FACULTAD DE INGENIERÍA

Universidad Nacional de Jujuy

Unidad 1

Introducción a la Seguridad Informática

Seguridad y Auditoría Informática

Contenidos de la Unidad 1

1.1 Introducción

La información como activo estratégico

Características únicas

Se copia en segundos, se transmite globalmente, se modifica de forma imperceptible y se destruye sin dejar evidencia física.

Superficie de exposición

Internet, nube, móviles, IoT, IA y trabajo remoto ampliaron las posibilidades de acceso a la información y generaron nuevos riesgos.

Más que un producto

La seguridad informática es un proceso continuo que involucra personas, procesos, tecnologías y políticas.

Riesgo residual

La seguridad absoluta no existe. El objetivo es administrar los riesgos hasta un nivel aceptable.

1.2 Evolución Histórica de la Seguridad Informática

La seguridad ha evolucionado en paralelo con las tecnologías de la información.

1950-60

Mainframes

Protección física del hardware

1970

Multiusuario

Primeros controles de acceso

1980

PCs + Malware

Virus Brain y antivirus

1990

Internet

Firewalls, VPN, gusanos

2000+

Ciberseguridad

Amenazas globales y estatales

1.2.1 – 1.2.2 Décadas 1950 a 1970

1950 – 1960 · Mainframes

Computadoras de gran tamaño en organismos gubernamentales, universidades y grandes empresas.

Seguridad enfocada casi exclusivamente en:
- Protección del hardware
- Restricción del acceso físico

Amenazas: errores operativos y fallas de equipamiento más que ataques deliberados.

1970 · Control de acceso

Sistemas multiusuario → necesidad de identificar y autenticar usuarios.

Aparecen:
- Primeras contraseñas
- Modelos básicos de control de acceso

Se sientan las bases de la seguridad lógica moderna.

1.2.3 – 1.2.4 Décadas 1980 y 1990

1980 · Nacimiento del malware

Expansión de las computadoras personales.

Virus Brain (1986)
Primer virus para PCs basado en MS-DOS.
Infectaba el sector de arranque de los disquetes.

Aparecen los primeros programas antivirus comerciales.

1990 · Expansión de Internet

Los sistemas dejan de estar aislados → exposición permanente a ataques externos.

Nuevas amenazas:
- Gusanos · DoS · Robo de contraseñas
- Intrusiones remotas · Ingeniería social

Tecnologías: Firewalls y VPN.

1.2.5 Siglo XXI: Ciberseguridad Global

La seguridad pasa de ser un tema técnico a un componente esencial de la gestión organizacional y el gobierno corporativo.

Ransomware

Secuestro de datos a cambio de rescate

Ataques estatales

Ciberespionaje y operaciones patrocinadas

Infraestructuras críticas

Energía, salud, transporte, agua

Robo masivo de datos

Filtraciones a gran escala

Servicios en la nube

Nuevos vectores de ataque

IA ofensiva

Amenazas dirigidas con inteligencia artificial

1.3 Concepto de Seguridad Informática

Definición conceptual

La disciplina que estudia, diseña e implementa mecanismos destinados a proteger los sistemas informáticos, los recursos tecnológicos y la información contra accesos no autorizados, modificaciones indebidas, pérdidas, interrupciones del servicio y cualquier otro evento que comprometa la continuidad o el correcto funcionamiento de dichos sistemas.

Definición según el NIST

La protección de los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

1.3.3 ¿Qué protege la Seguridad Informática?

Información	Historias clínicas, datos bancarios, patentes, planos, bases de datos, expedientes…
Hardware	Servidores, PCs, routers, switches, discos, dispositivos móviles…
Software	Sistemas operativos, aplicaciones, bases de datos, software industrial…
Servicios	Correo, sitios web, facturación, plataformas educativas, nube, banca…
Personas	Administran, desarrollan, gestionan información sensible y toman decisiones.

1.3.4 ¿Por qué es necesaria la Seguridad Informática?

01

Crecimiento de la información digital

Transacciones, expedientes, historias clínicas, imágenes médicas, correos…

02

Aumento de los ataques

Millones de ataques diarios. Herramientas cada vez más sofisticadas.

