gestión para dar respuesta a Eventos e Incidentes de Seguridad y Privacidad de la Información en dos bloques: Gestión de incidentes de seguridad de la información Gestión de Eventos de seguridad de la información y privacidad

### 4.1. Gestión de Incidentes de Ciberseguridad y Seguridad y Privacidad de la Información

La Gestión de Incidentes de Seguridad de la Información es realizada por el personal del Equipo SOC/NOC, tiene como función implementar las acciones encaminadas a contrarrestar de manera oportuna las amenazas que afectan los activos de información, mediante el monitoreo permanente de la plataforma de seguridad perimetral a la infraestructura y servicios tecnológicos y servicios de aplicación, y contar con la información generada por los diferentes incidentes que permite responder de forma sistemática, minimizar su ocurrencia de las amenazas y facilitar la recuperación rápida del activo afectado y eficiente de las actividades.

La Gestión de Incidentes de Seguridad de la Información se desarrolla a través de fases orientadas a minimizar la pérdida de información y la interrupción de los servicios, a mejorar continuamente la seguridad y el proceso de tratamiento de incidentes, y a gestionar correctamente los aspectos legales que puedan surgir durante este proceso. La Gestión de Incidentes se fundamenta en el estándar NIST SP 800-61 rev2 Computer Security Incident Handling Guide, que desarrolla acciones y controles como buenas prácticas en cuatro fases: (i) prevención, (ii) detección y análisis, (iii) contención, erradicación y recuperación, y (iv) acciones posteriores al incidente o acciones complementarias.


**Gráfico 1. Ciclo de vida de la respuesta de incidentes estándar NIST SP 800-61 rev2.**

### 4.1.1. Contactos de la Gestión de Incidentes de Seguridad de la Información

i. Contactos Internos en la Oficina de Sistemas de Información, relacionados en el siguiente cuadro:

| Rol de Gestión | Gestión Tecnológica |
|---|---|
| **Jefe Oficina Sistemas de Información** | Administración de los recursos tecnológicos y la toma de decisiones estratégicas y tácticas y operativas para la gestión de incidentes. |
| **Coordinador Grupo Ingeniería y Soporte Técnico** | Responsable Gestión Mesa de Ayuda, Servicios de Antivirus – Antimalware, Office 365 y Suite de Aplicaciones, Mantenimiento de Equipos portátiles y dispositivos |
| **Coordinador Grupo Desarrollo y Mantenimiento de Aplicaciones** | Ingeniero encargado de Servicios de Aplicación |
| **Proveedores Servicios Tecnológicos** | Apoyo y coordinación en la implementación de acciones de remediación a nivel del servicio de aplicación y servicios tecnológicos |
| **Oficial de Seguridad de la Información – o Quien Haga sus Veces** | Responsable del seguimiento a la implementación de acciones de remediación |

| Rol de Gestión | SOC/NOC | Administrador Servidores | Administrador Telecomunicaciones | Administrador Red |
|---|---|---|---|---|
| **Proveedor Servicios Tecnológicos** | Monitoreo, Análisis, Reporte y Aplicación de Políticas de Contención | Responsable de la administración de la plataforma tecnológica (servidores de Aplicaciones y bases de datos, equipos de red y componentes de TI. | Apoyo y coordinación en la implementación de acciones de remediación a nivel del servicio de aplicación | Apoyo y coordinación en la implementación de acciones de remediación a nivel de los dispositivos que conforman la plataforma tecnológica |

**ii. Contactos con Autoridades Cibernéticas:** ColCERT, CSIRT Policía Nacional, CSIRT Gobierno MinTIC, CCOC – Comando Conjunto Cibernético, para la atención de boletines o alertas de ciberseguridad o el reporte de incidentes de seguridad de la información en los canales de comunicación definidos por cada una de estas entidades:

**- ColCERT** http://www.colcert.gov.co/

**Quien Reporta:** El Jefe de la Oficina de la Oficina de Sistemas de Información, y en su ausencia el Oficial de Seguridad de la Información o Quien Haga sus Veces, o Quien designe el Jefe de la Oficina de Sistemas de Información. Alcance del Reporte: Los incidentes que se reportan ante CSIRT son todos los relacionados con la Plataforma VUCE, por estar categorizada como infraestructura y servicio crítico ante el Comando Conjunto Cibernético del Ministerio de Defensa.

**Donde se Reporta:** El reporte se realiza al correo electrónico contacto@colcert.gov.co atendiendo los requerimientos para el "Reportar un Incidente" indicados en el enlace http://www.colcert.gov.co/?q=contenido/reportar-un-incidente - CSIRT Policía Nacional https://cc-csirt.policia.gov.co/ El reporte de la Denuncia Virtual se realiza en el CAI Virtual se realiza en el "Sistema Nacional de Denuncia Virtual en el enlace https://adenunciar.policia.gov.co/adenunciar/Login.aspx?ReturnUrl=/adenunciar/%20.

**Quien Reporta:** El Jefe de la Oficina de la Oficina de Sistemas de Información, y en su ausencia el Oficial de Seguridad de la Información o Quien Haga sus Veces, o Quien designe el Jefe de la Oficina de Sistemas de Información.

**Alcance del Reporte:** Los incidentes de seguridad de la información o ciberseguridad que se reporten ante CSIRT Policía Nacional son los relacionados con la categoría "Delitos Informáticos" de acuerdo con Ley 1273 de 2009 – Capítulo I: Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, Interceptación de datos informáticos, Daño Informático, Uso de software malicioso, Violación de datos personales, Suplantación de sitios web para capturar datos personales, Hurto por medios informáticos y Transferencia no consentida de activo.

**Donde se Reporta:** El reporte se realiza en el sitio web CAI Virtual – "A denunciar", siguiendo el siguiente flujo de registro:


Gráfico 2. Flujo de Registro de Reporte de Incidente en CSIRT Ponal

**- Comando Conjunto Cibernético** https://www.ccoc.mil.co/

Ante esta Autoridad no se reportan incidentes de seguridad de la información o de ciberseguridad.

