PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

INNOVATION TELECOMUNICACIONES SAS

1. OBJETIVO

Establecer los lineamientos y el procedimiento para la detección, identificación, registro, análisis, clasificación, contención, atención, recuperación, cierre y seguimiento de los eventos e incidentes de seguridad de la información que puedan presentarse en la organización.
El procedimiento tiene como finalidad permitir una respuesta oportuna y proporcional al nivel de riesgo, minimizar los impactos tecnológicos, operativos, económicos, legales y reputacionales, preservar las evidencias disponibles y facilitar el cumplimiento de las obligaciones legales y regulatorias aplicables.

2. ALCANCE

El presente procedimiento aplica a:

- Trabajadores, contratistas, proveedores y terceros que utilicen sistemas de información, recursos tecnológicos o tengan acceso autorizado a la infraestructura o información de la organización.
- Equipos de cómputo, dispositivos, servidores, aplicaciones, plataformas, servicios en la nube, redes, bases de datos, sistemas de telecomunicaciones y demás recursos tecnológicos utilizados por la organización.
- Información creada, recibida, almacenada, procesada, transmitida o eliminada mediante los recursos de la organización, independientemente de su formato.
- Incidentes que puedan comprometer información propia, de usuarios, clientes, trabajadores, proveedores o terceros.

3. DEFINICIONES

3.1. Evento de seguridad de la información

Situación, alerta, comportamiento o condición identificada en un sistema, servicio, red, aplicación o recurso tecnológico que pueda ser relevante para la seguridad de la información y que requiera, de acuerdo con sus características, validación o seguimiento.

Pueden constituir eventos de seguridad, entre otros:

- Intentos reiterados o anómalos de autenticación.
- Alertas generadas por herramientas de seguridad.
- Conexiones o tráfico inusual.
- Cambios inesperados en configuraciones.
- Comportamientos anormales de sistemas o dispositivos.

La existencia de un evento no implica necesariamente la existencia de un incidente.

3.2. Incidente de seguridad de la información

Evento o conjunto de eventos que comprometa o pueda comprometer de manera relevante la confidencialidad, integridad, disponibilidad o trazabilidad de la información, de los sistemas o de los servicios tecnológicos de la organización.

Son ejemplos:

- Accesos no autorizados.
- Infecciones por malware o código malicioso.
- Ataques de ransomware.
- Pérdida, alteración o eliminación no autorizada de información.
- Exposición o extracción no autorizada de información.
- Compromiso de credenciales.
- Interrupción de servicios críticos derivada de un evento de seguridad.
- Vulneración de sistemas o infraestructura tecnológica.
- Incidentes que involucren datos personales.

3.3. Incidente de seguridad de datos personales

Evento que genere acceso, consulta, uso, pérdida, adulteración, circulación, divulgación o tratamiento no autorizado o fraudulento de datos personales.
Cuando se identifique un incidente de esta naturaleza, deberá realizarse el análisis correspondiente para determinar las actuaciones y reportes exigibles conforme al régimen colombiano de protección de datos personales y demás normas aplicables.

3.4. Indicador de Compromiso – IoC

Dato o evidencia técnica que puede indicar la existencia de actividad maliciosa o no autorizada en un sistema o red.
Pueden comprender direcciones IP, dominios, URL, hashes, archivos, procesos, comportamientos, patrones de tráfico u otros elementos técnicos.

3.5. Evidencia digital

Información almacenada o transmitida en medios tecnológicos que puede resultar relevante para establecer las circunstancias, alcance, origen o consecuencias de un incidente.

4. PRINCIPIOS PARA LA GESTIÓN DE INCIDENTES

La gestión de eventos e incidentes se desarrollará atendiendo los siguientes principios:

Detección oportuna: procurar identificar los incidentes en el menor tiempo razonablemente posible.

Proporcionalidad: las medidas implementadas deberán corresponder a la naturaleza, alcance, criticidad y riesgo del incidente.

