Oficial de Protección Certificado
Certified Protection Officer

CPO©

Protección de Información

CPO©

INSTRUCTOR

CPP©

Carlos Ramírez Rodríguez, CPP

Consultor internacional en seguridad convergente, ciberseguridad y gestión de riesgos, con amplia experiencia liderando proyectos de protección de infraestructuras críticas en sectores como energía, minería y telecomunicaciones.

Es miembro activo de ASIS International e IFPO, y ha sido expositor en congresos internacionales sobre protección de activos, ciberdefensa y cultura de seguridad.

Fundador de Smart Spartans, empresa dedicada al cumplimiento normativo y la integración de seguridad física y cibernética, y creador de la plataforma SECURIX, una solución tecnológica para la gestión de incidentes y riesgos convergentes.

Autor del libro “Defensa Total: Ciberseguridad y Seguridad Física en la Protección de Infraestructuras Críticas”, reconocido por su enfoque innovador en la formación de profesionales de seguridad moderna.

Su misión es elevar el nivel profesional del sector de la protección, inspirando a los futuros Oficiales Certificados CPO a comprender que la verdadera prevención se logra con conocimiento, ética y liderazgo.

OBJETIVO DEL UNIDAD

1. Entender las definiciones importantes relacionadas con la seguridad de la información y la contrainteligencia.
2. Explicar la diferencia entre 'contrainteligencia' como se utiliza en el sector privado versos del sector del gobierno federal.
3. Describen las principales amenazas a la información y los recursos intangibles en el sector público y privado.
4. Identificar diversos tipos de vulnerabilidades de seguridad de la información, mitigación razonable del riesgo y contramedidas de seguridad.
5. Detallar el papel del oficial de protección profesional y los proveedores de servicios de seguridad en la protección de la información sensible y los recursos intangibles.

Protección de la Información

La protección de la información ya no es un tema técnico ni de espías, sino un mecanismo vital de resguardo en un mundo impulsado por la tecnología y los negocios.

Su gestión adecuada puede determinar el futuro de una compañía.

Demostración de un Ciberataque

https://www.youtube.com/watch?v=Vsb0x1mcNyc

Información Crítica

CPO©

Información crítica

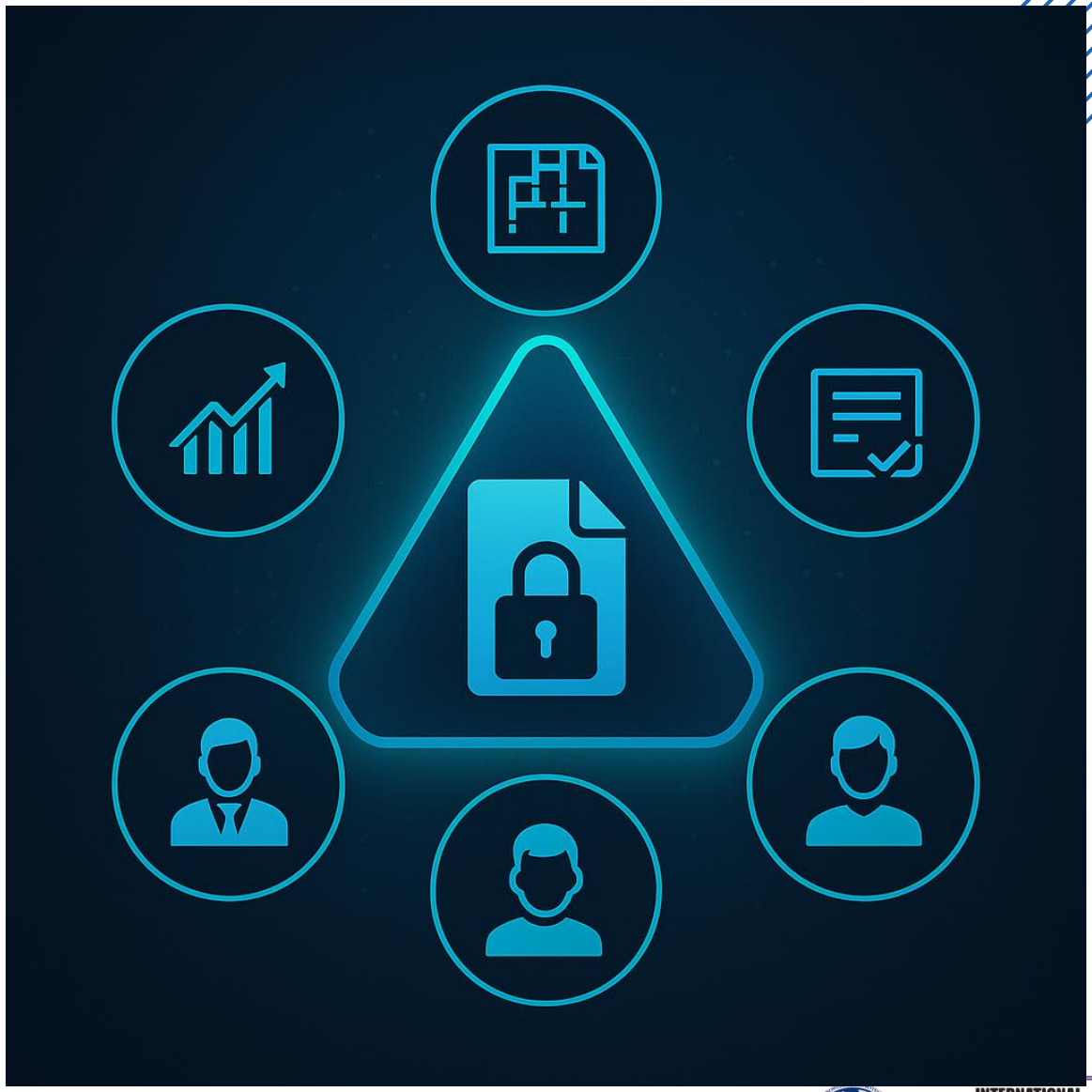
Información Crítica: el núcleo del valor corporativo

Un pequeño porcentaje de información propietaria puede cambiar el rumbo de una empresa —positiva o negativamente.

Ejemplos de información crítica:

1. Planes estratégicos y financieros.
2. Diseños, planos y proyectos.
3. I+D, patentes y programas.
4. Contratos y acuerdos legales.
5. Datos de clientes y empleados.

Su exposición o pérdida puede afectar la competitividad, reputación y continuidad del negocio.



Factores de Políticas y Procedimientos

“Dos pilares de la protección de la información”

La protección se basa en dos preguntas esenciales:

1. ¿Quién debe tener acceso? (Necesidad de conocer)
2. ¿Cómo se mantiene la información? (Forma y custodia)

El nivel de acceso depende del nivel de criticidad.

Principio de Necesidad de Conocer

‘Need to know’ = Menos exposición, más seguridad.

Solo acceden quienes requieren la información para cumplir sus funciones.

Ejemplo práctico:

- Todo el personal conoce el manual de emergencias.
- Solo algunos tienen acceso a los planos de seguridad o códigos de alarma.

Formas de la Información

- Documento físico: fácil de guardar, pero vulnerable a pérdida o incendio.

- Archivo digital: accesible, pero susceptible a intrusiones o malware.

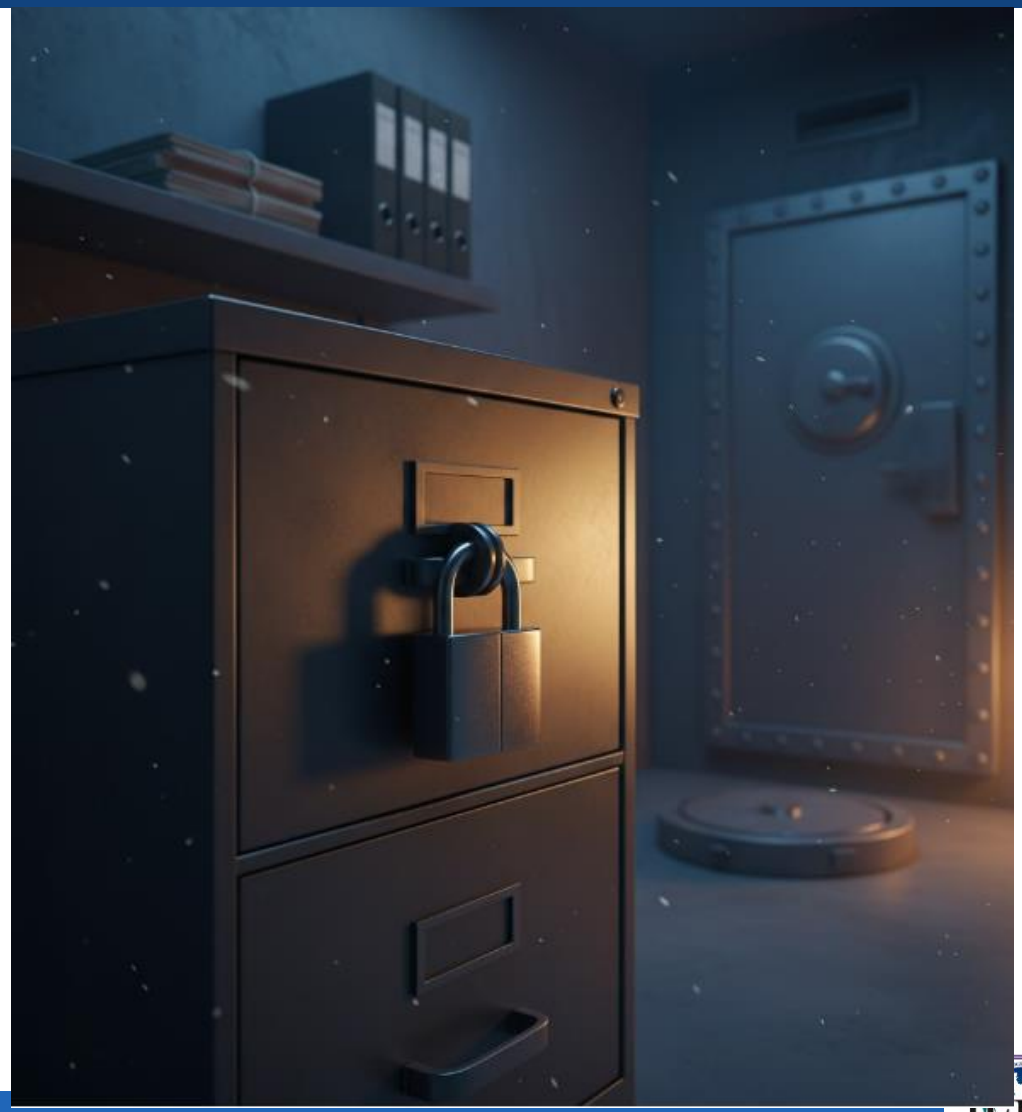
En ambos casos, el objetivo principal es mantener control y trazabilidad.