Una vez informado el Ministerio de Boletines de Alertas, se procede a la implementación de las acciones de contención y prevención para el aseguramiento de la infraestructura y servicios tecnológicos de acuerdo con el procedimiento IC-PR-028 Gestión de Incidentes de Seguridad y Privacidad de la Información.

**Quien Reporta:** El Jefe de la Oficina de la Oficina de Sistemas de Información, y en su ausencia el Oficial de Seguridad de la Información o Quien Haga sus Veces, o Quien designe el Jefe de la Oficina de Sistemas de Información.

**Alcance del Reporte:** Los incidentes de seguridad de la información relacionados con los servicios de aplicación.

**Donde se Reporta:** El reporte se realiza al correo electrónico csirtgob@mintic.gov.co

**(ii) Contactos con Grupos de Interés, entidades u organismos de Control:** Policía Nacional, Fiscalía General de la Nación, Contraloría General de la República, Procuraduría General de la Nación, MinTIC, u otras entidades u organismos que con sustento legal requieran del reporte de incidentes o que como resultado de la gestión de incidentes de seguridad y privacidad de la información en el Ministerio se determina la necesidad de informar sobre el incidente.

**Quien Reporta:** El Jefe de la Oficina de la Oficina de Sistemas de Información, y en su ausencia el Oficial de Seguridad de la Información o Quien Haga sus Veces, o Quien designe el Jefe de la Oficina de Sistemas de Información.

**Alcance del Reporte:** Los incidentes de seguridad de la información que afecten la infraestructura y servicios de aplicación y que utilicen como vector de ataque servicios tecnológicos – como correo electrónico servicios de aplicación de otras organizaciones, Entidades o Empresas.

**Donde se Reporta:** El reporte se realizará al canal de comunicación oficial de la organización, Entidad o empresa relacionada con el incidente.

### 4.1.2. Información requerida en la Gestión de Incidentes


### 4.1.3. Recursos para la Recolección de Evidencias y Análisis forense ante Incidentes de Seguridad y Privacidad de la Información

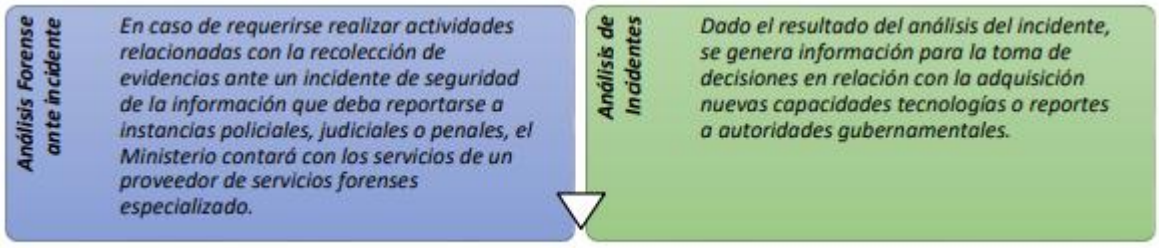


**Gráfico 4. Información para análisis de Incidentes.**

## 5. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio a través de la Oficina de Sistemas de Información ha dispuesto de los recursos y capacidades para llevar a cabo de la gestión de incidentes de seguridad y privacidad de la información, y desarrollada a través de las siguientes actividades:


**Gráfico 5. Actividades de la Gestión de Incidentes de Seguridad y Privacidad de la Información.**

## 5.1. Reporte del Incidente de Seguridad y Privacidad de la Información

La Mesa de Ayuda recepciona las solicitudes o requerimientos de soporte técnico a través de los canales de atención dispuestos por la Oficina de Sistemas de Información.


**Gráfico 6. Canales de reporte de solicitudes o requerimientos de Soporte Técnico.**

- La Mesa de Ayuda genera automáticamente un número de CASO para la solicitud reportada.

## 5.2. Identificar y valorar el incidente

### 5.2.1. Identificación El Técnico en Mesa de Ayuda:

a. Analiza el CASO reportado y recolecta la información preliminar que le permita clasificar el CASO como: Incidente, Requerimiento, Cambio, o Problema.

b. Sí el alcance del CASO "NO" se encuentra dentro del Catálogo de Servicios de "Seguridad de la Información y Continuidad" implementado en la herramienta de Mesa de Ayuda, se realiza la gestión pertinente, documenta y cierra el caso. c. Si se encuentra dentro de la Categoriza el CASO "Seguridad de la Información y Continuidad" se procede a valorar el CASO.

### 5.2.2. Valoración Para los CASOS clasificados dentro del Catálogo de Servicios de "Seguridad de la Información y Continuidad", el Técnico en Mesa de Ayuda:

a. Tipifica el CASO de acuerdo con el tipo de servicio y adelanta las Acciones de Nivel 1 definidas en la Catálogo de Servicios de "Seguridad de la Información y Continuidad".

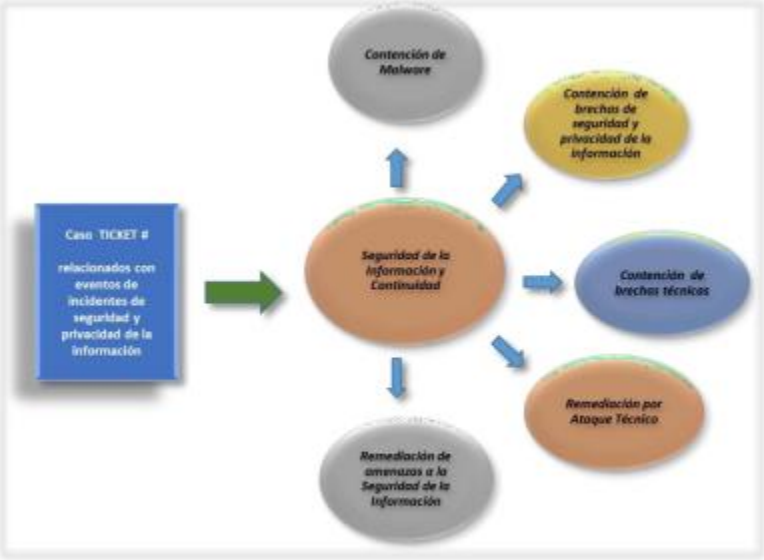


**Gráfico 7. Categorización de Caso de Incidentes de Seguridad y Privacidad de la Información.**

b. Valida "Acciones de Nivel 1" para el tipo de servicio recolecta información, documenta y procede a asignar el CASO; de acuerdo con el Catálogo de Servicios de "Seguridad de la Información y Continuidad", especifica: Proveedor del Servicio, Especialista, ANS – Acuerdo de Nivel de Servicio, Urgencia y Servicio:


**Gráfico 8. Flujo de Asignación CASO.**

c. Asignación del caso de acuerdo con el tipo de servicio, inicialmente se asignará al rol de "Especialista" indicado en Catálogo de Servicios de "Seguridad de la Información y Continuidad", quien adelantará las Acciones de Nivel 2. Detalladas en la Catálogo de Servicios de "Seguridad de la Información y Continuidad".

## 5.3. Gestionar las acciones para atender el incidente

d. El Especialista Analista Nivel 2 del equipo SOC/NOC, de acuerdo con lo definido en el Catálogo de Servicios de "Seguridad de la Información y Continuidad".

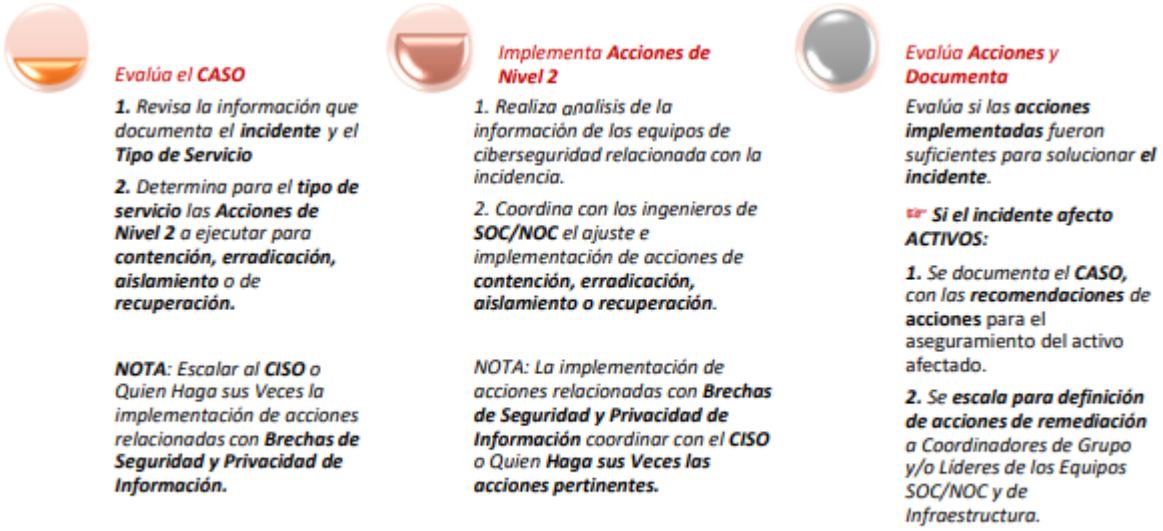


**Gráfico 9. Flujo de Acciones de Nivel 2.**

## 5.4. Realizar pruebas de aseguramiento

El Especialista Analista Nivel 2 del equipo SOC/NOC para determinar el aseguramiento de las acciones implementadas:

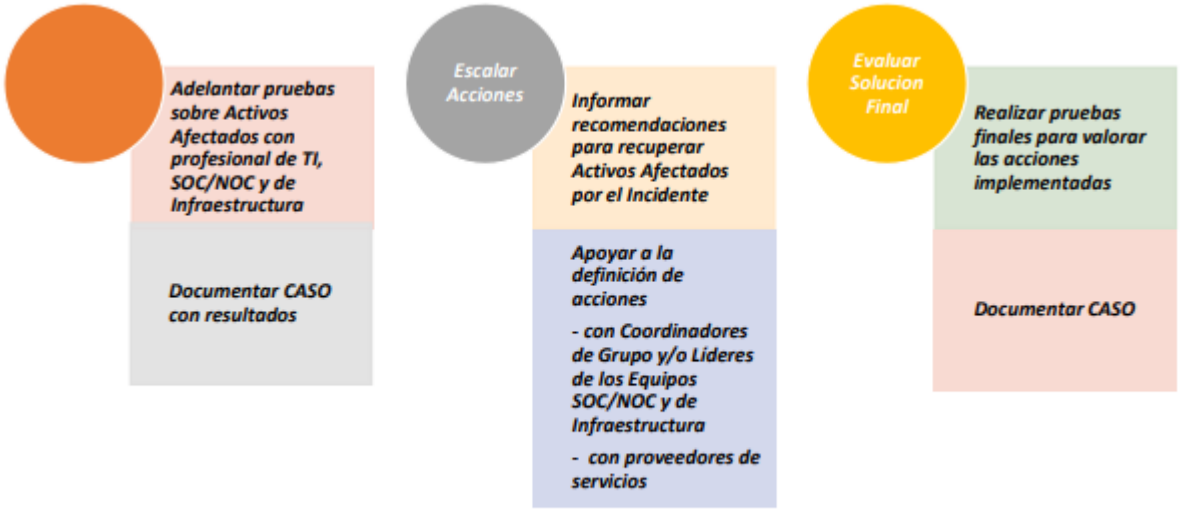


Gráfico 10. Flujo de Acciones de Nivel 3 y Aseguramiento.

## 5.5. Cierre del Incidente

• Una vez documentado el caso por todos los roles involucrados, se realiza el cierre de gestión.
• La Mesa de Ayuda cierra el CASO, una vez verificado la solución del Incidente.
• Automáticamente la herramienta de Mesa de Ayuda notificación del cierre del CASO a la fuente de origen, con el resultado de las acciones tomadas.

