MAN-01 Gestión de Incidentes Versión: 1.0	Aprobado por: Gerencia de S.I Fecha: 28/02/2026

Contenido

1. Definiciones.....2

2. Marco de Referencia.....4

3. Objetivo.....7

4. Alcance.....7

5. Proceso de Gestión de Incidentes.....7

5.1. Preparación.....8

5.2. Detección y Análisis.....11

5.3. Respuesta.....15

5.4. Actividades Posteriores al Incidente.....18

6. Métricas de Desempeño del Proceso de Gestión de Incidentes.....19

MAN-01 Gestión de Incidentes Versión: 1.0	Aprobado por: Gerencia de S.I Fecha: 28/02/2026

1. Definiciones

- **Activo de información:** Elemento que tiene valor para la organización y requiere protección. Puede ser información, sistemas, infraestructura, personas o servicios.
- **Análisis de causa raíz:** Proceso sistemático para identificar el origen real de un incidente, con el fin de evitar su recurrencia.
- **Análisis de impacto:** Evaluación del efecto del incidente sobre la confidencialidad, integridad y disponibilidad de la información.
- **Backups (Respaldos):** Copias de seguridad de información o sistemas que permiten su restauración en caso de pérdida o daño.
- **Cadena de custodia:** Procedimiento que garantiza la integridad y trazabilidad de la evidencia digital desde su identificación hasta su uso en análisis o procesos legales.
- **Clasificación del incidente:** Proceso mediante el cual se categoriza el incidente según su tipo (malware, acceso no autorizado, denegación de servicio, entre otros) para facilitar su tratamiento.
- **Confidencialidad:** Propiedad que asegura que la información solo sea accesible a personas autorizadas.
- **CSIRT (Computer Security Incident Response Team):** Equipo designado para coordinar y ejecutar la respuesta ante incidentes de seguridad de la información.
- **Denegación de servicio (DoS):** Ataque o evento que impide la disponibilidad normal de un sistema o servicio mediante la saturación o bloqueo de recursos.
- **Detección:** Identificación de un evento que puede constituir un incidente de seguridad.
- **Disponibilidad:** Propiedad que garantiza que la información y los sistemas estén accesibles cuando se requieran.
- **Erradicación:** Fase del proceso de respuesta orientada a eliminar la causa raíz del incidente.

- **Evento de seguridad:** Cualquier ocurrencia identificable en un sistema o red. No todos los eventos constituyen incidentes.
- **Incidente de seguridad de la información:** Evento o conjunto de eventos que comprometen la confidencialidad, integridad o disponibilidad de la información.
- **Incidente relacionado con datos de tarjeta:** Evento que afecta o puede afectar sistemas que procesan, almacenan o transmiten datos de tarjeta de pago.
- **Integridad:** Propiedad que garantiza que la información no ha sido alterada de manera no autorizada.
- **Líder del CSIRT:** Responsable de coordinar la gestión del incidente y tomar decisiones técnicas y operativas.
- **Malware:** Software malicioso diseñado para afectar sistemas, robar información o interrumpir operaciones.
- **Matriz RACI:** Herramienta que define responsabilidades en un proceso mediante las categorías Responsable, Aprobador, Consultado e Informado.
- **Monitoreo:** Proceso continuo de revisión de eventos y registros para detectar comportamientos anómalos.
- **MTTD (Mean Time to Detect): Tiempo** promedio transcurrido desde la ocurrencia de un incidente hasta su detección.
- **MTTR (Mean Time to Recover):** Tiempo promedio necesario para restaurar un servicio afectado tras un incidente.
- **PCI DSS:** Estándar de seguridad que establece requisitos para proteger datos de tarjetas de pago.
- **Plan de respuesta a incidentes:** Documento formal que describe las actividades, roles y procedimientos para gestionar incidentes de seguridad.
- **Recuperación:** Fase en la que se restablece la operación normal de los sistemas afectados.

- **Severidad del incidente:** Nivel asignado al incidente según su impacto, alcance y criticidad para el negocio.
- **SIEM (Security Information and Event Management):** Herramienta que centraliza, correlaciona y analiza eventos de seguridad provenientes de múltiples fuentes.
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Marco de gestión basado en riesgos para proteger la información de la organización.

2. Marco de Referencia

Se realizó un análisis comparativo entre ISO 27035 y NIST SP 800-61, en el cual se identificaron las fases equivalentes, sus diferencias metodológicas y los elementos complementarios de cada enfoque.