Documentos de Papel

Medidas básicas:

- Guardar en áreas restringidas.
- Control de acceso físico.
- Protección contra fuego, agua y manipulación.
- Destrucción segura (triturado / bóveda).

“Si no puede entrar al cuarto, no puede acceder al contenido.”



Información Electrónica y protección Física

Riesgos electrónicos:

- Accesos remotos no verificados.
- Contraseñas débiles.
- Datos sin cifrar en tránsito.

Controles físicos complementarios:

- Auditorías periódicas.
- Inspección de cableado y equipos.
- Protección de salas de servidores.
- Vigilancia frente a espionaje o sabotaje

Métodos Legales para asegurar la Información

“La protección legal: el respaldo invisible de la seguridad corporativa”

- La protección de la información no depende solo de la tecnología o de los controles físicos.
- Los métodos legales refuerzan el resguardo y otorgan validez jurídica ante una fuga o uso indebido.

Herramientas principales:

- Secreto comercial.
- Patentes y propiedad intelectual.
- Acuerdos de confidencialidad (NDA).

El Secreto Comercial

Información propietaria que otorga ventaja competitiva.

Para ser clasificada como secreto comercial debe:

1. Ser propiedad legítima de la organización.
2. Estar protegida de forma efectiva por su dueño.
3. Estar etiquetada como “confidencial”.
4. Tener acceso restringido.
5. Entregarse solo bajo acuerdo de confidencialidad.

No tiene vencimiento: dura mientras se mantenga en secreto.

Patentes y Propiedad Intelectual

Patentes:

- Protegen invenciones nuevas, útiles y no obvias.
- Deben registrarse y hacerse públicas.
- Duran generalmente 20 años.
- No son renovables.

Propiedad Intelectual:

- Protege obras de autor (informes, software, manuales, diseños).
- Vigente durante la vida del autor + 70 años post mortem.
- Evita copias o uso sin autorización.

Acuerdos de Confidencialidad (NDA)

Acuerdos de Confidencialidad = Compromiso formal para proteger información sensible.

Aplican entre:

- ❑ Empleados y empleadores.
- ❑ Proveedores, contratistas y clientes.
- ❑ Colaboradores externos y socios estratégicos.

Cláusulas clave:

- ❑ Alcance y definición de la información confidencial.
- ❑ Obligaciones de las partes.
- ❑ Duración y sanciones por incumplimiento.

Integración: Legal + Seguridad

Protección integral = Legal + Física + Cibernética

- Los métodos legales dan sustento formal a las medidas técnicas.
- Permiten actuar frente a fugas, espionaje o robo de información.
- Transforman la seguridad en un sistema de responsabilidad compartida.

Fuentes de Amenaza

“¿De dónde provienen las amenazas a la información?

Las fuentes de amenaza dependen del tipo de información y del valor que tenga en el mercado.

Principales categorías:

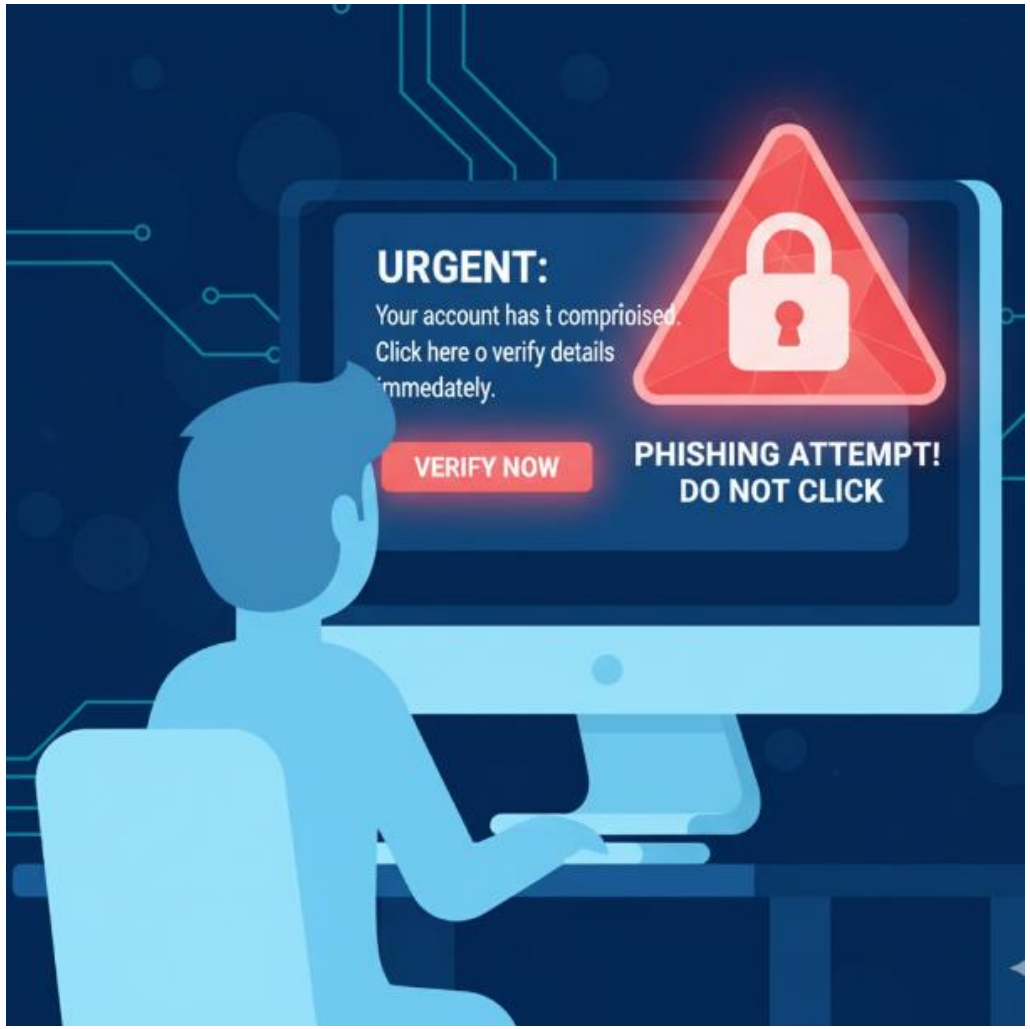
- Empleados no capacitados.
- Empleados descontentos.
- Espionaje corporativo.
- Ataques maliciosos externos.

Empleados no Capacitados

La ignorancia también es una vulnerabilidad.

- ❑ No saben cómo detectar intentos de acceso.
- ❑ Pueden entregar información por error (phishing, llamadas, redes sociales).
- ❑ No reconocen la ingeniería social como amenaza.

Solución: Capacitación continua + cultura de reporte.



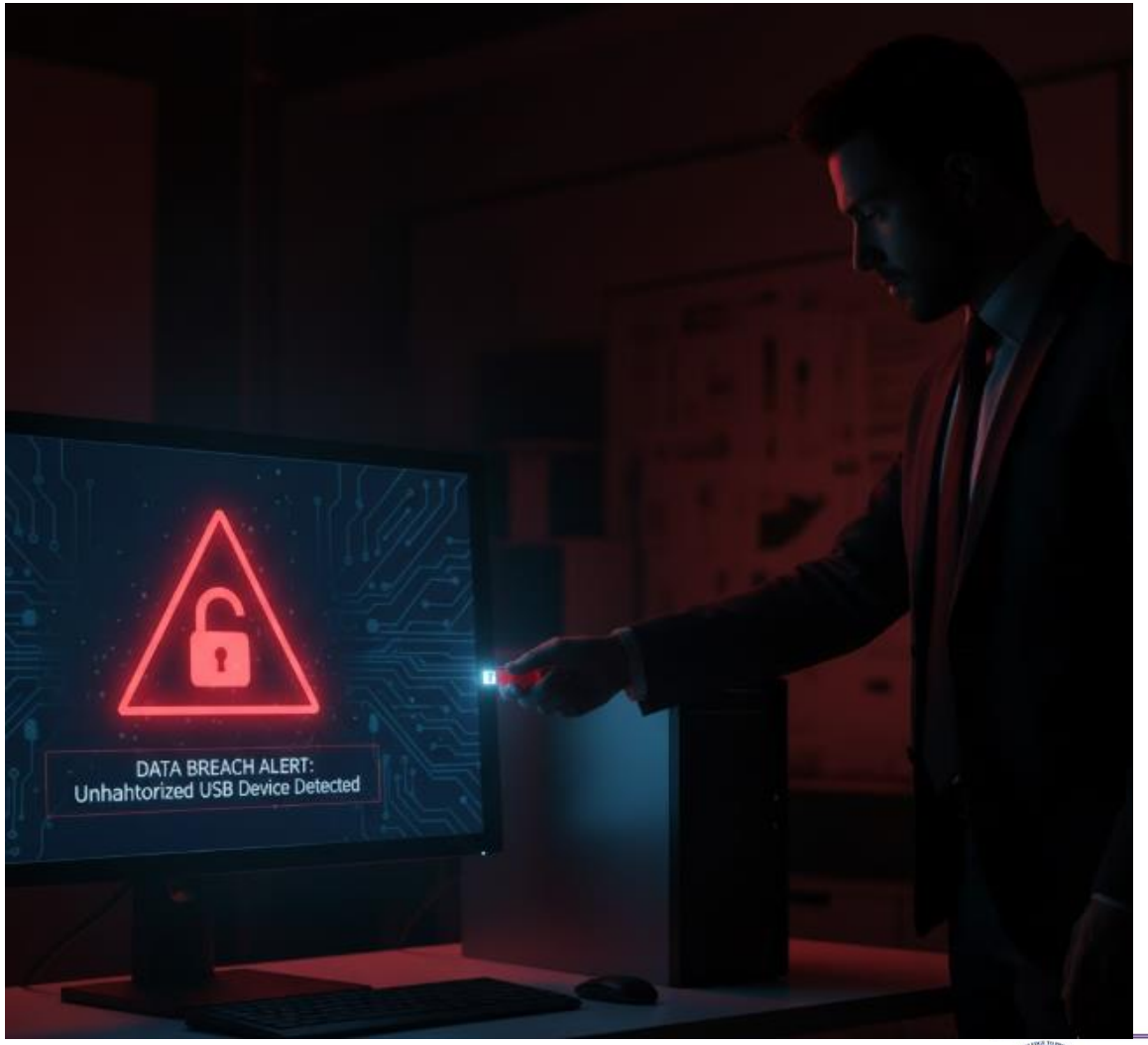
Empleados Descontentos

La amenaza interna más peligrosa.