Registro y trazabilidad: los eventos relevantes y los incidentes deberán quedar documentados de manera que pueda realizarse seguimiento a las actuaciones adelantadas.

Preservación de evidencia: cuando corresponda, deberán adoptarse medidas razonables para evitar la alteración, pérdida o destrucción de información relevante para el análisis del incidente.

Confidencialidad: la información relacionada con los incidentes será conocida únicamente por las personas que deban intervenir en su gestión.

Continuidad: la respuesta deberá procurar minimizar las afectaciones sobre la operación y restablecer los servicios de manera segura.

Cumplimiento: deberán verificarse las obligaciones legales, regulatorias, contractuales y de protección de datos personales que resulten aplicables.

Mejoramiento continuo: los incidentes deberán utilizarse como fuente de información para fortalecer los controles y prevenir su repetición.

5. FUENTES DE DETECCIÓN E IDENTIFICACIÓN

Los eventos e incidentes podrán identificarse mediante fuentes tecnológicas, humanas o externas.

5.1. Fuentes tecnológicas

De acuerdo con la infraestructura, capacidad, riesgos y herramientas disponibles en la organización, podrán utilizarse:

- Antivirus y antimalware.
- Firewall.
- IDS/IPS.
- EDR/XDR.
- SIEM o herramientas de correlación y gestión de eventos.
- Sistemas de monitoreo de red.
- Registros o logs de servidores, bases de datos, aplicaciones, VPN y dispositivos de red.
- Herramientas de monitoreo de servicios en la nube.
- Sistemas de detección de anomalías.
- Herramientas de monitoreo de integridad.
- Demás soluciones implementadas por la organización.

La enumeración anterior no implica la obligación de implementar todas las herramientas señaladas. La organización determinará las soluciones aplicables de acuerdo con sus características, infraestructura, riesgos y recursos disponibles.

5.2. Fuentes humanas y externas

Los eventos también podrán ser identificados mediante:

- Reportes de trabajadores o usuarios.
- Reportes del área de tecnología o soporte.
- Hallazgos de auditorías.
- Reportes de clientes.
- Notificaciones de proveedores o terceros.
- Alertas provenientes de autoridades o equipos de respuesta a incidentes.
- Información pública sobre vulnerabilidades o amenazas relevantes para la infraestructura de la organización.

6. REPORTE DE EVENTOS E INCIDENTES

Toda persona que identifique una situación que razonablemente pueda constituir un incidente deberá reportarla inmediatamente mediante los canales establecidos por la organización.

El reporte deberá contener, cuando sea posible:

- Fecha y hora de identificación.
- Persona que realiza el reporte.
- Descripción de la situación.
- Equipo, sistema, aplicación o servicio afectado.
- Información disponible sobre la posible afectación.
- Evidencias disponibles.
- Acciones realizadas antes del reporte.

La persona que detecte el evento deberá evitar realizar acciones que puedan destruir evidencias o aumentar la afectación, salvo aquellas necesarias para proteger la integridad de las personas, la información o la continuidad de servicios críticos.

7. ANÁLISIS INICIAL Y CLASIFICACIÓN

Recibido el reporte o generada una alerta, el responsable designado realizará una valoración inicial o **triage**, que podrá comprender:

1. Validar la existencia del evento.
2. Analizar la información disponible.
3. Revisar registros, alertas y evidencias relacionadas.
4. Determinar los sistemas, servicios o información posiblemente afectados.
5. Identificar si el comportamiento corresponde a una actividad legítima.
6. Estimar el posible impacto.
7. Determinar si corresponde clasificarlo como evento o incidente.
8. Definir su nivel de criticidad y las medidas iniciales necesarias.

El análisis deberá realizarse con la mayor oportunidad posible, atendiendo la naturaleza y criticidad del evento.