## 5.6. Reporte a Autoridades Cibernéticas

Si el Incidente es reportado por una Autoridad cibernética – ColCERT, CSIRT Policía Nacional, CCOCI – Comando Conjunto Cibernético o CSIRT Gobierno – MinTIC, se debe:
• Registrar CASO en la herramienta de Mesa de Ayuda.
• Ejecutar el procedimiento IC-PR-028: Gestión de Incidentes de Seguridad y Privacidad de la Información.
• Si es requerido por la Autoridad Cibernética informar las Acciones adelantadas de acuerdo con lo documentado en el respectivo CASO y enviar respuesta a través del canal de comunicación definido por la Autoridad Cibernética (Ver 4.2. Contactos de la Gestión de Incidentes de Seguridad de la Información).

## 5.7. Proyectar reiteraciones de incidentes

El análisis de reiteraciones de incidentes requiere del trabajo conjunto de los Ingenieros de SOC/NOC, Infraestructura y Coordinaciones de Desarrollo y Mantenimiento de Aplicaciones y de Ingeniería y Soporte Técnico. Esta actividad se realizará de acuerdo con los incidentes gestionados y documentados en la Mesa de Ayuda.

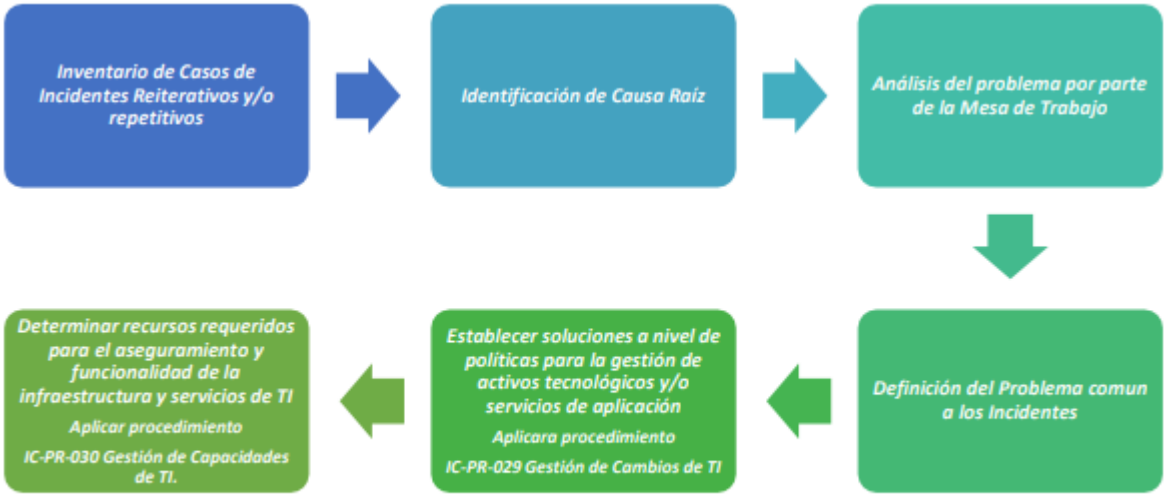


**Gráfico 11. Flujo de Acciones de Nivel 3 y Aseguramiento.**

**Catálogo de Servicios de "Seguridad de la Información y Continuidad"**

| **Tipo de Evento:** | ***INCIDENTE DE CIBERSEGURIDAD*** | | | |
|---|---|---|---|---|
| **Tipo de Servicio** | ***CONTENCIÓN DE MALWARE*** | | | |
| **Fuente de Reporte** | **Prioridad (Criticidad)** | **Impacto** | **ANS (default LOW)** | **Asignación Especialista** |
| *SOC/NOC*<br>*Infraestructura Tecnológica*<br>*Gestor de Aplicaciones*<br>*Autoridades cibernéticas: ColCERT, CSIRT Policía Nacional, CCOCI, CSIRT Gobierno MinTIC* | *ALTA* | *ALTO* | *CRITICA: 1 -6 horas*<br>*ALTA: 6-12 horas*<br>*BAJA: 12 -24 horas* | *SOC/NOC Gestor Nivel 2* |
| **Descripción del Servicio** | **Mesa de Ayuda**<br>**Acciones Nivel 1** | **SOC / NOC**<br>**Acciones Nivel 2** | **Escalamiento**<br>**Acciones Nivel 3** | **Urgencia (nivel de atención)** |
| *1. Realizar el análisis para la identificación del tipo de malware:*<br>*Worm (Gusano)*<br>*Virus (Troyano)*<br>*Botnet*<br>*Inyección Web de código malicioso*<br>*Trojan*<br>*Virus Polimórficos*<br>*Otros (rootkit, spyware, malvertising)*<br>*Ransomware*<br>*2. Definir los mecanismos de contención y erradicación del malware.*<br>*3. Implementar las acciones de contención y erradicación.*<br>*4. Notificar acciones implementadas para Recuperación del Servicio o Dispositivo.*<br>*5. Documentar CASO y/o la Base de Conocimiento.* | *1. Verificar con el usuario final, el contexto del CASO, con el fin de descartar una mala interpretación, el CASO debe estar dentro de lo conocido como un evento de **Malware**.*<br>*2. Recolectar las evidencias como: archivos, fotos, videos, imágenes, audios, entre otros.*<br>*3. Realizar las siguientes acciones:*<br>*a. Actualización del programa antivirus (firmas de virus).*<br>*b. Escaneo rápido a todo el sistema o escaneo puntual de la amenaza sobre un archivo.*<br>*c. Descargar el **LOG** del antivirus local de la máquina del usuario y adjuntarlo al CASO.*<br>*d. Descargar copia del **regedit** y adjuntarlo al CASO.*<br>*e. Si se trata de una falla sobre un sistema específico, se debe copiar en un **txt** la salida de las siguientes comandos y adjuntarlo al CASO:*<br>*adjuntar los **Logs** del sistema afectado*<br>*ejecutar el comando "**netstat -aon**" en la línea de comandos de DOS o "**netstat -tupan**" en la **CLI***<br>*g. Si se trata de un archivo sospechoso, antes de moverlo o copiarlo se debe agregar en **Zip protegido**, con la contraseña **$r4nda2021*** y adjuntarlo al CASO.*<br>*4. Documentar CASO con la evidencia consolidada y escalar al **SOC/NOC Gestor Nivel 2** para revisión y tratamiento.* | *1. Analizar del escenario del CASO.*<br>*2. Realizar análisis avanzado de la evidencia, con herramientas como **sandboxing**, inteligencia de amenazas avanzadas, entre otras.*<br>*3. Concluir el análisis con acciones adicionales de remediación si es el caso.*<br>*4. Documentar el CASO y escalarlo a quien corresponda para revisión y tratamiento, con el fin de aplicar las acciones que se requieran para la contención.* | *En este nivel se declara la necesidad de tratamiento de un problema, dirigido al Proveedor del hardware o software de las soluciones de ciberseguridad con las que cuenta la Entidad, con el fin de lograr acciones de contención a mediano plazo.* | *- CRITICA*<br>*Infraestructura Tecnológica:*<br>*Servidores de aplicación y bases de datos*<br>*Servicios tecnológicos*<br>*Correo electrónico*<br>*Infraestructura de Red (LAN, WAN, Equipos de comunicación, routers, VPN, Switches, canales dedicados.)*<br>*Aplicativos: VUCE, Sitio web institucional, Gestión Documental*<br>*- ALTA*<br>*Aplicativos de gestión administrativa (Nómina, Inventarios, Gestión Disciplinaria)*<br>*Redes Sociales (Twitter, Facebook, Instagram, YouTube)*<br>*- BAJA*<br>*Aplicativos de Gestión (ITA, PAASOCI, FURAG, RAAM)*<br>*Equipos de usuario final.* |