- Motivados por resentimiento, venganza o inconformidad.
- Pueden tener acceso privilegiado.
- Pueden destruir o filtrar información crítica.

Medidas:

- Control de accesos.
- Revocación inmediata de credenciales.
- Monitoreo de actividad inusual.



Espionaje Corporativo

La competencia desleal también es una amenaza.

- ❑ Roban información estratégica o comercial.
- ❑ Utilizan ingeniería social, sobornos o infiltración.
- ❑ Apuntan a sectores de alto valor: energía, tecnología, defensa, salud.

Contramedidas:

- ❖ Clasificación de información.
- ❖ Acuerdos de confidencialidad.
- ❖ Control de dispositivos y visitantes.

Ataques Maliciosos Externos

Los cibercriminales no siempre buscan dinero.

- ❑ Hackers, Ransomware, sabotaje o robo de identidad
- ❑ Pueden actuar por vandalismo, activismo o simple curiosidad.
- ❑ El daño depende del nivel de sofisticación y del valor de la información.

Medidas:

- ❖ Cifrado.
- ❖ Copias de respaldo.
- ❖ Firewalls y monitoreo constante.

La Amenaza es Evolutiva

Las amenazas cambian, pero los principios permanecen:

- Capacitar
- Controlar
- Clasificar
- Concienciar

La mejor defensa no es la tecnología, sino personas informadas, responsables y vigilantes.

Conclusión: El Valor de la Información

“La información: un activo que solo existe si está protegida”

- Toda información que tiene valor también tiene un riesgo.
- Su protección debe ser proporcional a su importancia.
- Ningún secreto es seguro sin una gestión activa.
- La seguridad no es un estado, es una actividad continua.

La Evolución de la Protección

La protección de la información ya no se limita al secreto:

- Privacidad de datos personales.
- Confidencialidad corporativa.
- Integridad de sistemas.
- Disponibilidad operativa.

El profesional CPO debe entender que la información tiene valor intrínseco y debe tratarla como un activo de seguridad.

Las Tres Medidas Claves

“Tres pilares de la protección de información”

Medidas de Prevención

- ❑ Evitar pérdida, daño o alteración.
- ❑ Controles físicos, técnicos y administrativos.
- ❑ Ejemplo: acceso restringido a salas de servidores.

Medidas de Mitigación

- ❑ Detectar alteraciones, robos o fugas.
- ❑ Alarmas, auditorías, monitoreo continuo.

Medidas de Respuesta

- ❑ Recuperar información dañada o perdida.
- ❑ Restaurar operaciones y aprender del incidente.

El Rol del Oficial de Protección

El Oficial de Protección debe:

- Comprender el valor y las amenazas a la información.
- Promover políticas de acceso y clasificación
- Integrar la seguridad física, digital y legal.
- Mantener cultura de mejora continua.

“No se puede proteger lo que no se comprende.”

El Robo de Alta Tecnología

CPO©

Robo de Tecnología en el Lugar de Trabajo

“El nuevo rostro del robo corporativo: la tecnología como blanco”

- El robo dentro del lugar de trabajo ha evolucionado: hoy los equipos tecnológicos son el principal objetivo.
- Computadores, portátiles y componentes desaparecen con frecuencia alarmante.
- En más de la mitad de los casos, hay participación interna.
- Las pérdidas superan 10 veces el valor del equipo, considerando información y productividad.
- El Oficial de Protección debe reconocer estas amenazas y aplicar controles físicos y de acceso adecuados.

Dimensión Económica del Problema

Las pérdidas por robo de tecnología superan cifras alarmantes:

- $200 mil millones USD (EE.UU., año 2000).
- $40 millones USD solo en microprocesadores.
- Los chips son tan pequeños que $1 millón en componentes cabe en una bolsa.
- Muchos terminan en otros países o mercados grises tras el robo inicial..

Robo de Componentes: Una Amenaza Invisible

“Más allá del hardware: el crimen dentro de los equipos”

No solo los equipos completos son robados — los componentes individuales también son un blanco valioso.

- RAM, microprocesadores, discos duros y tarjetas son los más codiciados.

- Los robos ocurren en escuelas, oficinas, industrias y bibliotecas.

Un mercado negro global compra y revende estos componentes en cuestión de días.

Modalidades de Robo

- Hurto interno: extracción de piezas por personal o contratistas.
- Robo armado: sustracción de equipos completos bajo amenaza.
- Sabotaje o espionaje: copia o retiro de memorias con datos críticos.
- Recolección no autorizada: manipulación o acceso sin supervisión.

Cada modalidad afecta no solo el inventario, sino la integridad operativa.

Impacto y Contramedidas

Impacto de una pérdida tecnológica:

- Costo de reemplazo.
- Pérdida de datos.
- Interrupción de la operación.
- Pérdida de confianza institucional.

Medidas de protección:

- Áreas restringidas y selladas.
- Inventarios y auditorías físicas regulares.
- Trazabilidad de componentes (seriales legibles, códigos QR).
- Políticas de salida y transporte controladas.

Medidas de Protección: Endurecimiento del Blanco

“Endurecer el blanco: disuadir, retrasar y detectar”

El endurecimiento del blanco consiste en crear barreras físicas y disuasivas que dificulten el robo o sabotaje.

Objetivo:

1. Hacer desistir al delincuente.
2. Aumentar el tiempo de respuesta.
3. Permitir la intervención del personal de seguridad o emergencias.

Puntos críticos: entradas, salidas y áreas de servicio.

Protección del Perímetro

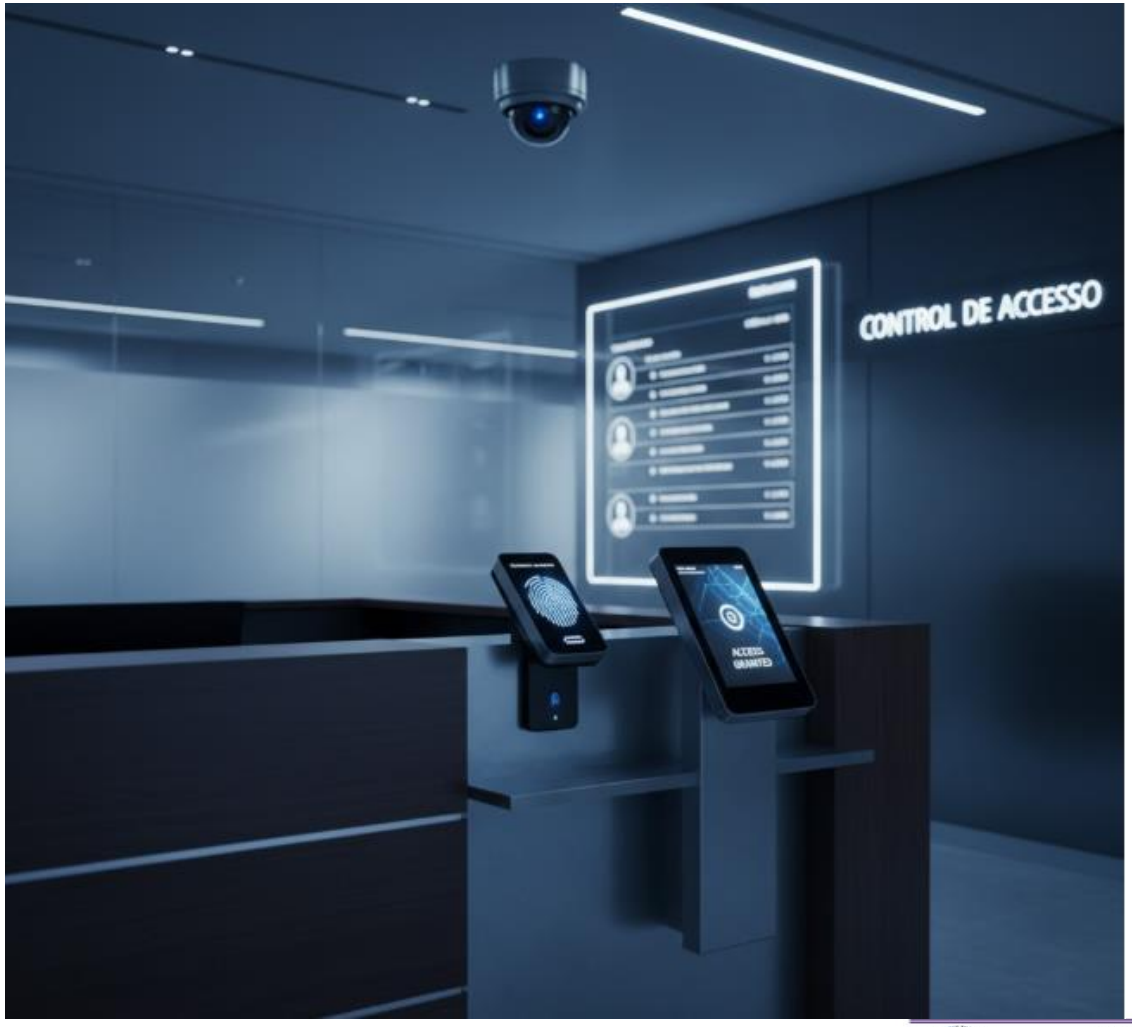
Recomendaciones clave:

- Mantener puertas y ventanas cerradas con llave y herrajes robustos.
- Controlar entradas y zonas de entrega.
- Implementar sistemas de control de acceso (manuales o electrónicos).
- Verificar daños y roturas.
- Monitorear con CCTV y patrullas 24/7.
- Mejorar iluminación perimetral: sin sombras, sin puntos ciegos.

Protección Interna del Establecimiento

Una vez asegurado el perímetro, se debe controlar el flujo interno:

- Punto único de acceso para empleados y visitantes.
- Registro, identificación y escolta a visitantes.
- Controles de acceso mecánicos, electrónicos o biométricos.
- Entrega de llaves solo a personal autorizado.
- Inventario y marcaje permanente de equipos tecnológicos.
- Comunicación con policía sobre equipos marcados o registrados.
- Custodia y resguardo fuera de la vista de laptops y dispositivos.