8. CRITERIOS PARA LA DETERMINACIÓN DE UN INCIDENTE

Para determinar si un evento constituye un incidente podrán analizarse, entre otros, los siguientes elementos:

8.1. Indicadores técnicos

- Intentos anómalos o reiterados de autenticación.
- Elevación no autorizada de privilegios.
- Instalación o ejecución de software desconocido.
- Conexiones externas anómalas.
- Tráfico irregular.
- Cambios no autorizados en configuraciones.
- Archivos o procesos sospechosos.
- Compromiso de cuentas o credenciales.
- Detección de malware.

8.2. Impacto

Se analizará si el evento:

- Compromete datos personales.
- Afecta información confidencial.
- Produce interrupción total o parcial de servicios.
- Altera o destruye información.
- Permite acceso no autorizado.
- Genera exposición pública de información.
- Compromete infraestructura tecnológica.
- Puede afectar usuarios, clientes o terceros.

8.3. Probabilidad y nivel de amenaza

Podrá considerarse:

- Existencia de vulnerabilidades conocidas.
- Disponibilidad de actualizaciones o parches.
- Coincidencia con indicadores de compromiso.
- Existencia de campañas o amenazas conocidas.
- Exposición del activo comprometido.
- Facilidad de explotación de la vulnerabilidad.

9. CLASIFICACIÓN DEL INCIDENTE

Los incidentes podrán clasificarse de acuerdo con su impacto:
Bajo: afectación limitada, sin compromiso relevante de información ni interrupción significativa de servicios.
Medio: afectación controlada que involucra uno o varios activos, usuarios o servicios y requiere intervención técnica.

Alto: afectación significativa de información, sistemas o servicios, posible compromiso de datos personales o afectación relevante de la operación.
Crítico: compromiso grave de información o infraestructura, interrupción de servicios esenciales, afectación masiva de usuarios, exposición significativa de datos o situación que pueda generar consecuencias legales, regulatorias, económicas u operativas graves.
La organización podrá establecer criterios adicionales de clasificación de acuerdo con su infraestructura y nivel de riesgo.

10. REGISTRO DEL INCIDENTE

Todo incidente confirmado deberá registrarse como mínimo con:

- Número o código de identificación.
- Fecha y hora de detección.
- Fecha y hora del reporte.
- Fuente de detección.
- Descripción.
- Sistemas, servicios o activos afectados.
- Información posiblemente comprometida.
- Clasificación y criticidad.
- Responsable de la gestión.
- Evidencias disponibles.
- Medidas de contención adoptadas.
- Acciones de recuperación.
- Comunicaciones y escalamiento efectuados.
- Determinación sobre posibles reportes a autoridades.
- Fecha de cierre.
- Causa identificada, cuando pueda determinarse.
- Acciones correctivas o preventivas.

El registro deberá conservarse en condiciones que garanticen razonablemente su integridad, disponibilidad y acceso restringido.

11. CONTENCIÓN

Confirmado un incidente, deberán adoptarse las medidas razonables necesarias para limitar su propagación y reducir sus efectos.
Dependiendo de las circunstancias, podrán adoptarse acciones como:

- Aislar equipos o dispositivos comprometidos.
- Bloquear cuentas o credenciales.

- Restringir conexiones.
- Bloquear direcciones IP, dominios o servicios maliciosos.
- Suspender temporalmente servicios comprometidos.
- Segmentar redes.
- Preservar registros y evidencias.
- Activar mecanismos de continuidad.

Las medidas deberán procurar un equilibrio entre la seguridad, la preservación de evidencia y la continuidad del servicio.

12. ERRADICACIÓN Y RECUPERACIÓN

Controlado el incidente, deberán identificarse y eliminarse, cuando sea posible, sus causas o mecanismos de persistencia.
Las actividades podrán incluir:

- Eliminación de malware.
- Corrección de configuraciones.
- Instalación de actualizaciones.
- Cambio o restablecimiento de credenciales.
- Restauración de información desde respaldos confiables.
- Reinstalación o recuperación de sistemas.
- Cierre de vulnerabilidades identificadas.
- Validación de la integridad de los sistemas.

Antes del restablecimiento completo del servicio deberá verificarse razonablemente que el activo pueda retornar a operación en condiciones seguras.