Fase	ISO 27035	NIST SP 800-61	Diferencia Clave	Propuesta
Preparación	**Planificación y Preparación:** -Definir política de gestión de incidentes -Establecer equipo de respuesta (CSIRT) -Definir roles y responsabilidades -Crear procedimientos y playbooks -Capacitación y concienciación -Implementar herramientas de monitoreo	**Preparación:** -Políticas y procedimientos -Capacitación -Herramientas forenses -Configuración de monitoreo -Backups	ISO es más normativo; NIST más técnico	-Definir política de gestión de incidentes. -Establecer equipo de respuesta (CSIRT). -Definir roles y responsabilidades. -Crear procedimientos y playbooks. -Capacitación y concienciación. - Backups

				-Implementar herramientas de monitoreo.
Detección y análisis	**Detección y Reporte:** -Identificación de eventos -Registro de incidentes -Clasificación inicial -Evaluación preliminar	**Detección y ánalisis** - Identificación del incidente - Análisis técnico -Determinación del alcance -Documentación	NIST enfatiza análisis forense	Aquí se determina si el evento es realmente un incidente. - Identificación del incidente -Clasificación inicial y Severidad.
	Evaluación y Decisión: -Análisis técnico -Determinar severidad -Evaluar impacto (C-I-D) -Decidir estrategia de respuesta		NIST es más granular	
Respuesta	**Respuesta:** Contención Erradicación Recuperación Comunicación interna y externa	**Contención, Erradicación y recuperación:** -Contención a corto plazo. -Contención a largo plazo. - Eliminación de causa raíz. -Restauración de	NIST separa contención y erradicación	- Contención. - Eliminación causa Raiz - Restauración de sistemas. -Monitoreo y seguimiento. - Comunicación.

		sistemas. -Monitoreo post recuperación.		
Actividades post incidentes:	**Lecciones Aprendidas:** -Análisis post-incidente. -Mejora de controles. -Actualización de matriz de riesgos. -Ajustes a procedimientos.	**Actividades post incidentes:** -Lecciones aprendidas -Reporte final -Mejora de controles -Actualización de políticas	ISO lo integra a mejora del sistema	-Análisis post-incidente. -Actualización de matriz de riesgos. /Mejora de controles -Ajustes a procedimientos y actualización de políticas. -Reporte final - Lecciones aprendidas

Del análisis se concluye que:

- ISO 27035 establece el marco de gobierno, control y mejora continua.
- NIST SP 800-61 desarrolla con mayor profundidad la gestión operativa y técnica del incidente.
- Ambas normas son compatibles y pueden integrarse sin contradicción.

Adicionalmente, el proceso se alinea con el requisito 12.10 de PCI DSS 4.0.1, el cual exige un plan formal de respuesta a incidentes, definición de responsabilidades, procedimientos específicos ante compromiso de datos de tarjeta y pruebas periódicas del plan.

Con base en lo anterior, se estructura el siguiente proceso integrado dentro del SGSI.

3. Objetivo

Establecer el marco formal para la gestión de incidentes de seguridad de la información, garantizando una respuesta oportuna, controlada y documentada que minimice el impacto operativo, legal y reputacional.

4. Alcance

Aplica a todos los activos incluidos dentro del alcance del SGSI y, de manera prioritaria, a los sistemas que procesan, almacenan o transmiten datos sensibles o datos de tarjetas de pago.

Cuando el incidente involucre el entorno CDE, se activarán los lineamientos específicos establecidos para cumplimiento de PCI DSS 4.0.1.

5. Proceso de Gestión de Incidentes

El proceso se compone de cuatro fases principales:

1. Preparación
2. Detección y análisis
3. Respuesta
4. Cierre y mejora

5.1. Preparación

Responsable principal: Oficial de Seguridad de la Información

Objetivo de la fase: Garantizar que se cuente con capacidades organizativas, técnicas y procedimentales para responder a incidentes.

Actividades

a. Política y marco formal

- Definir y aprobar la política de gestión de incidentes.
- Definir alcance del proceso.
- Establecer obligación de reporte.

b. Designación del Equipo CSIRT

El Oficial de Seguridad designa formalmente el CSIRT, el cual debe quedar documentado.

Estructura mínima:

1. Líder del CSIRT
    - Coordina la respuesta.
    - Define severidad.
    - Autoriza acciones técnicas.
2. Responsable Técnico (TI)
    - Ejecuta análisis.
    - Implementa contención y recuperación.
3. Representante de Alta Dirección
    - Autoriza comunicaciones externas.
    - Toma decisiones estratégicas.

4. Jurídica (según necesidad)
    - Evalúa obligaciones regulatorias.
5. Comunicaciones (según necesidad)
    - Gestiona mensajes internos y externos.

c. Preparación técnica

Esta actividad tiene como finalidad garantizar que se cuente con medios técnicos y operativos suficientes para detectar, reportar y gestionar incidentes de forma oportuna.