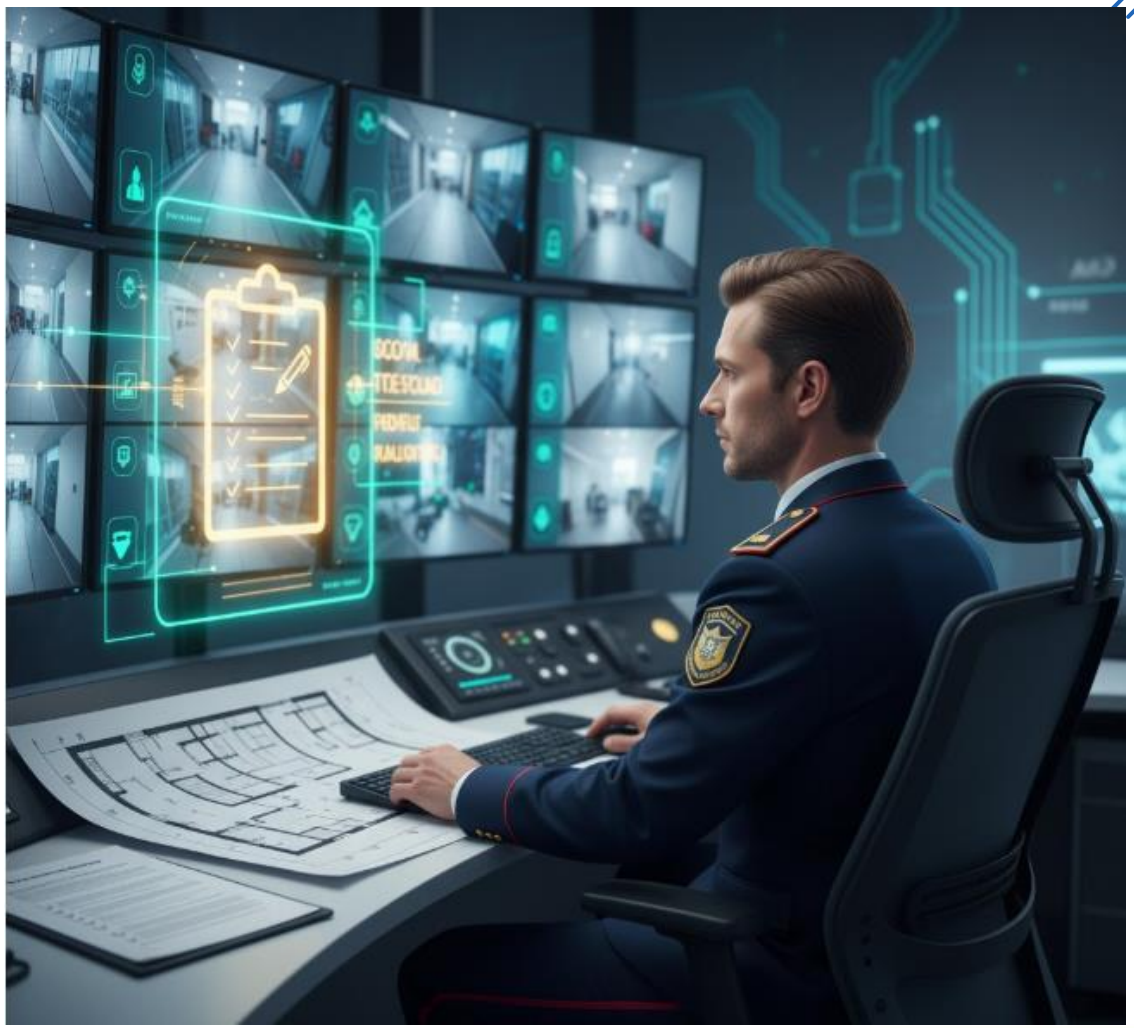


El Papel del Oficial de Protección

El Oficial debe:

- Evaluar vulnerabilidades físicas y procedimentales.
- Emitir observaciones y recomendaciones al cliente.
- Supervisar patrullas, controles y puntos críticos.
- Asegurar la aplicación de medidas dentro del marco legal.
- Capacitar al personal y reforzar la cultura de vigilancia.

Un entorno protegido no depende de muros, sino de personas atentas y procedimientos consistentes.



Dispositivos de Protección Especializada

“Tecnología al servicio de la seguridad tecnológica”

- Existen múltiples dispositivos diseñados para prevenir uso no autorizado, daño o robo de equipos.
- Complementan los controles físicos y humanos.
- Incluyen: Alarmas, Software de rastreo, Sellos de protección, Fijaciones y cerraduras, Cables de seguridad

Alarmas y Software de Rastreo

Alarmas: Internas o externas al CPU.

- Actúan como disuasivo sonoro, no como barrera física.
- Alertan al personal cercano.

Software de rastreo:

- Reporta ubicación al conectarse a Internet.
- Útil para equipos portátiles.
- Debe evaluarse su costo-beneficio frente a soluciones físicas.

Sellos y Etiquetas de Protección

Sellos, etiquetas plastificadas y luces UV permiten detectar manipulación o apertura no autorizada.

Sirven como indicadores visuales de integridad.

Sin embargo:

- Su eficacia depende del control visual frecuente.
- No evitan el robo, solo evidencian intervención.

Fijaciones y Cables de Seguridad

Fijaciones metálicas:

- Estructuras que encierran CPU, monitores y periféricos.
- Tornillos y adhesivos especiales.
- Dificultan la extracción o traslado.

Cables de acero:

- Económicos y versátiles.
- Retardan el robo, aunque pueden cortarse con tiempo.
- Tapas con llave protegen los puertos o componentes.

Procedimientos de Control y Revisión

Controles administrativos:

- ❑ “Levantamiento de propiedad” para retirar equipos: solo con orden gerencial.
- ❑ Requisas de salida: revisión de personas, vehículos y paquetes.
- ❑ Uso de detectores de metal (arco o manual).
- ❑ Aplicación consistente y legalmente respaldada.

Personal y cultura:

- ❑ Empleados temporales = riesgo elevado.
- ❑ Supervisión legítima y formación continua son esenciales.
- ❑ Controles internos no deben relajarse jamás.

Registro e Inventario de Equipos

Más allá del hardware, debe existir un registro actualizado de bienes tecnológicos.

Incluye:

- Números de serie y de parte.
- Descripciones detalladas.
- Historial de mantenimiento o ubicación.

Conocer qué se posee es la única forma de saber qué se ha perdido.

Tecnología: Definiciones Básicas

“Hablando el idioma de la tecnología”

Un Oficial de Protección debe conocer los términos tecnológicos básicos para entender y comunicarse con el personal de TI.

- Estos conceptos permiten reconocer vulnerabilidades, entender reportes y coordinar acciones de seguridad.

Toda organización, sin importar su tamaño, depende hoy de recursos tecnológicos.

Hardware y Software

Hardware:
Componentes físicos — CPU, teclado, impresora, chips, servidores.

Software:
Programas o instrucciones que permiten que el hardware funcione.

Licencia:
Contrato legal que autoriza el uso del software bajo condiciones específicas.

Piratería:
Uso ilegal o copia no autorizada de software.

Redes, Servidores y Datos

Red:
Conjunto de computadoras que comparten recursos e información.

Servidor:
Equipo central que distribuye programas, datos e impresoras.

Ethernet:
Estándar que define cómo las computadoras se comunican en red.

Correo Electrónico:
Servicio de comunicación y transferencia de datos.

Cliente de correo:
Software que permite enviar o recibir mensajes (Outlook, Thunderbird).

Componentes Clave y Seguridad Operativa

Backup:
Copia de seguridad de datos críticos.

UPS:
Fuente de poder ininterrumpida — protege contra cortes eléctricos.

Microprocesador:
“Cerebro” del computador (CPU).

RAM:
Memoria de acceso rápido para programas en uso.

Tarjeta Madre:
Placa principal que conecta todos los componentes.

- **Interface:**
  Medio que permite la interacción entre usuario y sistema.
- **Recuperación de información:**
  restaurar datos dañados o perdidos.

PREGUNTAS DE AUTOEVALUACIÓN

Introducción a la Protección Informática

CPO©

Introducción a la Protección Informática

“Del resguardo físico al ciberespacio: el nuevo desafío del Oficial de Protección”

Las computadoras y redes nacieron para compartir información, no para protegerla.

Hoy, el Oficial de Protección enfrenta un entorno tecnológico donde:

- ❑ Los sistemas son interconectados y accesibles desde cualquier lugar.
- ❑ Las amenazas digitales crecen tan rápido como la innovación.
- ❑ La confidencialidad, integridad y disponibilidad son los pilares de la seguridad moderna.

Su rol evoluciona: asesorar, prevenir y proteger frente a los riesgos informáticos.

El Problema Creciente

“La expansión del riesgo digital: una realidad global”

En 2002, el Computer Security Institute y el FBI publicaron un estudio pionero:

- 90% de las organizaciones detectaron fallas de seguridad en 12 meses.
- 80% sufrió pérdidas económicas por esas fallas.
- $455 millones USD en pérdidas reportadas.

La seguridad informática dejó de ser un tema técnico para convertirse en un problema financiero y estratégico.

Principales Modalidades de Pérdidas

Principales causas de pérdida financiera:

- Robo de información: $170 millones.
- Fraude financiero: $115 millones.
- Conexión a Internet = punto de ataque más frecuente.
- Solo 33% reportó que los ataques vinieron desde redes internas.

Comportamiento Organizacional y Respuesta

- Solo 34% de las organizaciones denunció los delitos.
- 40% detectó intrusiones externas.
- 40% negó haber sido afectado.
- 78% detectó abuso de Internet por empleados.
- 85% sufrió ataques de virus.
- La negación y el silencio también son vulnerabilidades.

Impacto del Internet y el Comercio Electrónico

Internet amplificó la exposición:

- 98% de las organizaciones tenía sitio web.
- 52% hacía comercio electrónico.
- 38% sufrió accesos no autorizados.
- 70% vandalismo.
- 55% ataques de denegación de servicio.
- 20% robo de información.
- 6% fraude financiero.

El crimen digital evolucionó junto al crecimiento de la red.

¿Que es la Protección Informática?

“La información: motor y vulnerabilidad de la sociedad moderna”

Vivimos en la sociedad de la información, donde:

- El volumen de datos procesados y transmitidos es mayor que en toda la historia.
- La información se considera un activo estratégico y prioritario para las organizaciones.
- Su pérdida o alteración puede impactar directamente en la economía y estabilidad social.

La información no solo genera valor: también debe ser protegida.

El Desafío de las Tecnologías y las Redes

La informática y las redes son el núcleo del progreso actual… y del riesgo.

La conexión a Internet multiplicó las oportunidades y los ataques:

- Un equipo conectado puede ser objetivo desde cualquier parte del mundo.
- Los ataques ya no dependen de proximidad física, sino de vulnerabilidades digitales.

