CURSO

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Profesor: Lautaro Cabezas

UNIDAD 1

PRINCIPIOS Y CONCEPTOS FUNDAMENTALES DE LA GESTIÓN DE INCIDENTES

Contenidos

- Entendiendo los Ciberataques.
- Conceptos básicos y principios de la gestión de incidentes.
- Objetivos de la gestión de incidentes.
- Ventajas y Beneficios de un enfoque estructurado.
- Marcos de gestión de incidentes de Seguridad de la información.

Objetivo General

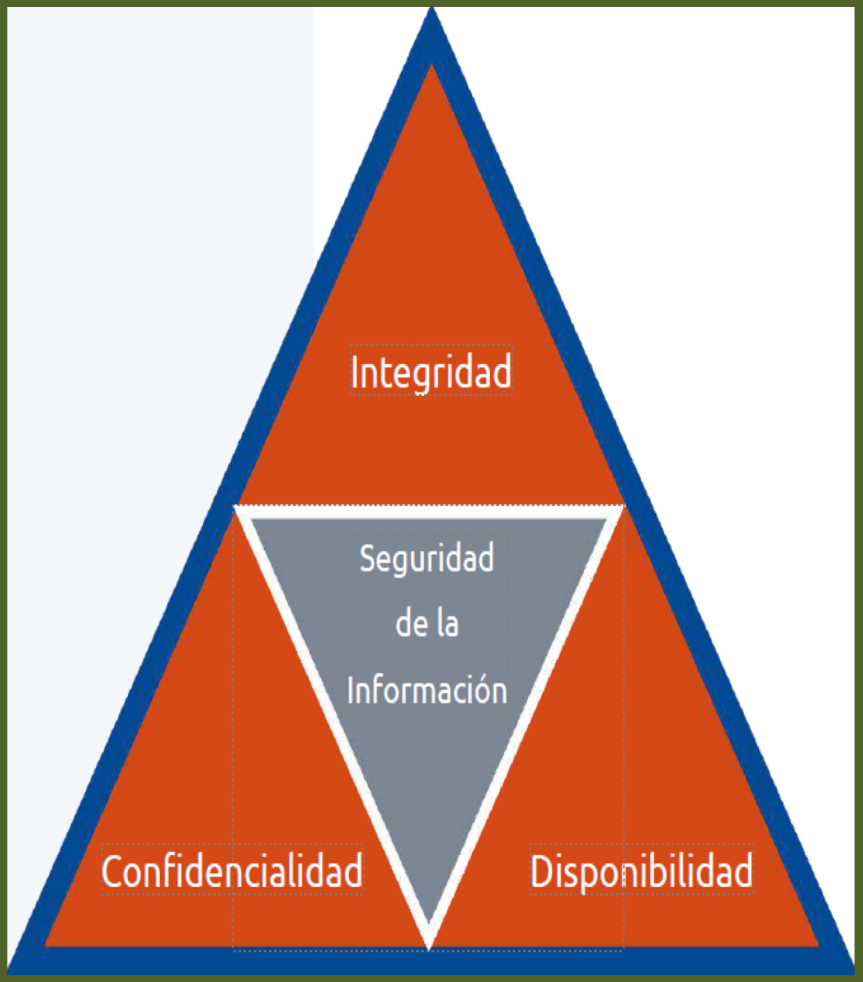
- Desarrollar competencias en "Respuesta a Incidentes de Seguridad de la Información", que les permita a los participantes realizar análisis de antecedentes en forma eficaz de los incidentes que puedan afectar la integridad de la información disponible de la institución.

- Que, adquieran herramientas, que puedan identificar, evaluar, contener y erradicar los posibles incidentes y amenazas. A fin que se pueda minimizar cada impacto que pueda vulnerar la seguridad de la información.

Seguridad de la información

Comprende todas las medidas y actividades que intentan proteger los activos de información, es decir, la protección de la información o datos que tienen valor para una organización, a través de la reducción de riesgos y mitigando las amenazas posibles.

Seguridad de la información



Se preocupa de la preservación de la:

- Confidencialidad
- Integridad
- Disponibilidad de la información.