Incluye:

- **Implementar herramientas de monitoreo:** Se debe contar con mecanismos que permitan la identificación temprana de eventos de seguridad 7 x 24, tales como:
    - Recolección y revisión periódica de logs.
    - Plataforma SIEM o herramienta equivalente.
    - Alertas automáticas en sistemas críticos.
    - Monitoreo de accesos privilegiados.
    - Registro de eventos en servidores, bases de datos y dispositivos de red.
- **Definir mecanismos de reporte interno**

Todo colaborador debe conocer cómo reportar un posible incidente. El mecanismo debe estar formalizado y comunicado.

Se podrán habilitar una o varias de las siguientes opciones:

1. Correo electrónico institucional exclusivo para incidentes

   Ejemplo: seguridad@empresa.com

   Permite centralizar reportes y mantener trazabilidad.

2. Formulario interno (intranet o herramienta de tickets)

   - Registro estructurado del evento.
   - Asignación automática de número de caso.
   - Seguimiento documentado.

3. Mesa de ayuda o Service Desk

   - Registro telefónico o presencial.
   - Clasificación inicial por personal de soporte.
   - Escalamiento al CSIRT.

4. Canal directo al Oficial de Seguridad

   - Debe quedar registro posterior del reporte.

- **Asegurar respaldos y pruebas periódicas**
  - Definir política de respaldos.
  - Establecer periodicidad.
  - Realizar pruebas de restauración.
  - Documentar evidencias de prueba.

Los respaldos deben cubrir información crítica y sistemas incluidos en el alcance del SGSI.

- **Formato para documentar el incidente**

  anexo FRM-01 Formato Incidente de seguridad de la información

- **Realizar prueba anual del plan**

Conforme a PCI DSS 4.0.1 requisito 12.10, el plan de respuesta a incidentes debe probarse al menos una vez al año o tras cambios significativos que puedan afectar el entorno de datos de tarjeta.

La prueba puede realizarse mediante:

- Simulación de incidente.
- Ejercicio de mesa.
- Escenario hipotético documentado.

Debe generarse acta con resultados, hallazgos y acciones de mejora.

5.2. Detección y Análisis

Responsable principal: Equipo de Monitoreo / Área TI

Objetivo de la fase: Determinar si un evento corresponde a un incidente y establecer su alcance y severidad.

¿Cómo se detecta un incidente?

La detección puede originarse por:

- Alertas automáticas de herramientas de monitoreo.
- Revisión de logs.

- Reporte de usuario.
- Notificación de proveedor.
- Hallazgo de auditoría.
- Alerta de marca adquirente (en caso PCI).

Todo evento debe registrarse formalmente. - anexo FRM-01 Formato Incidente de seguridad de la información

Identificación y Registro

- Asignar número de caso.
- Registrar fecha, hora y fuente.
- Describir evento inicial.
- Identificar activos involucrados.

Clasificación del incidente:

a) **Tipo de incidente:** La clasificación tiene como finalidad categorizar el incidente según su naturaleza técnica, lo que facilita la definición de la respuesta, el análisis del impacto y la priorización.

Tipo de Incidente	Definición	Ejemplos	Impacto Principal
Acceso no autorizado	Situación en la que una persona o sistema obtiene acceso a recursos sin autorización válida o	Uso de credenciales robadas, escalamiento de privilegios, acceso	Confidencialidad e Integridad

Tipo de Incidente	Definición	Ejemplos	Impacto Principal
	excediendo los privilegios asignados.	indebido a información restringida.	
Denegación de servicio (DoS)	Interrupción intencional o maliciosa de la disponibilidad de un sistema, aplicación o servicio mediante saturación o bloqueo de recursos.	Sobrecarga de solicitudes, saturación de red, caída de servicio por ataque externo.	Disponibilidad
Malware	Instalación o ejecución de software malicioso que afecta el funcionamiento normal de los sistemas.	Ransomware, virus, troyanos, spyware, scripts maliciosos.	Confidencialidad, Integridad y Disponibilidad
Pérdida de información	Eliminación, alteración o divulgación no autorizada de información sensible o crítica.	Borrado accidental de base de datos, envío erróneo de información, robo de dispositivo con datos.	Confidencialidad e Integridad
Compromiso de credenciales	Exposición o uso indebido de credenciales legítimas que permite acceso no autorizado.	Phishing, fuerza bruta, filtración de contraseñas, uso compartido indebido.	Confidencialidad
Incidente relacionado con	Evento que afecta o puede afectar sistemas que procesan, almacenan	Exposición de PAN, malware en sistema de	Confidencialidad y Cumplimiento PCI

Tipo de Incidente	Definición	Ejemplos	Impacto Principal
datos de tarjeta	o transmiten datos de tarjeta (CDE).	pagos, acceso no autorizado al entorno de tarjetas.	