La interconexión global hace que la protección informática sea esencial para la continuidad operativa.

Concepto de Protección Informática

Protección de los Sistemas de Información (PSI):
Conjunto de medidas que garantizan:

- ❖ Confidencialidad — la información solo accesible a quien corresponde.
- ❖ Integridad — los datos permanecen completos y sin alteraciones.
- ❖ Disponibilidad — los sistemas y la información están operativos cuando se necesitan.

También llamada:

- ✓ Seguridad de la información
- ✓ Seguridad de datos
- ✓ Protección informática

¿Qué es Información?

“La información: la materia prima de la decisión”

Información: conjunto de datos que permiten tomar decisiones.

Es esencial para:

- La planificación estratégica.
- El control operativo y la corrección de desvíos.
- La evaluación del desempeño.

Tipos de sistemas de información:

- Subsistema formalizado: normas, reportes, procedimientos oficiales.
- Subsistema no formalizado: conversaciones, rumores, llamadas o mensajes informales.

¿Qué es un Sistema Informático?

Sistema Informático: conjunto de recursos técnicos, humanos y financieros destinados a almacenar, procesar y transmitir información.

- Subconjunto del sistema formalizado.

- Permite que la información circule con rapidez, precisión y trazabilidad.

Componentes:

- ❑ Técnicos: hardware, redes, software.
- ❑ Humanos: personal informático y usuarios.
- ❑ Financieros: inversión, mantenimiento, soporte.

Aspectos Clave en la PSI

“El equilibrio esencial: información, tecnología y protección”

La difusión de las tecnologías de la información expone a las organizaciones a riesgos crecientes:

- ❑ Falta de controles básicos en equipos personales.
- ❑ Conectividad global y acceso múltiple.
- ❑ Los fallos en confidencialidad, integridad y disponibilidad (CID) son las principales causas de vulnerabilidad.

La Protección de los Sistemas de Información (PSI) busca garantizar estos tres pilares.

Confidencialidad

Confidencialidad: la información solo debe estar disponible para personas autorizadas.

También conocida como secreto o privacidad.

- En gobiernos → acceso según nivel de autoridad.
- En empresas → protección de información estratégica, nóminas, contratos, etc.

Mecanismos:

- Control de accesos.
- Cifrado de información y comunicaciones.

Integridad

Integridad: garantiza que la información no sea alterada, dañada o manipulada sin autorización.

Incluye conceptos de:

- Precisión: datos exactos.
- Autenticidad: origen verificado.

“Lo que se envía es lo que se recibe.”

Ejemplo: transacciones bancarias, registros contables, historiales médicos.

Disponibilidad

Disponibilidad: Grado en que los datos están accesibles para los usuarios autorizados cuando los necesitan.

Un sistema seguro debe:

- ❑ Mantener su funcionamiento continuo.
- ❑ Recuperarse rápidamente ante fallos.

Su opuesto: Denegación de Servicio (DoS) — usuarios no pueden acceder a los recursos.

Otros Aspectos Relacionados

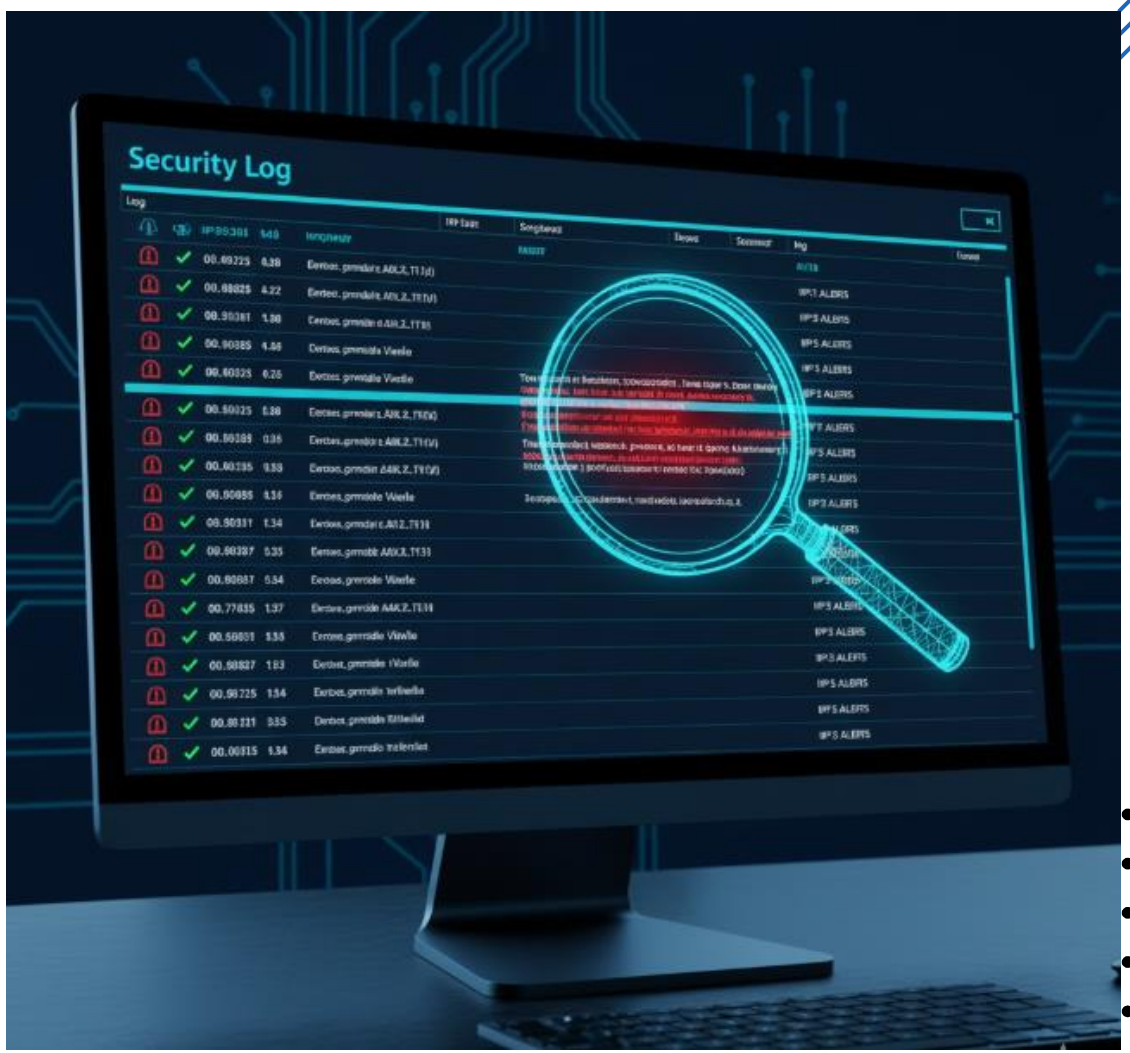
- Autenticidad: verificar el origen de la información.
- No repudio: garantizar que nadie pueda negar haber enviado o recibido algo.
- Consistencia: el sistema se comporta como se espera.
- Aislamiento: limita el acceso al sistema a usuarios autorizados.
- Auditoría: registrar actividades para detectar, prevenir y responder a incidentes.

Importancia de la Auditoría

Auditoría: permite saber qué ocurrió, quién lo hizo y cuándo.

Funciones:

- ❑ Prevención: el registro disuade.
- ❑ Mitigación: detecta anomalías.
- ❑ Monitoreo: verifica funcionamiento continuo.
- ❑ Respuesta: apoya la investigación forense y recuperación.



Un Sistema Seguro

Definición operacional: Un sistema informático es seguro cuando su hardware y software se comportan como se espera.

La seguridad no es un estado permanente, sino un proceso continuo de prevención, monitoreo y respuesta.

Política de Protección Informática

“De la intención al compromiso: la política de protección de sistemas”

La política de protección es una declaración formal de intenciones de la dirección:

- ❑ Define responsabilidades técnicas y organizativas.
- ❑ Establece normas, protocolos y controles.
- ❑ Asegura que la protección sea parte del negocio, no un añadido.

Debe ser aprobada y respaldada por la alta dirección, con participación de expertos TI.

Principios para establecer una Política

Principios clave de una política de protección SI:

- Holística: cubre lo físico, humano, lógico y logístico.
- Adecuada: proporcional al valor de la información y los recursos disponibles.
- Basada en gestión de riesgos: identifica activos, amenazas y medidas.
- Revisable: debe monitorearse y actualizarse regularmente.

Políticas de Contraseñas

Las contraseñas son la primera línea de defensa, pero también el punto más débil.

Recomendaciones esenciales:

- ❑ Cambiar contraseñas al enrolarse y periódicamente.
- ❑ Mantenerlas en secreto absoluto.
- ❑ No compartirlas, ni siquiera con administradores.
- ❑ Usar autenticación de hora o doble factor.
- ❑ Registrar y firmar compromiso de uso responsable.

Políticas de Correo Electrónico e Internet

Correo electrónico:

- Solo para fines oficiales.
- Prohibido uso personal o envío no autorizado
- Mensajes confidenciales = cifrado y control de acceso.

Internet:

- Riesgo de entrada a la red corporativa.
- Uso controlado mediante firewalls, filtros y políticas de acceso.
- Debe existir trazabilidad de navegación.

Políticas de Respaldo y Recuperación

Los respaldos garantizan la continuidad operativa ante fallas o desastres.
Razones: fallas de disco, errores humanos, vandalismo o desastres naturales.

Buenas prácticas:

- Programar respaldos regulares (nocturnos o automáticos).
- Usar respaldos incrementales y diferenciales.
- Proteger los medios en caja fuerte o depósito externo.
- Documentar qué, cómo y cuándo se respalda.

Monitoreo y Revisión de Políticas

Una política efectiva no termina con su creación:

- ❑ Debe monitorearse su cumplimiento.
- ❑ Auditarse periódicamente.
- ❑ Revisarse y actualizarse cuando surjan cambios tecnológicos o incidentes.

La mejora continua es la esencia de la seguridad.

Análisis de Costo - Beneficio

“Proteger con inteligencia: el equilibrio entre costo y valor”

Toda medida de protección debe ser proporcional al valor del activo y al costo de la amenaza.

Relación ideal: Ca > Cr > Cs
Donde:

- Ca: Costo de atacar el sistema
- Cr: Valor del sistema / información
- Cs: Costo de protegerlo

Principio clave: Debe costar más atacar que proteger, y nunca debe costar más proteger que el valor del activo.

Vulnerabilidades, Amenazas y Contramedidas

“Vulnerabilidades, amenazas y contramedidas: el triángulo de la protección informática”

Vulnerabilidad: debilidad o punto susceptible de ataque.