La triada de seguridad de la información

- Confidencialidad: La información debe ser divulgada sólo a personas y procesos autorizados.

- Integridad: La información debe estar libre de modificaciones no autorizadas.

- Disponibilidad: La información debe encontrarse a disposición de quienes deben acceder a ella.

Ejemplos de activos de información según la organización

Para una compañía de Tele-comunicaciones

- Sus bases de clientes y planes.

Para una clínica privada

- Las fichas medicas de sus pacientes.

Para una compañía minera

- Un plan de expansión a un nuevo yacimiento.

Para una institución educacional

- Las fichas académicas de sus alumnos.
- Las concentraciones de notas.

¿Cuáles serían los activos a proteger por parte de carabineros?

Los activos a proteger por parte de carabineros

Carabineros de Chile protege una amplia gama de activos:

- La seguridad pública
- El orden público
- La vida y dignidad humana
- Los bienes tanto públicos como privados.

Además, resguardan:

- La legalidad
- Velan por el cumplimiento de las leyes
- Normativas vigentes.

Importancia para Instituciones Públicas

- Riesgos crecientes de ciberataques.
- Pérdida de datos sensibles o estratégicos.
- Impacto en la seguridad nacional y confianza ciudadana.

¿Qué es un Ciberataque?

- Acceso no autorizado, sabotaje o bloqueo de sistemas.

- Ejemplos: ransomware, phishing, denegación de servicio (DoS).

Ejemplo Real: Instituciones Públicas

- Un ejemplo de ciberataque de ransomware a un organismo público en Chile es el ataque que sufrió el Servicio Nacional del Consumidor (SERNAC) en 2022. Este ataque, realizado con ransomware, interrumpió los sistemas y servicios online del organismo, y se extendió a servidores Microsoft y VMware ESXi, según reportó el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Chile. Los atacantes cifraron los archivos, cambiando su extensión a .crypt, y solicitaron un rescate para evitar la publicación de la información robada en la dark web.

Reflexión

- ¿Estamos preparados para enfrentar un incidente digital?

- ¿Cómo responderías si tu unidad recibe un ataque?

¿Qué es la Gestión de Incidentes?

- Proceso estructurado para detectar, analizar y responder.

- Ciclo de vida: detección, análisis, contención, erradicación, recuperación y mejora continua.

Rol de Carabineros

- Apoyo en ciberseguridad institucional
- Preservación de evidencia digital
- Coordinación con CSIRT nacional

Objetivos de la Gestión de Incidentes

- Minimizar daños
- Restaurar operaciones
- Mejorar capacidades futuras
- Cumplir normativas
- Proteger la reputación y confianza

Beneficios de un Enfoque Estructurado

- Respuesta rápida
- Continuidad operativa
- Mejora continua
- Registro y trazabilidad

Ejercicio Breve

Identifica incidentes posibles en tu unidad:

- Filtración de correos
- Acceso no autorizado
- Robo de información

¿Qué son los marcos de gestión de incidentes de seguridad de la información?

Es un conjunto estructurado de procesos, procedimientos y herramientas que una organización utiliza para identificar, analizar, responder y aprender de los incidentes de seguridad. Estos marcos ayudan a las organizaciones a minimizar el impacto de los incidentes, restaurar las operaciones normales rápidamente y mejorar su postura general de seguridad.

Marco NIST SP 800-61

1. Preparación
2. Detección y análisis
3. Contención
4. Erradicación
5. Recuperación
6. Lecciones aprendidas

Marco SANS

Seis pasos clave similares al NIST:

1. Preparación
2. Identificación
3. Contención
4. Erradicación
5. Recuperación
6. Lecciones aprendidas

Otros Marcos Internacionales

- ISO 27001 / 27005
- CSIRT Services Framework
- NIST Cybersecurity Framework
- PCI-DSS, COBIT, CIS Controls

CSIRT Chile

- Apoyo técnico a organismos del Estado
- Recepción de incidentes
- Coordinación nacional

Sugerencias para Carabineros

- Inventario de sistemas críticos
- Planes de contingencia
- Canales de comunicación internos/externos

Proceso NIST Paso a Paso

1. Preparación
2. Detección y análisis
3. Contención
4. Erradicación
5. Recuperación
6. Lecciones aprendidas

Entendiendo los ciberataques

- ¿Qué es un ciberataque? Intento deliberado y malicioso de interrumpir, dañar o acceder ilegalmente a sistemas informáticos, redes o dispositivos digitales, a menudo con el objetivo de robar datos, interrumpir servicios o causar daños.