**Catálogo de Servicios de "Seguridad de la Información y Continuidad"**

| ***Tipo de Servicio*** | ***REMEDICIÓN POR ATAQUE TÉCNICO*** | | | |
|---|---|---|---|---|
| ***Fuente de Reporte*** | ***Prioridad (Criticidad)*** | ***Impacto*** | ***ANS (default LOW)*** | ***Asignación Especialista*** |
| *SOC/NOC*<br>*Infraestructura Tecnológica*<br>*Gestor de Aplicaciones*<br>*Autoridades cibernéticas: ColCERT, CSIRT*<br>*Policía Nacional, CCOCI, CSIRT Gobierno MinTIC*<br>*CISO o quien haga sus veces* | *ALTA* | *ALTO* | *CRITICA: 1 -6 horas*<br>*ALTA: 6-12 horas*<br>*BAJA: 12 -24 horas* | *SOC/NOC Gestor Nivel 2* |
| ***Descripción del Servicio*** | ***Mesa de Ayuda***<br>***Acciones Nivel 1*** | ***SOC / NOC***<br>***Acciones Nivel 2*** | ***Escalamiento***<br>***Acciones Nivel 3*** | ***Urgencia (nivel de atención)*** |
| *1. Realizar el análisis para identificar el contexto de la remediación.*<br>*Escaneo de redes*<br>*Aprovechamiento de vulnerabilidades*<br>*Ataques de fuerza bruta*<br>*Denegación de Servicio*<br>*SQL Injection*<br>*XSS/XSRF*<br>*otros*<br>*2. Definir las acciones de remediación.*<br>*3. Implementar las acciones de remediación.*<br>*4. Documentar lecciones aprendidas.*<br>*5. Definir e implementar las acciones de remediación complementarias.*<br>*6. Documentar CASO y/o Base de Conocimiento.* | *1. Verificar con el usuario final, el contexto del caso, el CASO debe estar dentro de lo conocido como un evento de **Ataque Tecnico**.*<br>*2. Recolectar las evidencias como: archivos, fotos, videos, imágenes, audios, entre otros.*<br>*3. Realizar las siguientes acciones:*<br>*a. Adjuntar evidencia especifica del evento descrito.*<br>*b. Documentar el CASO con la descripción del caso, citando lo más cercano y/o parecido posible a lo que indica el usuario final.*<br>*c. Agregar al CASO, los datos específicos del dispositivo o sistema como: dirección IP, recurso URL o URI (uniform resource identifier), tipo de servicio, tipo de error de seguridad especifico en texto claro.*<br>*d. Informar el estado de disponibilidad actual, del recurso tecnológico afectado.*<br>*4. Documentar CASO con la evidencia consolidada y escalar al **SOC/NOC Gestor Nivel 2** para revisión y tratamiento.* | *1. Analizar del escenario del CASO.*<br>*2. Realizar análisis avanzado de la evidencia, utilizar herramientas para identificar vulnerabilidades, intrusiones, correlacionado de eventos.*<br>*3. Concluir el análisis con acciones adicionales de remediación si es el caso.*<br>*4. Documentar el CASO y escalarlo a quien corresponda para revisión y tratamiento, con el fin de aplicar las acciones que se requieran para la contención.* | *En este nivel se declara la necesidad de tratamiento de un problema, dirigido al Proveedor del hardware o software que soporta la tecnología que se observa afectada, o que soporta el servicio la aplicación.* | *- CRITICA*<br>*Denegación de Servicio*<br>*SQL Injection*<br>*XSS/XCRF*<br>*LFI*<br>*- ALTA*<br>*Aprovechamiento de vulnerabilidades*<br>*Ataques de fuerza bruta*<br>*- BAJA*<br>*Escaneo de redes* |