Amenaza: agente o evento que aprovecha la vulnerabilidad.

Contramedida: acción o técnica que reduce o elimina la amenaza.

“No existen sistemas completamente seguros; solo sistemas mejor protegidos.”

Tipos de Vulnerabilidad

Principales vulnerabilidades en sistemas informáticos:

- Físicas → acceso no autorizado o daños estructurales.
- Naturales → fuego, agua, fallas eléctricas, clima.
- Hardware / Software → fallos técnicos o bugs.
- Comunicaciones → intercepción de red, sniffing, intrusiones.
- Humanas → errores, negligencia o abuso de confianza (la más común).

Vulnerabilidad Humana

El factor humano: el eslabón más débil.

- Administradores con acceso total.
- Usuarios con malas prácticas.
- Empleados descontentos o descuidados.

+50% de los incidentes de protección tienen origen interno.

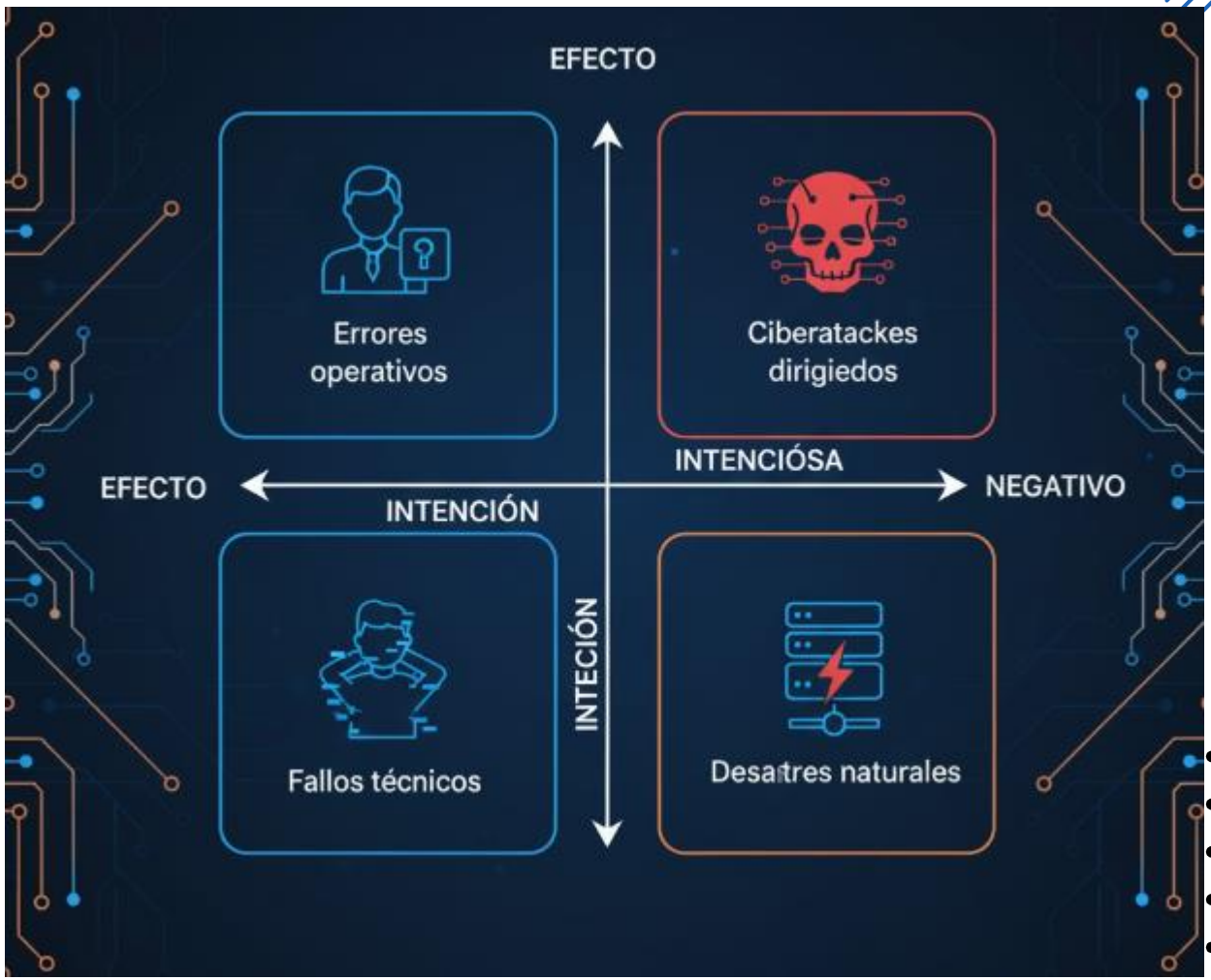
Tipos de Amenazas

Según su efecto en el sistema:

- ❑ Intercepción: acceso no autorizado (espionaje, sniffing).
- ❑ Modificación: alteración de datos o programas.
- ❑ Interrupción: bloqueo o destrucción (DoS, fallos).
- ❑ Generación: inserción de código o datos falsos (virus, spam).

Según su origen:

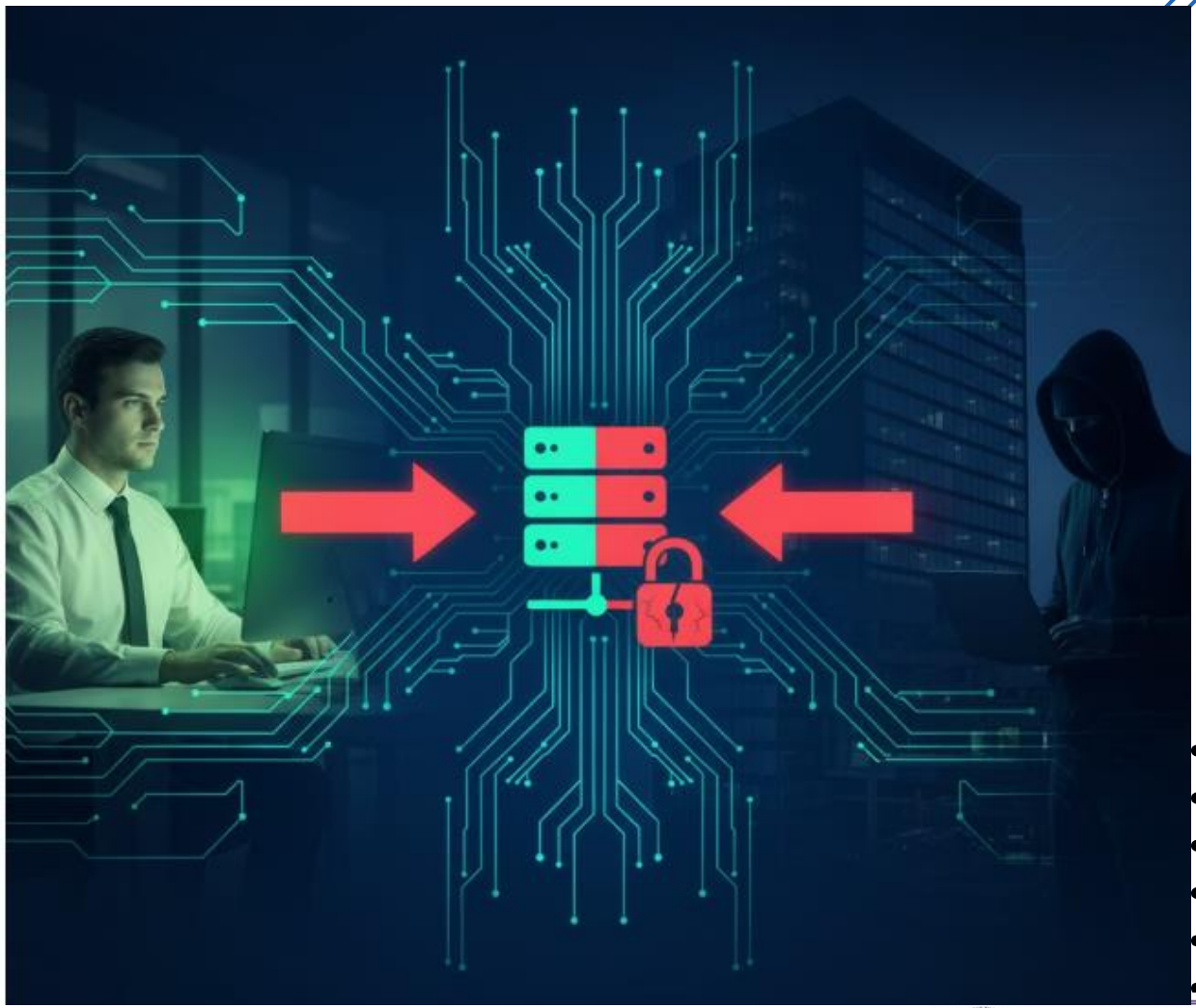
- ❑ Naturales
- ❑ Involuntarias
- ❑ Intencionadas
- ❑ (internas o externas)



Amenazas Internas y Externas

- Internas: empleados, contratistas o socios con acceso autorizado.
- Externas: hackers, competidores, delincuentes, eventos naturales.

Los ataques más dañinos suelen combinar ambos mundos (ingeniería social + acceso técnico).



Anatomía de un Ataque de Ransomware

https://www.youtube.com/watch?v=3r7qwIRwrOU

Contramedidas: el arte de Defender

Contramedidas: acciones técnicas, físicas, administrativas o legales que reducen riesgos.

Tipos principales:

1. Físicas — control de acceso, vigilancia, UPS, extintores.
2. Lógicas — contraseñas, criptografía, firewall, auditoría.
3. Administrativas — formación, roles, políticas, conciencia.
4. Legales — leyes y sanciones disuasivas.

Contramedidas Físicas y Lógicas

- Físicas: control de acceso, CCTV, sensores, extintores, energía ininterrumpida.

- Lógicas: autenticación, permisos, cifrado, políticas de software, monitoreo y auditoría.

La seguridad digital empieza en la puerta… y termina en el código.

Contramedidas Administrativas y Legales

Administrativas:

- Capacitación y concientización.
- Roles y responsabilidades definidos.
- Procedimientos documentados.

Legales:

- Cumplimiento normativo.
- Políticas de privacidad y datos personales.
- Sanciones y denuncias frente a ataques.

Planes de Contingencia

Ningún sistema es infalible; la clave es saber recuperarse.

Un plan de contingencia debe definir:

- Qué respaldos se realizan y dónde se guardan.
- Tiempo máximo aceptable de recuperación.

