



Gestión de Ciberincidentes

Introducción

Un ciberincidente es cualquier evento que compromete la confidencialidad, integridad o disponibilidad de los sistemas de información. La gestión adecuada de ciberincidentes es crucial para minimizar los riesgos operativos, económicos y reputacionales. La falta de una respuesta efectiva puede llevar a interrupciones del negocio, pérdida de datos críticos, multas regulatorias y daños a la reputación.

Identificación y Detección



Para detectar amenazas en tiempo real, las empresas utilizan diversas técnicas y herramientas:

- SIEM (Security Information and Event Management): Agrega y analiza eventos de seguridad en tiempo real.
- EDR (Endpoint Detection and Response): Supervisa y responde a actividades sospechosas en los endpoints.
- Correlación de Eventos: Relaciona datos de múltiples fuentes para identificar patrones de amenaza.

Contención y Respuesta

Los pasos inmediatos para minimizar el impacto de un incidente incluyen:

- Segmentación de Red: Aislar segmentos comprometidos para evitar la propagación.
- Revocación de Accesos: Retirar permisos a usuarios comprometidos.
- Mitigación de la Amenaza: Implementar contramedidas específicas para neutralizar el ataque.

Erradicación y Recuperación



Para eliminar la amenaza y restaurar sistemas:

- Eliminación Completa de la Amenaza: Borrar todas las huellas del atacante.
- Restauración desde Copias de Seguridad Seguras: Reinstalar datos y sistemas desde backups no comprometidos.
- Validación de la Integridad Post-Incidente: Asegurarse de que todos los sistemas funcionan correctamente y están libres de amenazas.

Evaluación Post-Incidente



El análisis posterior al incidente es vital para mejorar la resiliencia:

- **Análisis Forense:** Estudiar el incidente para entender como ocurrió .
- **Auditorías Internas:** Revisar los controles y políticas de seguridad.
- **Ajustes en Estrategias de Ciberseguridad:** Mejorar las defensas en base a lecciones aprendidas.

Normativas y Cumplimiento



Las empresas deben seguir leyes y regulaciones específicas:

- **RGPD:** Informe de incidentes dentro de las 72 horas.
- **NIS2:** Plazos y medidas para infraestructuras críticas.
- **LOPDGDD:** Regulaciones nacionales complementarias.

Las sanciones por incumplimiento pueden incluir multas significativas y responsabilidades legales.

Ejemplos Prácticos

Tipo de Incidente	Impacto	Medidas Tomadas	Tiempo de Recuperación
Ransomware	Interrupción total de servicios	Pago de rescate, Restauración de sistemas	1 semana
Phishing	Robo de credenciales	Revocación de accesos, Cambio de contraseñas	2 días
Malware	Compromiso de datos	Eliminación de malware, Restauración de datos	3 días

Acciones Recomendadas en Cada Fase del Incidente

Fase	Acciones
Identificación	Uso de SIEM y EDR, Monitoreo de actividad sospechosa
Contención	Segmentación de red, Revocación de accesos
Erradicación	Eliminación de amenazas, Limpieza de sistemas
Recuperación	Restauración de sistemas, Validación postincidente
Evaluación	Análisis forense, Auditoría interna

Herramientas Utilizadas Según el Tipo de Amenaza

Tipo de Amenaza	Herramientas
Ransomware	Antivirus, SIEM, Backups
Phishing	Filtros de correo, EDR
Malware	Antimalware, EDR, SIEM

Responsabilidades Dentro de la Empresa en la Gestión del Incidente

Rol	Responsabilidades
CEO	Dirección estratégica, Comunicación con stakeholders
CISO	Liderazgo técnico, Coordinación de respuesta
Equipo de TI	Implementación de medidas, Monitoreo continuo
RRHH	Capacitación, Manejo de comunicación interna

Comparación de Plazos de Notificación Según la Normativa Aplicable

Normativa	Plazo de Notificación
RGPD	72 horas
NIS2	Varía según la infraestructura
LOPDGDD	Tan pronto como sea posible

Organismos Nacionales e Internacionales en Ciberseguridad

En el ámbito de la ciberseguridad, existen organismos encargados de establecer normativas, gestionar incidentes y proteger infraestructuras críticas. A continuación, se presenta una tabla con los principales organismos nacionales e internacionales, junto con sus contactos oficiales.

País/Región	Organismo Responsable	Sitio Web/Contacto
España	INCIBE (Instituto Nacional de Ciberseguridad)	www.incibe.es · Tel: 017
España	AEPD (Agencia Española de Protección de Datos)	www.aepd.es · Tel: 901 100 099 · info@aepd.es
Unión Europea	ENISA (Agencia de Ciberseguridad de la UE)	www.enisa.europa.eu
EE.UU.	CISA (Cybersecurity & Infrastructure Security Agency)	www.cisa.gov · Tel: +1 888-282-0870
México	INAI (Protección de Datos)	www.inai.org.mx
México	CSIRT-MX (Centro de Respuesta a Incidentes de México)	Contacto: contacto@csirt.gob.mx
Argentina	Dirección Nacional de Protección de Datos Personales	www.argentina.gob.ar/protecciondedatos
Colombia	ColCERT (Equipo de Respuesta a Incidentes)	www.colcert.gov.co
Brasil	ANPD (Autoridade Nacional de Proteção de Dados)	www.gov.br/anpd
Chile	CSIRT-Gob (Centro de Respuesta a Incidentes del Gobierno)	www.csirt.gob.cl
Peru	PCM-CERT (Centro de Respuesta a Incidentes)	Contacto: soporte@pcm.gob.pe
Ecuador	CSIRT-ECU (Centro de Respuesta a Incidentes)	Contacto: seguridad@ec-cert.gov.ec
Canada	Canadian Centre for Cyber Security	www.cyber.gc.ca
Reino Unido	NCSC (National Cyber Security Centre)	www.ncsc.gov.uk
Interpol	Unidad de Ciberdelitos	www.interpol.int
OEA	CICTE (Comité Interamericano contra el Terrorismo)	www.oas.org

Estos organismos son clave para la respuesta ante incidentes, la formulación de políticas de ciberseguridad y la protección de infraestructuras críticas. La cooperación internacional es fundamental para enfrentar las amenazas digitales de manera efectiva.