**Catálogo de Servicios de "Seguridad de la Información y Continuidad"**

| ***Tipo de Evento:*** | ***INCIDENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*** | | | |
|---|---|---|---|---|
| ***Tipo de Servicio*** | ***REMEDIACIÓN DE AMENAZA A LA SEGURIDAD DE LA INFORMACIÓN*** | | | |
| ***Fuente de Reporte*** | ***Prioridad (Criticidad)*** | ***Impacto*** | ***ANS (default LOW)*** | ***Asignación Especialista*** |
| *SOC/NOC*<br>*Infraestructura Tecnológica*<br>*Gestor de Aplicaciones*<br>*Autoridades cibernéticas: ColCERT, CSIRT Policía Nacional, CCOCI, CSIRT Gobierno MinTIC* | *ALTA* | *ALTO* | *CRITICA: 1 -6 horas*<br>*ALTA: 6-12 horas*<br>*BAJA: 12 -24 horas* | *SOC/NOC Gestor Nivel 2* |
| ***Descripción del Servicio*** | ***Mesa de Ayuda Acciones Nivel 1*** | ***SOC / NOC Acciones Nivel 2*** | ***Escalamiento Acciones Nivel 3*** | ***Urgencia (nivel de atención)*** |
| *1. Realizar el análisis para identificar el contexto de la remediación.*<br>*Interceptación*<br>*Espionaje*<br>*Ingeniería social: Phishing, Spam, Spoofing, Vishing, Shoulder Surfing, Dumpter Diving, etc.*<br>*Suplantación: de Personas, de Imagen institucional (Correo electrónico, sitios web, mensajería instantánea, redes sociales, programas misionales.*<br>*Otros (Especifique)*<br>*2. Definir las acciones de remediación.*<br>*3. Implementar las acciones de remediación.*<br>*4. Definir e implementar las acciones de remediación complementarias.*<br>*5. Documentar CASO y/o Base de Conocimiento.* | *1. Verificar con el usuario final, el contexto del caso, el CASO debe estar dentro de lo conocido como un evento de **Amenazas de Seguridad**.*<br>*2. Recolectar las evidencias como: archivos, fotos, videos, imágenes, audios, entre otros.*<br>*3. Realizar las siguientes acciones:*<br>*a. Adjuntar copia original del mensaje (correo, mensaje instantáneo, SMS, etc.) si es un contenido malicioso se debe comprimir en **Zip protección** de acceso con la contraseña: **$r4nda2021*** y adjuntarlo al CASO.*<br>*b. Se debe agregar descripción del evento en el CASO, lo más cercano a lo precisado por el usuario.*<br>*4. Documentar CASO con la evidencia consolidada y escalar al **SOC/NOC Gestor Nivel 2** para revisión y tratamiento.* | *1. Analizar del escenario del CASO.*<br>*2. Realizar análisis avanzado de la evidencia, utilizar herramientas como sandboxing, con soluciones de seguridad perimetral, OSINT, entre otras.*<br>*3. Concluir el análisis con acciones adicionales de remediación si es el caso.*<br>*4. Documentar el CASO y escalarlo a quien corresponda para revisión y tratamiento, con el fin de aplicar las acciones que se requieran para la contención.* | *Dado el caso que las soluciones de seguridad son insuficientes o ineficientes para mitigación, se declara la necesidad de **Gestión de Problema**, se escala Proveedor o fabricante de las tecnologías CORE o de ciberseguridad afectadas, con el fin de lograr acciones de mitigación a mediano plazo.* | - *ALTA*<br>*Interceptación*<br>*Espionaje*<br>*Ingeniería social: Phishing, Vishing, Shoulder Surfing, Dumpter Diving.*<br>- *MEDIA*<br>*Suplantación: Personas, imagen institucional (Correo electrónico, sitios web, mensajería instantánea, redes sociales, programas misionales.*<br>- *BAJA*<br>*Otros (Especificar)* |

**Catálogo de Servicios de "Seguridad de la Información y Continuidad"**

| ***Tipo de Servicio*** | ***CONTENCIÓN DE BRECHAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*** | | | |
|---|---|---|---|---|
| ***Fuente de Reporte*** | ***Prioridad (Criticidad)*** | ***Impacto*** | ***ANS (default LOW)*** | ***Asignación Especialista*** |
| *Funcionarios/Contratistas*<br>*SOC/NOC*<br>*PQRS -INFO*<br>*Autoridades cibernéticas: ColCERT, CSIRT Policía Nacional, CCOCI, CSIRT Gobierno MinTIC*<br>*CISO o quien haga sus veces* | *ALTA* | *ALTO* | *CRITICA: 1 -6 horas*<br>*ALTA: 6-12 horas*<br>*BAJA: 12 -24 horas* | *CISO o quien haga sus veces* |
| ***Descripción del Servicio*** | ***Mesa de Ayuda Acciones Nivel 1*** | ***CISO o quien haga sus veces*** | ***Escalamiento Acciones Nivel 3*** | ***Urgencia (nivel de atención)*** |
| *1. Realizar el análisis para identificar el contexto de la brecha materializada.*<br>*Uso no autorizado de recursos (navegación no permitida, uso a título personal de correo electrónico institucional)*<br>*Incumplimiento de las políticas internas (de comunicaciones, de sistema de gestión, de privacidad)*<br>*Incumplimiento de normatividad que aplica: de derechos de autor, protección de datos personales, propiedad intelectual, entre otras.*<br>*Fuga o Pérdida de información.*<br>*Uso indebido de imagen o afectación a la reputación corporativa.*<br>*Suplantación de identidad corporativa.*<br>*Fraude o engaño financiero o corporativo.*<br>*Contenidos inadecuados: (Contenido ilegal, Contenido de pánico, contenido malicioso, contenido abusivo, etc.)*<br>*Otros eventos que puedan generar incidencias en relación con la información*<br>*2. Definir los mecanismos de control (gestión y tecnológicos).*<br>*3. Implementar las acciones de control.*<br>*4. Definir e implementar las acciones de control complementarias.*<br>*5. Documentar CASO y/o Base de Conocimiento.* | *1. Verificar con el usuario final, el contexto del caso, el CASO debe estar dentro de lo conocido como un evento de* ***Brechas de Seguridad****.*<br>*2. Recolectar las evidencias como: archivos, fotos, videos, imágenes, audios, entre otros.*<br>*3. Realizar las siguientes acciones*<br>*a. Documentar el CASO con la descripción del caso, citando lo más cercano y/o parecido posible a lo que indica el usuario final.*<br>*b. Confirmar con el Usuario, si se tomaron acciones para controlar esta situación, atendiendo las Política de Seguridad y Privacidad de la Información y Buenas Prácticas.*<br>*4. Documentar CASO con la evidencia consolidada y escalar al* ***CISO o quien haga sus veces*** *para revisión y tratamiento.* | *1. Analizar del escenario del CASO.*<br>*2. Realizar mapeo frente al análisis de riesgos de la Entidad para determinar acciones a tomar y/o aplicar controles según el caso.*<br>*3. Concluir el análisis con acciones adicionales a aplicar para de remediación.*<br>*4. Documentar el CASO y escalarlo a quien corresponda para revisión y tratamiento, con el fin de aplicar las acciones que se requieran para la contención.* | *Realizar mesa de trabajo con el equipo o roles que estén a cargo del activo de información afectado, para determinar las acciones de control a aplicar a mediano plazo.* | - *CRITICA*<br>*Imagen y reputación*<br>*Incumplimiento de normas o políticas*<br>*Fuga o pérdida de información*<br>*Fraude o engaño*<br>- *ALTA*<br>*Verificación de la aplicación de controles de acceso y navegación de usuarios*<br>*Verificación de la disponibilidad de la información en los repositorios*<br>- *BAJA*<br>*Otros* |