Medios alternativos:

- Instalación fría: espacio listo en días.
- Instalación caliente: operación completa en horas.

Prepararse “para cuando falle”, no “por si falla”.

Principios Fundamentales de la Protección Informática

“La seguridad no solo se implementa… se piensa”

En la protección informática existen principios universales que orientan toda política o diseño de seguridad:

1. Menor privilegio
2. Transparencia (no por oscuridad)
3. Eslabón más débil
4. Defensa en profundidad
5. Control centralizado
6. Falla segura
7. Participación universal
8. Simplicidad

Principio de Menor Privilegio

Dar solo los accesos necesarios, nada más.

Cada usuario, programa o proceso debe tener los privilegios mínimos para cumplir su tarea y solo durante el tiempo necesario

- Limita el impacto de errores y abusos.

- Reduce la superficie de ataque.

La Protección no se obtiene a través de la oscuridad

La seguridad no se basa en ocultar vulnerabilidades, sino en conocerlas y corregirlas.

“Seguridad por oscuridad” = falsa confianza.

“Seguridad por diseño” = conocimiento, educación y mejora continua.

Principio del Eslabón más Débil

Una cadena es tan fuerte como su eslabón más débil.

Un sistema es tan seguro como su componente más vulnerable.

Evaluar todo el entorno, no solo los puntos “visibles” de protección.

Defensa en Profundidad y Punto de Control Centralizado

Defensa en profundidad: múltiples capas de protección → si una falla, otra actúa.

Control centralizado: un único punto de acceso y monitoreo para todo el sistema.

“Más barreras, menos brechas.”

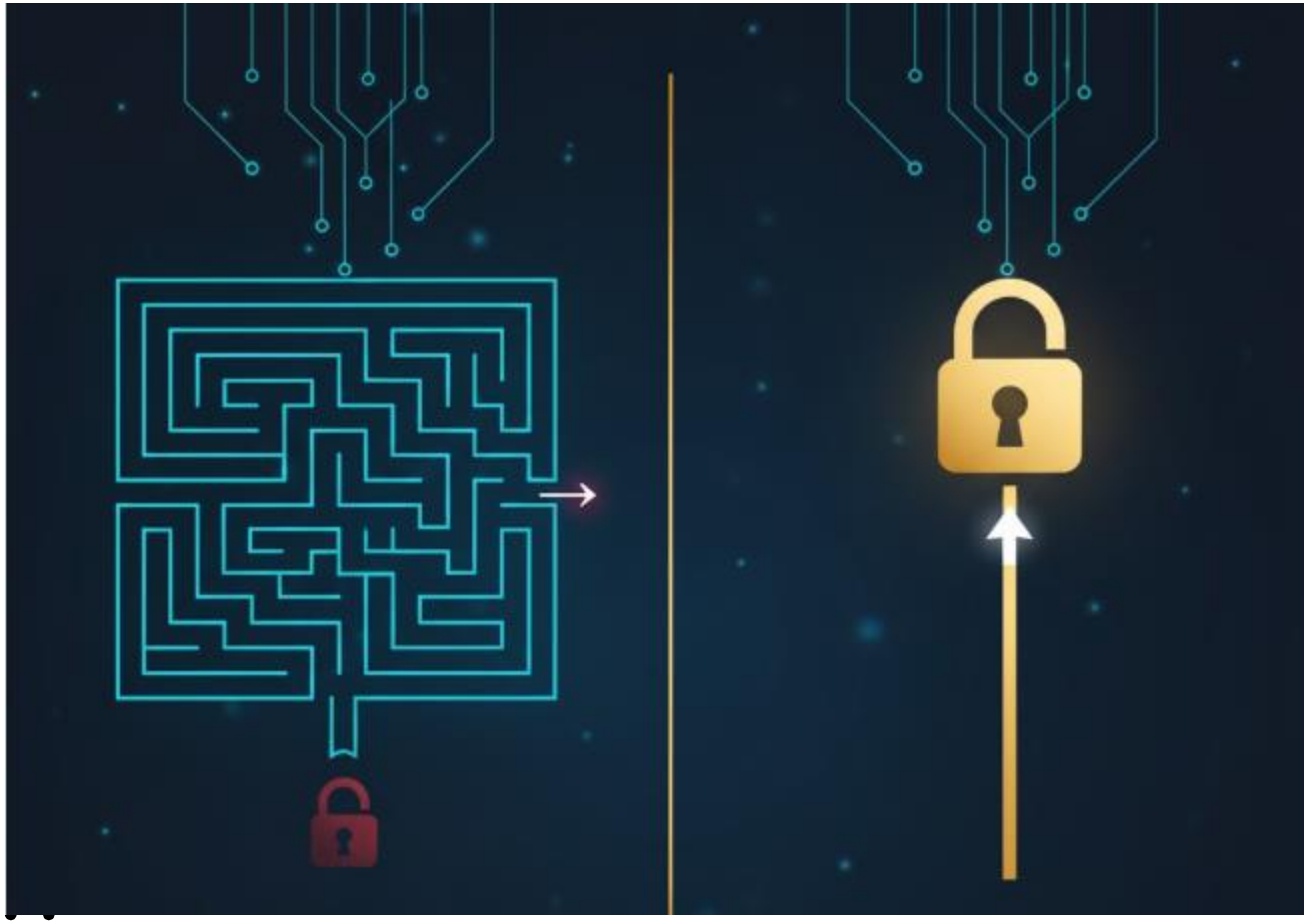
Protección en caso de Fallo y Participación Universal

Falla segura: si algo falla, el sistema debe quedar bloqueado, no abierto.

Participación universal: todos los usuarios deben apoyar y cumplir las medidas de seguridad.

“Un sistema seguro no depende solo de tecnología, sino de cultura.”

Principio de Simplicidad



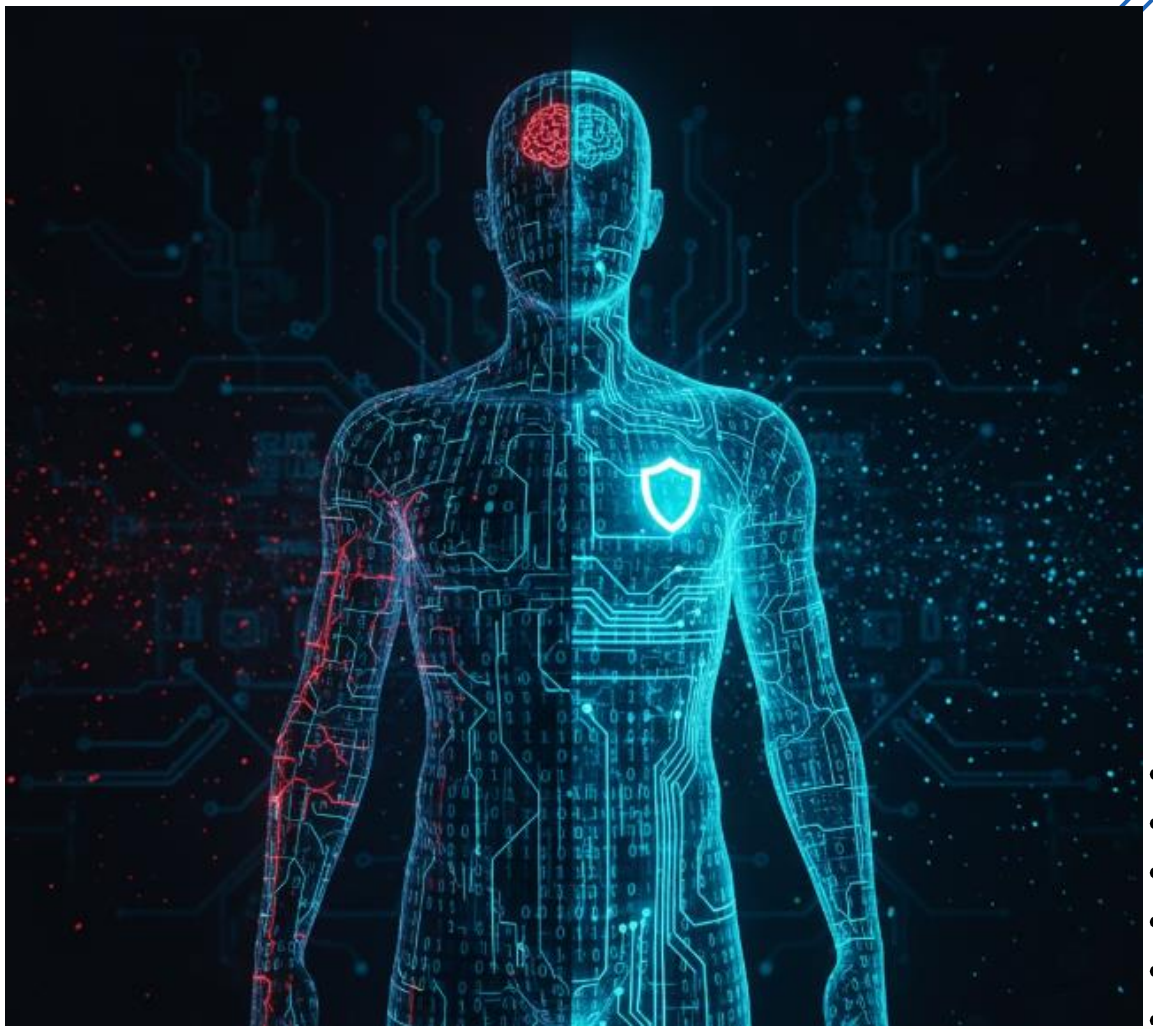
“Lo simple es más seguro.”

- Sistemas claros = más comprensibles.
- Menos complejidad = menos errores.
- La simplicidad reduce el riesgo de fallas ocultas.

Amenazas Humanas: el factor más impredescible

- El 70% de los incidentes de seguridad involucran error o acción humana.
- Los atacantes internos son los más peligrosos: conocen procesos, sistemas y puntos débiles.
- Las amenazas pueden ser maliciosas (intencionales) o no maliciosas (por desconocimiento).

“La mayor vulnerabilidad no está en la red, sino detrás del teclado.”



Tipos de Amenazas Humanas

Internas: empleados, contratistas, socios, exempleados.

Externas: ciberdelincuentes, competidores, hacktivistas.

Dos tipos de riesgos:

- Maliciosos: sabotaje, espionaje, venganza, robo.
- No maliciosos: errores, descuidos, falta de capacitación.