- Motivos: Espionaje, sabotaje, extorsión, activismo.

- Tipos comunes: phishing, ransomware, DDoS, explotación de vulnerabilidades.

Clasificación de incidentes de seguridad

- Por naturaleza: Accesos indebidos, malware, pérdida de dispositivos, etc.

- Por severidad: Bajo, medio, alto, crítico.

Principios de la gestión de incidentes

- Rapidez en detección y respuesta.
- Minimización del impacto.
- Coordinación y comunicación eficaz.
- Mejora continua.

Ventajas de un enfoque estructurado

- Menor tiempo de inactividad.
- Mejor coordinación del equipo.
- Cumplimiento normativo.
- Reducción de impactos financieros y reputacionales.

Actores de Amenazas

1. Internos: Empleados descontentos, negligencia.

2. Externos: Hackers, ciberdelincuentes, grupos APT.

3. Perfil y motivación de cada actor.

Indicadores de compromiso (IoC)

1. Evidencias técnicas de intrusiones (IP sospechosa, hash malicioso, etc.).

2. Cómo se detectan: SIEM, virustotal, antivirus, análisis forense digital.

3. Ejemplos de IoC reales: Hashes de archivos maliciosos:

   Si se detecta un archivo con un hash (como MD5 o SHA256) conocido por ser malware, ese hash se convierte en un IoC.

Ejemplos varios de Indicadores de compromiso (IoC)

1. Archivos nuevos o modificados con nombres inusuales:

La aparición de archivos con nombres extraños o extensiones inusuales en ubicaciones inesperadas puede ser una señal de alerta.

2. Cambios en archivos de configuración del sistema:

Modificaciones en el registro de Windows o archivos de configuración del sistema operativo, especialmente si se busca la persistencia del malware, son IoCs.

3. Actividad de usuario anómala:

Acceso a archivos o sistemas que no son usuales para un usuario específico, o intentos de acceso desde ubicaciones geográficas inusuales, pueden ser IoCs.

Herramientas y tecnologías clave

1. SIEM: correlación y monitoreo en tiempo real.
2. IDS/IPS: detección y prevención.
3. SOAR: automatización de respuesta.
4. Menciones de herramientas: Splunk, AlienVault, Qradar (plataformas de gestión de seguridad de redes), etc.

Aspectos éticos y legales

- Manejo responsable de la información.
- Respeto a la privacidad de los usuarios.
- Legislación aplicable: Ley de protección de datos, notificación obligatoria.

Comunicación y reportes de incidentes

- Importancia de la transparencia interna.
- Cómo y cuándo notificar a autoridades.
- Comunicación efectiva y control de crisis.

Errores comunes

- Subestimar señales de alerta.
- Falta de registro/documentación.
- No ejecutar lecciones aprendidas.
- Falta de simulacros en tiempo real.

Plantillas de Registro

- Fecha y hora de detección
- Sistemas afectados
- Tipo de incidente
- Responsables asignados

Plan de Contención

- Aislar dispositivos
- Desactivar accesos
- Comunicar rápidamente

Recuperación y Monitoreo

- Restaurar desde backups
- Validar sistemas
- Supervisión por X días

Roles y responsabilidades

- CSIRT: Equipo de respuesta a incidentes.
- Ciso: Encargado de seguridad digital estratégica.
- Personal idóneo: Analistas de seguridad, personal de TI, legal, comunicaciones.

Resumen Final

- Los incidentes son inevitables
- La preparación y estructura marcan la diferencia
- Existen marcos claros y adaptables

Reflexión Final

- ¿Está mi unidad preparada?
- ¿Contamos con protocolos, responsables y herramientas?

Preguntas

1. ¿Cuál es el primer paso del NIST?
2. ¿Qué beneficios trae una gestión estructurada?
3. ¿Qué rol cumple Carabineros ante un ciberincidente?

Gracias