**Catálogo de Servicios de "Seguridad de la Información y Continuidad"**

| **Tipo de Evento:** | ***REQUERIMIENTO*** | | | |
|---|---|---|---|---|
| **Tipo de Servicio** | ***CONTENCIÓN DE BRECHAS TÉCNICAS*** | | | |
| **Fuente de Reporte** | **Prioridad (Criticidad)** | **Impacto** | **ANS (default LOW)** | **Asignación Especialista** |
| *SOC/NOC*<br>*Infraestructura, gestores de aplicación* | *ALTA* | *ALTO* | *CRITICA: 1 -6 horas*<br>*ALTA: 6-12 horas*<br>*BAJA: 12 -24 horas* | *SOC/NOC Gestor Nivel 2* |
| **Descripción del Servicio** | **Mesa de Ayuda**<br>**Acciones Nivel 1** | **SOC / NOC**<br>**Acciones Nivel 2** | **Escalamiento**<br>**Acciones Nivel 3** | **Urgencia (nivel de atención)** |
| *1. Realizar el análisis para identificar el contexto de la remediación de* ***Brechas Técnicas*** *generadas por debilidades en:*<br>*Configuración de Infraestructura de TI*<br>*(Servidores, equipos de red, otros servicios)*<br>*Desarrollo de las aplicaciones.*<br>*Usuarios desatendidos, usuarios por defecto, usuarios pruebas o de desarrollo habilitados).*<br>*Otros.*<br>*2. Definir las acciones de remediación.*<br>*3. Implementar las acciones de remediación*<br>*4. Documentar CASO y/o Base de Conocimiento.* | *1. Verificar con el usuario final, el contexto del caso, con el fin de descartar una mala interpretación, este caso debe estar dentro de lo conocido como un evento de Brechas Técnicas.*<br>*2. Recolectar las evidencias como: archivos, fotos, videos, imágenes, audios, entre otros.*<br>*3. Realizar las siguientes acciones:*<br>*a. Adjuntar evidencia especifica del evento descrito.*<br>*b. Agregar al CASO:*<br>*Descripción del evento lo más cercano a lo precisado por el usuario.*<br>*Datos específicos del dispositivo o sistema como: dirección IP, recurso URL o URI (Uniform Resource Identifier)*<br>*Tipo de servicio.*<br>*Tipo de error de seguridad especifico en texto claro.*<br>*4. Documentar CASO con la evidencia consolidada y escalar al* ***SOC/NOC Gestor Nivel 2*** *para revisión y tratamiento.* | *1. Analizar del escenario del CASO.*<br>*2. Realizar análisis avanzado de la evidencia, con el fin de aplicar según se requiera los controles que apliquen a:*<br>*Actualización de Parches de seguridad o de versiones de los sistemas.*<br>*Configuraciones especificas a servidores, equipos de red, de seguridad y software para fortalecer los servicios tecnológicos.*<br>*Controles sobre los usuarios a través del directorio activo.*<br>*3. Concluir el análisis con acciones adicionales de remediación si es el caso.*<br>*4. Documentar el CASO y escalarlo a quien corresponda para revisión y tratamiento, con el fin de aplicar las acciones que se requieran para la contención.* | *En este nivel se declara la necesidad de tratamiento de un problema, dirigido al Proveedor o Fabricante que soporta la tecnología que se observa afectada, o de soporte de software aplicativo o con el Coordinador de Desarrollo y Mantenimiento de Aplicaciones (in-house).* | - *CRITICA*<br>*Infraestructura Tecnológica: servidores de aplicación y bases de datos, Servicios tecnológicos*<br>*Correo electrónico*<br>*Infraestructura de Red (LAN, WAN, Equipos de comunicación, routers, VPN, Switches, canales dedicados.)*<br>*Aplicativos: VUCE, Sitio web institucional, Gestión Documental*<br>*ALTA*<br>*Aplicativos de gestión administrativa (Nómina, Inventarios, Gestión Disciplinaria)*<br>*Redes Sociales (Twitter, Facebook, Instagram, YouTube)*<br>- *BAJA*<br>*Aplicativos de Gestión (ITA, PAASOCI, FURAG)* |

## 6. GESTIÓN DE EVENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Ministerio a través de la Oficina de Sistemas de Información ha dispuesto de los recursos y capacidades para llevar a cabo la gestión de Eventos de Seguridad y Privacidad de la información - ESPI, así:


**Gráfico 12. Flujo de Acciones de la Gestión de Eventos SPI**

Los Eventos de Seguridad y Privacidad de la Información – ESPI son generados por brechas que pueden generar un incidente y materializar un riesgo de seguridad informática, seguridad y privacidad de la información o de ciberseguridad.