13. PRESERVACIÓN DE EVIDENCIAS

Cuando la naturaleza del incidente lo requiera, se procurará:

- Preservar logs y registros relevantes.
- Documentar fecha, hora y fuente de obtención.
- Evitar alteraciones innecesarias de los sistemas comprometidos.
- Obtener copias de la información relevante cuando técnicamente corresponda.
- Utilizar mecanismos de verificación de integridad, como funciones hash, cuando resulte pertinente.
- Restringir el acceso a las evidencias.

- Documentar las personas que intervienen en su obtención, almacenamiento o transferencia.
- Cuando exista posibilidad de actuaciones administrativas, judiciales o penales, deberá evaluarse la aplicación de medidas adicionales para garantizar la adecuada preservación y manejo de la evidencia digital.

14. ESCALAMIENTO Y COMUNICACIONES

Los incidentes deberán escalarse según su criticidad a:

- Responsable de seguridad de la información o quien haga sus veces.
- Responsable del área de tecnología.
- Líder del proceso afectado.
- Representante legal o Alta Dirección, cuando corresponda.
- Área jurídica, cuando existan posibles implicaciones legales, regulatorias, contractuales o relacionadas con datos personales.

Ningún trabajador, contratista o tercero podrá realizar comunicaciones públicas sobre un incidente sin autorización.

15. INCIDENTES QUE INVOLUCREN DATOS PERSONALES

Cuando exista afectación real o potencial de datos personales deberá realizarse un análisis específico que permita establecer, entre otros:

- Categorías de datos involucrados.
- Número aproximado de titulares afectados, cuando pueda determinarse.
- Naturaleza y alcance de la afectación.
- Existencia de datos sensibles o de especial protección.
- Posibles consecuencias para los titulares.
- Medidas adoptadas para contener y mitigar el incidente.
- Obligaciones aplicables a la organización en calidad de Responsable o Encargado del Tratamiento.
- Procedencia de reportes, comunicaciones o actuaciones ante la Superintendencia de Industria y Comercio u otras autoridades competentes.

La existencia de un incidente de seguridad no implica automáticamente que deban efectuarse los mismos reportes ante todas las autoridades. El responsable jurídico y/o de protección de datos deberá determinar las obligaciones aplicables a cada caso.

16. OBLIGACIONES SECTORIALES Y REPORTE A AUTORIDADES

Cuando el incidente afecte redes o servicios de telecomunicaciones, infraestructura crítica, continuidad del servicio u otros aspectos sujetos a regulación especial, la organización deberá verificar las obligaciones de reporte y atención establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Comisión de Regulación de Comunicaciones y demás autoridades competentes, según corresponda.
Los reportes se efectuarán únicamente cuando se configuren los presupuestos establecidos en la normativa aplicable y dentro de los términos y mecanismos previstos por la autoridad competente.

17. CIERRE DEL INCIDENTE

Un incidente podrá cerrarse cuando:

- La amenaza haya sido contenida.
- Se hayan ejecutado las acciones razonables de erradicación.
- Los servicios afectados hayan sido recuperados o estabilizados.
- Se hayan preservado las evidencias necesarias.
- Se hayan efectuado los reportes que resulten obligatorios.
- Se hayan identificado las acciones correctivas o preventivas correspondientes.

El cierre deberá quedar documentado.

18. LECCIONES APRENDIDAS Y MEJORA

Los incidentes de criticidad alta o crítica y aquellos que puedan evidenciar debilidades relevantes deberán ser objeto de revisión posterior.
La revisión podrá establecer:

- Causa del incidente.
- Controles que fallaron o resultaron insuficientes.
- Efectividad de las acciones adoptadas.
- Necesidad de modificar configuraciones o procedimientos.
- Controles adicionales requeridos.
- Necesidades de capacitación.
- Acciones preventivas y responsables de su ejecución.