b) Definición de Severidad

El Líder del CSIRT define la severidad considerando:

1. Impacto en el negocio
2. Alcance técnico
3. Tipo de información afectada
4. Existencia de datos de tarjeta

Niveles:

1. Crítico
   - Compromiso confirmado de datos de tarjeta
   - Interrupción total del servicio
2. Alto
   - Afectación significativa a operación
   - Posible exposición de información sensible
3. Medio

- Impacto limitado
- Sin evidencia de exfiltración

4. Bajo
    - Evento contenido sin impacto relevante

5.3. Respuesta

Una vez confirmado el incidente y definida su severidad, se ejecuta la estrategia de respuesta.

Responsable principal: Líder del CSIRT.

a) Contención

- Aislamiento de equipos.
- Bloqueo de accesos.
- Segmentación temporal.
- Deshabilitar accesos remotos.

b) Erradicación

- Eliminación de causa raíz.
- Corrección de vulnerabilidades.
- Actualización de configuraciones.
- Cambio de credenciales

c) Recuperación

- Restauración controlada.
- Validación de integridad.
- Monitoreo reforzado.

d) En caso de incidente PCI:

- Preservar evidencia.
- Notificar adquirente.
- No restaurar sin coordinación cuando aplique.

e) Comunicación del Incidente:

La comunicación debe realizarse de manera escalonada y controlada, de acuerdo con la severidad del incidente y el nivel de impacto.

1. Comunicación Interna

Se debe informar a:

- Oficial de Seguridad de la Información.
- Gerencia General.
- Área de TI.
- Área Jurídica (si hay posible impacto legal).
- Área de Comunicaciones (si existe impacto reputacional).

2. Comunicación Externa (si aplica)

- Clientes afectados.
- Proveedores críticos.
- Entidades regulatorias.
- Autoridades competentes.
- Marca adquiriente.

La activación de comunicación externa requiere aprobación de la Alta Dirección

Matriz de Interesados

Interesado	Tipo de Comunicación	Responsable
Gerencia	Informe ejecutivo	Oficial Seguridad
Clientes	Notificación formal	Comunicaciones
Regulador	Reporte obligatorio	Jurídica
Proveedor TI	Notificación técnica	TI

5.4. Actividades Posteriores al Incidente

Responsable principal: Oficial de Seguridad de la Información

Actividades

a. Análisis post-incidente

- Revisión cronológica del evento.
- Identificación de fallas en controles.

- Análisis de causa raíz.
- Revisión de controles.
- Ajuste de políticas o procedimientos.
- Presentación a la alta dirección.

b. Actualización de la Matriz de Riesgos

- Reevaluar riesgo materializado.
- Ajustar probabilidad o impacto.
- Definir nuevos controles si aplica.

c. Mejora de Controles

- Implementar controles adicionales.
- Ajustar configuraciones.
- Actualizar procedimientos.

d. Informe Final

Debe contener:

- Descripción del incidente.
- Impacto.
- Acciones ejecutadas.
- Evidencias.

- Recomendaciones.

Se presenta a la Alta Dirección.

6. Métricas de Desempeño del Proceso de Gestión de Incidentes

Las métricas permiten evaluar la efectividad del proceso y demostrar control ante auditorías internas, externas o evaluación PCI.

a) Indicadores de la Fase de Preparación

- **Prueba anual del plan**

  Indicador:

  Ejecución de prueba anual del plan de respuesta.

  Tipo: Cumplimiento (Sí / No)

  Debe existir evidencia documental.

- **Cobertura de monitoreo**

  Indicador:

  Porcentaje de activos críticos con monitoreo activo.

  Fórmula: (Activos críticos monitoreados / Total activos críticos) x 100

- **Pruebas de restauración de respaldos**

  Indicador:

  Porcentaje de pruebas de restauración exitosas.

  Fórmula: (Pruebas exitosas / Total pruebas realizadas) x 100

b) Indicadores de la Fase de Detección y Análisis

- **Tiempo promedio de detección**

  Indicador: Tiempo transcurrido entre ocurrencia del incidente y su identificación.

- **Tiempo promedio de clasificación**

  Indicador: Tiempo desde el registro hasta la asignación de severidad.

c) Indicadores de la Fase de Respuesta

- **Tiempo promedio de contención**

  Indicador: Tiempo transcurrido desde confirmación hasta control del incidente.

- **Tiempo promedio de recuperación**

  Indicador: Tiempo transcurrido desde la contención hasta restablecimiento del servicio.

- **Incidentes reabiertos**

  Indicador: Número de incidentes que requieren intervención posterior por falla en erradicación.