**Gráfico 13. Alcance Gestión de Eventos SPI**

### 6.1. Identificar el Evento SPI

El Técnico en Mesa de Ayuda:

a. Analiza el CASO reportado y recolecta la información preliminar que le permita clasificar el CASO dentro de la categoría "Seguridad de la Información y Continuidad" y tipo de servicio "Contención de Brechas de Seguridad y Privacidad de la Información"

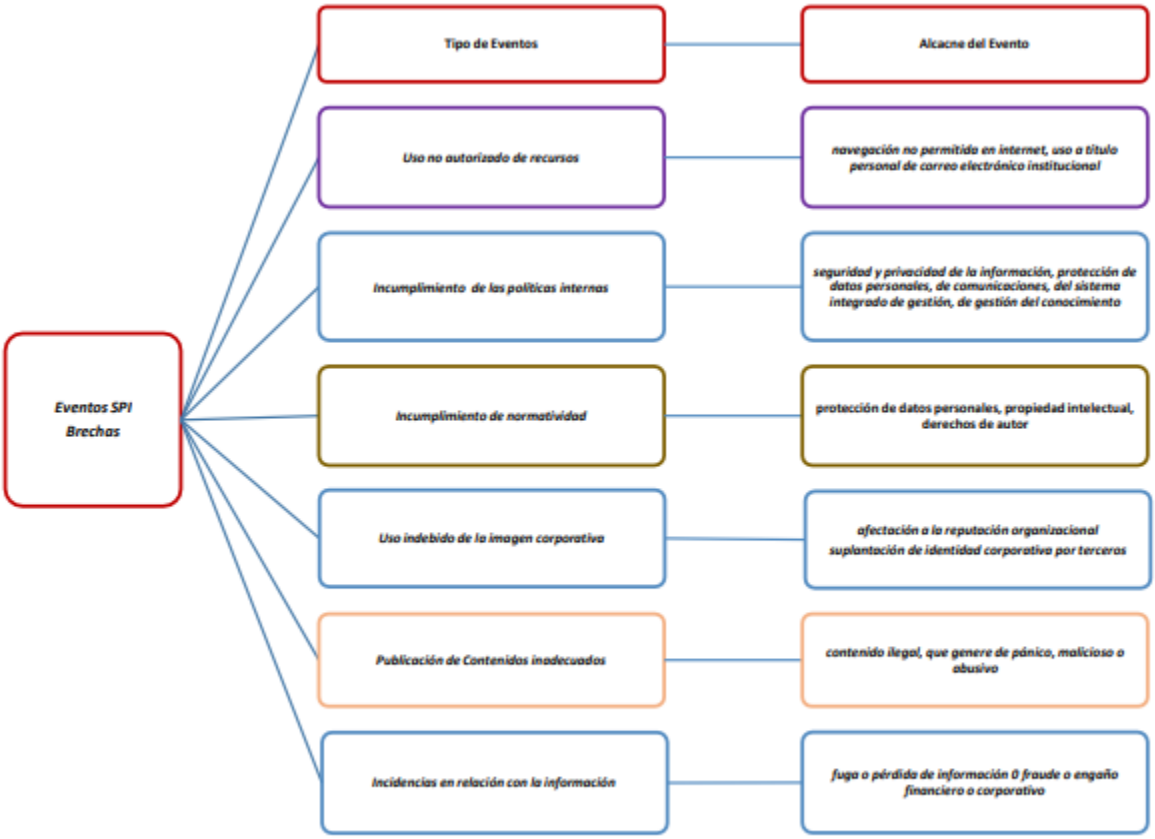


Gráfico 14. Eventos SPI - Brechas

b. Se procede a valorar el CASO.

## 6.2. Valoración

El Técnico en Mesa de Ayuda adelanta las Acciones de Nivel 1 para el tipo de servicio "Contención de Brechas de Seguridad y Privacidad de la Información" definidas en el Catálogo de Servicios de "Seguridad de la Información y Continuidad"


Gráfico 15. Acciones Nivel 1 para la Valoración del Eventos SPI

### 6.3. Gestionar las acciones para atender el Evento

De acuerdo con lo definido en el Catálogo de Servicios de "Seguridad de la Información y Continuidad":


### 6.4. Realizar pruebas de aseguramiento

De acuerdo con las acciones de remediación implementadas, se valida que tales acciones corrijan el evento.

### 6.5. Cierre del Evento

- Una vez documentado el caso por todos los roles involucrados, se realiza el cierre de gestión.
- La Mesa de Ayuda cierra el CASO, una vez verificado la solución del evento.
- Automáticamente la herramienta de Mesa de Ayuda notificación del cierre del CASO a la fuente de origen, con el resultado de las acciones tomadas.

## 7. HISTORIAL DE CAMBIOS

<table>
<tr><th>FECHA</th><th>VERSIÓN</th><th>DESCRIPCIÓN DEL CAMBIO</th></tr>
<tr><td>12/06/2026</td><td>0</td><td>Primera versión del documento para el nuevo Mapa de procesos.<br>Código anterior: GTI-DE-006. V00.<br><br>Para efectos de trazabilidad y soporte de la migración al nuevo aplicativo de administración de la documentación del Modelo Institucional de Operación (MIO), los siguientes fueron los responsables de la revisión y aprobación del documento migrado:<br><br>
<table>
<tr><td>REVISÓ</td><td>APROBÓ</td></tr>
<tr><td>IXEL RODRIGUEZ CORREA<br><br>Cargo: Profesional especializado</td><td>EDGAR GREGORIO CARRILLO MONCADA<br><br>Cargo: Jefe OSI</td></tr>
</table>
<br>Desde la OAPS se asegura que el contenido corresponde a la última versión vigente en ISOlución al momento de la migración a MIOsoft.</td></tr>
</table>

## FLUJO DE APROBACIÓN

| ELABORÓ | | APOYO OAPS | | REVISÓ | | APROBÓ | |
|---|---|---|---|---|---|---|---|
| Nombre: | | Nombre: | Jefferson López | Nombre: | | Nombre: | |
| Cargo: | | Cargo: | Profesional Especializado | Cargo: | | Cargo: | |