19. CAPACITACIÓN Y SENSIBILIZACIÓN

La organización promoverá actividades periódicas de sensibilización para que trabajadores y demás personas autorizadas puedan reconocer situaciones como:

- Correos o mensajes sospechosos.
- Solicitudes inusuales de credenciales.
- Enlaces o archivos potencialmente maliciosos.
- Comportamientos anormales de los equipos.
- Modificación inesperada de archivos.
- Instalación de aplicaciones desconocidas.
- Pérdida o sustracción de dispositivos.
- Accesos o solicitudes de información no habituales.

El personal deberá conocer los canales internos establecidos para reportar estas situaciones.

20. CONFIDENCIALIDAD

La información relacionada con eventos e incidentes deberá manejarse de manera reservada y únicamente podrá ser conocida por las personas autorizadas o que requieran intervenir en su atención.

El personal deberá abstenerse de divulgar información sobre incidentes a terceros, usuarios, medios de comunicación o redes sociales sin autorización de la organización, sin perjuicio de los reportes o comunicaciones exigidos por autoridad competente.

21. RESPONSABILIDADES

Usuarios, trabajadores y contratistas

- Cumplir las políticas de seguridad.
- Reportar oportunamente eventos o incidentes.
- Abstenerse de realizar acciones que puedan incrementar el impacto.
- Colaborar con el proceso de investigación y respuesta.

Área de Tecnología o quien haga sus veces

- Mantener los mecanismos de monitoreo definidos por la organización.
- Analizar alertas y reportes.
- Ejecutar medidas técnicas de contención, erradicación y recuperación.

- Preservar la información técnica y evidencias disponibles.
- Documentar las actuaciones realizadas.

Responsable de Seguridad de la Información o quien haga sus veces
- Coordinar la gestión de incidentes.
- Clasificar su criticidad.
- Coordinar las acciones de respuesta.
- Mantener el registro correspondiente.
- Promover acciones de mejora.

Responsable jurídico y/o de protección de datos
- Evaluar las implicaciones jurídicas del incidente.
- Determinar, conjuntamente con las áreas involucradas, las obligaciones de reporte o comunicación.
- Apoyar la gestión de incidentes que involucren datos personales, autoridades o terceros.

Alta Dirección
- Facilitar los recursos razonablemente necesarios.
- Participar en las decisiones asociadas a incidentes de alta criticidad.
- Promover el cumplimiento de las políticas de seguridad de la información.

22. MARCO NORMATIVO Y REFERENCIAS

El presente procedimiento deberá interpretarse de acuerdo con las normas que resulten aplicables a la organización, incluyendo, entre otras:

- Constitución Política de Colombia, particularmente las disposiciones relacionadas con intimidad, habeas data y protección de la información.

- Ley 1273 de 2009, sobre protección de la información y de los datos y delitos informáticos.

- Ley 1581 de 2012, régimen general de protección de datos personales.

- Decreto 1074 de 2015, en las disposiciones que compilan la reglamentación aplicable al régimen de protección de datos personales.

- Reglamentación e instrucciones expedidas por la Superintendencia de Industria y Comercio en materia de protección de datos personales y gestión de incidentes de seguridad.

- Normativa sectorial expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones y la Comisión de Regulación de Comunicaciones que resulte aplicable al proveedor.

- Lineamientos y buenas prácticas de seguridad digital emitidos por las autoridades colombianas competentes.

- ISO/IEC 27001 e ISO/IEC 27002, como estándares de referencia y buenas prácticas, cuando sean adoptados o utilizados por la organización.

23. REVISIÓN Y ACTUALIZACIÓN

El presente procedimiento deberá revisarse periódicamente y cuando:

- Se presenten cambios significativos en la infraestructura tecnológica.
- Se modifique la normativa aplicable.
- Se presenten incidentes que evidencien la necesidad de ajustar los controles.
- Se incorporen nuevos servicios o tecnologías.
- Los resultados de auditorías o evaluaciones de riesgo así lo recomienden.

Las modificaciones deberán ser aprobadas conforme a los mecanismos internos definidos por la organización.

FIN DEL DOCUMENTO