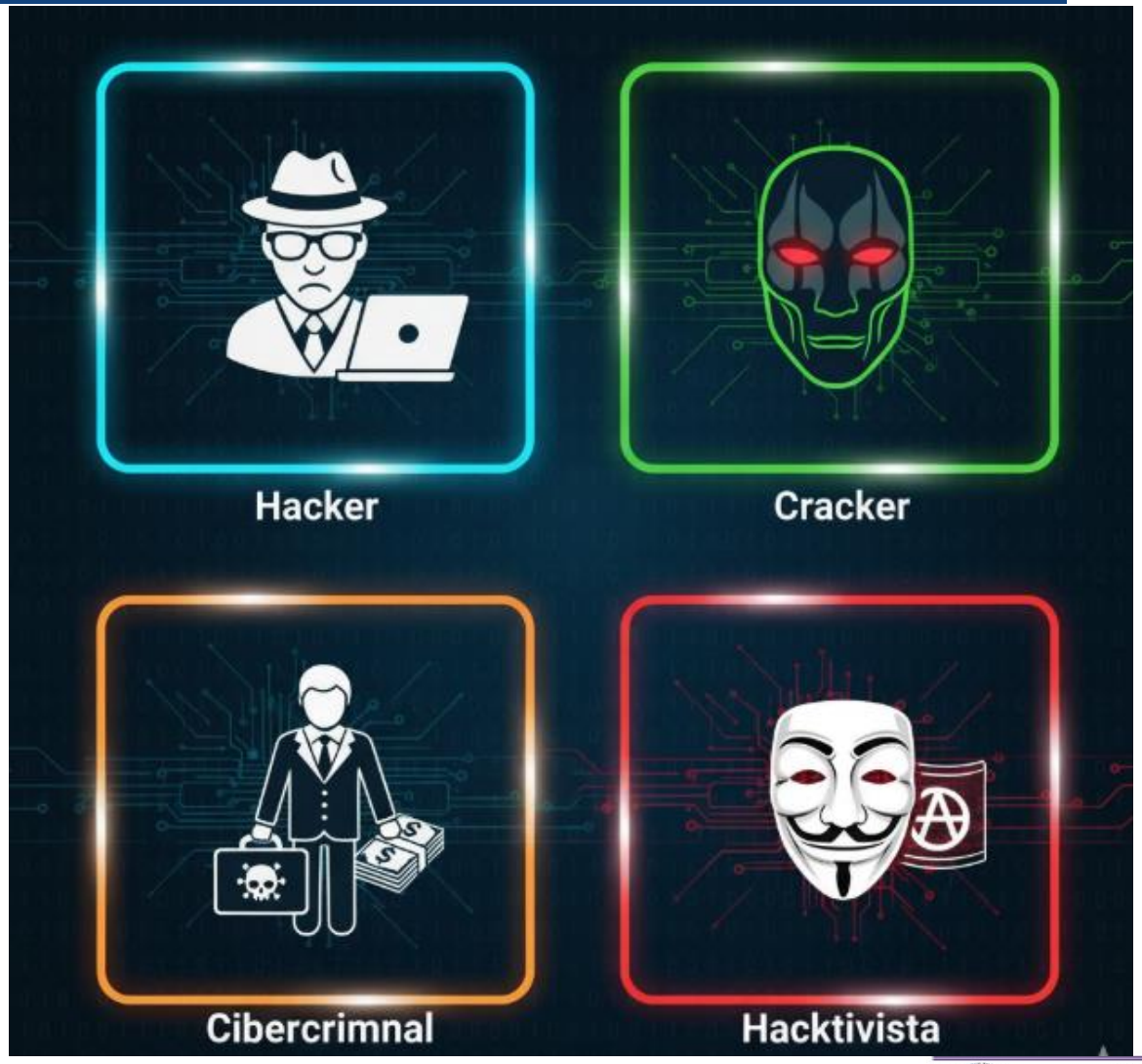
Hackers, Crackers y Cibercriminales

Hackers (White Hats): exploran y aprenden, prueban límites éticamente.

Crackers (Black Hats): rompen sistemas con fines destructivos o ilegales.

Cibercriminales: aprovechan vulnerabilidades para obtener beneficios o causar daño.

Hacktivistas: atacan por causas políticas o sociales.



Motivaciones detrás de los Ataques

¿Por qué atacan?

- Robo o fraude de información.
- Paralizar operaciones.
- Espionaje o competencia desleal.
- Venganza o desafío tecnológico.
- Causas ideológicas (hacktivismo).

Principales Métodos de Ataque

Los más comunes:

- ❑ Virus y malware
- ❑ Caballos de Troya
- ❑ Phishing y sitios falsos
- ❑ Robo o descifrado de contraseñas
- ❑ Ataques de denegación de servicio (DoS)
- ❑ Spoofing y manipulación de red
- ❑ Ingeniería social

El Poder de la Ingeniería Social

Ingeniería social: manipular a las personas para obtener información o acceso.

“No se hackean sistemas… se hackean emociones.”

Ejemplos:

- Llamadas fingiendo soporte técnico.
- Correos de urgencia o autoridad.
- QR o enlaces fraudulentos.
- Suplantación de identidad.

Ejemplo de Fraude Telefónico

https://www.youtube.com/watch?v=dp6bF3DPvN4&t=143s

Ataques al Correo y Red

Amenazas frecuentes:

- ❑ SPAM y phishing.
- ❑ Espionaje o manipulación de correos.
- ❑ Suplantación de sitios (web spoofing).
- ❑ Intrusiones por red (network spoofing).

Contramedidas:

- ❖ Filtrado de correo.
- ❖ Verificación de dominio.
- ❖ Cifrado de mensajes.
- ❖ Educación constante.

Conclusión: El Factor Humano como Centro

Tecnología + Procesos + Personas = Seguridad

Sin conciencia humana, ningún sistema es seguro.

“Educar no es un gasto, es la mejor contramedida.”

Terminología Clave en Protección Informática

“El lenguaje del Oficial de Protección Digital”

Comprender la terminología técnica es esencial para:

- ❑ Comunicar eficazmente con personal IT y directivos.
- ❑ Interpretar informes técnicos, vulnerabilidades y auditorías.
- ❑ Participar en incidentes o decisiones de ciberseguridad.

Un Oficial preparado domina tanto el lenguaje operativo como el estratégico.

Vocabulario de Defensa y Acceso

“Barreras, autenticación y control”

Firewall: barrera entre redes para limitar accesos.

Biometría: identificación por rasgos físicos (huella, iris, rostro).

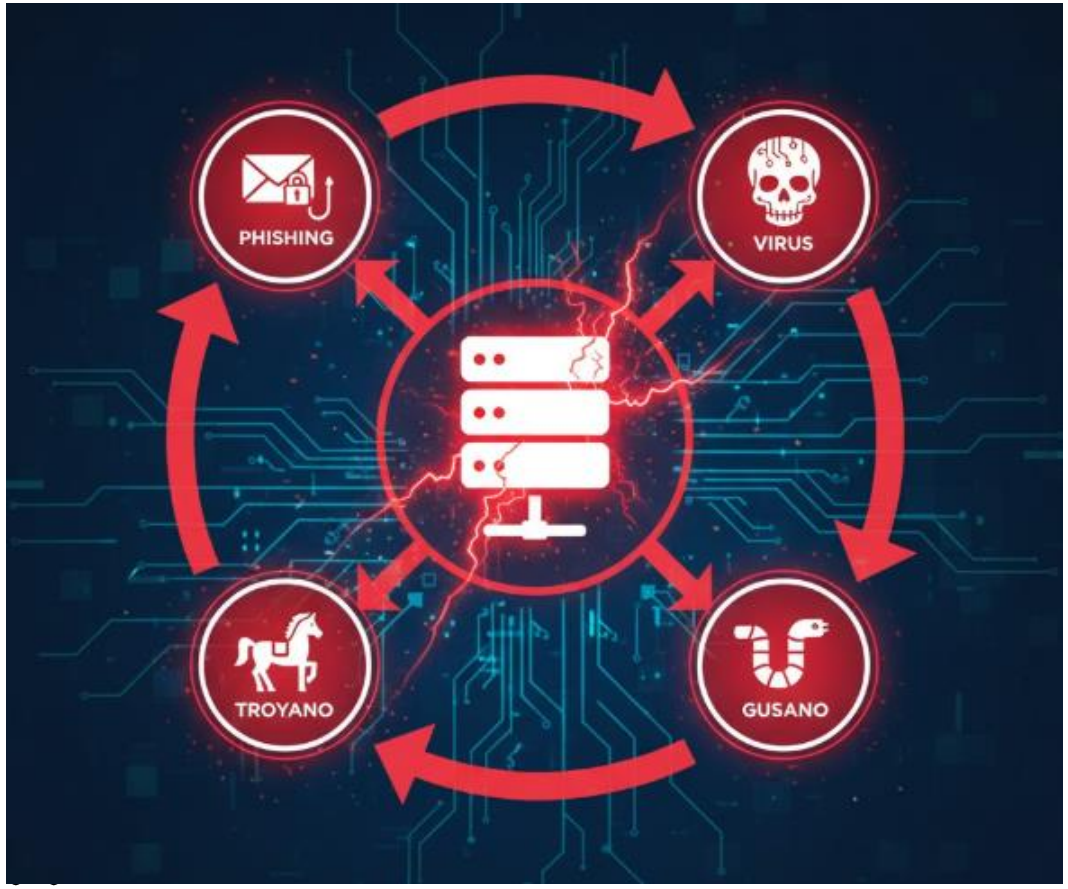
Contramedidas: acciones o dispositivos que reducen vulnerabilidades.

Backdoor: acceso oculto dejado intencionalmente en software o sistemas.

IDS / Detección de intrusión: monitoreo de actividad anómala en red.

CERT: equipos expertos que responden ante incidentes informáticos.

Vocabulario de Amenazas y Ataques



“El arsenal del adversario”

Virus: código que se replica automáticamente.

Gusano: programa autorreplicante que ocupa memoria o red.

Caballo de Troya: software disfrazado con fines maliciosos.

Phreaker: intruso en sistemas telefónicos.

Phishing: suplantación digital para engañar y robar datos.

Denial of Service (DoS): saturar un sistema hasta inutilizarlo.

Vocabulario de Gestión y Gobernanza

“Del incidente a la política: la mirada integral”

Protección de información: conjunto de políticas y procedimientos para resguardar datos.

Intranet: red interna de uso exclusivo de la organización.

Crimen cibernético: actos ilegales cometidos mediante sistemas informáticos.

Encriptación: proceso que convierte la información en código seguro.

Software / Hardware: capas lógicas y físicas que deben protegerse coordinadamente.

PREGUNTAS DE AUTOEVALUACIÓN