03

Dependencia tecnológica

Hospitales, bancos, aeropuertos, industrias… la indisponibilidad puede costar vidas.

04

Obligaciones legales

Protección de datos personales, firma digital, delitos informáticos.

05

Protección de la reputación

El daño reputacional suele superar las pérdidas económicas directas.

1.3.5 Seguridad como proceso y no como producto

Error frecuente: “Ya tenemos antivirus / compramos un firewall / instalamos monitoreo” → esas herramientas solas NO garantizan la seguridad.

La seguridad depende de:

- Políticas organizacionales
- Procedimientos
- Capacitación
- Controles técnicos
- Auditorías
- Gestión de riesgos
- Actualización permanente

1.3.6 Ejemplo práctico: Universidad

Una universidad almacena datos personales, calificaciones, títulos, información financiera e investigaciones.

Si un atacante accede al Sistema podría	Medidas necesarias para evitarlo
• Modificar notas • Eliminar registros • Robar datos personales • Cifrar todo con ransomware • Vender información en la dark web	• Políticas de seguridad • Control de acceso + MFA • Copias de seguridad • Capacitación a usuarios • Monitoreo y auditorías • Gestión de incidentes

1.4 Seguridad Informática, de la Información y Ciberseguridad

Aunque a menudo se usan como sinónimos, tienen alcances diferentes.

Seguridad de la Información

Protege la información independientemente del medio (papel, digital, verbal) en el que se encuentre almacenada, procesada o transmitida.
Norma ISO/IEC 27000. La preservación de la confidencialidad, la integridad y la disponibilidad de la información. Adicionalmente, pueden incluirse otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

Seguridad Informática

Es la disciplina encargada de proteger los sistemas informáticos y recursos tecnológicos que almacenan, procesan y transmiten la información. Protege computadoras, servidores, sistemas operativos, aplicaciones, bases de datos, redes de comunicación, dispositivos móviles, equipos de almacenamiento.

Ciberseguridad

Protege personas, organizaciones, los servicios y servicios que operan en el ciberespacio frente a amenazas digitales. A diferencia de la Seguridad Informática, la Ciberseguridad pone el foco en los riesgos derivados de la conectividad y de Internet. Protección frente a ransomware, defensa contra ataques distribuidos de denegación de servicio (DDoS), protección de infraestructuras críticas, seguridad en la nube, etc.

1.4.6 Comparación entre los conceptos

Aspecto	Seg. Información	Seg. Informática	Ciberseguridad
¿Qué protege?	La información	Los sistemas informáticos	El ciberespacio
Medio	Digital y no digital	Principalmente digital	Entornos conectados
Alcance	Más amplio	Tecnológico	Tecnológico y estratégico
Documentos en papel	Sí	No	Generalmente no
Redes e Internet	Puede incluirlas	Sí	Sí
Personas y procesos	Sí	Parcialmente	Sí

Ejemplo integrador: un hospital

Seguridad de la Información

Protege historias clínicas, resultados de laboratorio, estudios por imágenes… estén en base de datos, impresas o comunicadas verbalmente.

Seguridad Informática

Protege servidores, computadoras, bases de datos, aplicaciones médicas y dispositivos de almacenamiento.

Ciberseguridad

Protege frente a ransomware, ataques a la red, robo de credenciales, ataques a la nube y accesos remotos no autorizados.

1.5 Activo, Vulnerabilidad, Amenaza y Riesgo

Activo

Aquello que posee valor para la organización: bases de datos, servidores, documentos, sistemas, personal, infraestructura.

Vulnerabilidad

Debilidad que puede ser explotada: contraseña débil, software desactualizado, ausencia de backups, mala configuración.

Amenaza

Circunstancia, evento o actor con capacidad de explotar una vulnerabilidad: atacante, malware, incendio, error humano.

Riesgo

Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre un activo.

1.5 Ejemplo Activo, Vulnerabilidad y Amenaza

Activo

- bases de datos;
- servidores;
- documentos;
- sistemas;
- personal;
- infraestructura

Vulnerabilidad

- contraseña débil;
- software desactualizado;
- ausencia de copias de seguridad;
- mala configuración.

Amenaza

- un atacante;
- un malware;
- un incendio;
- un error humano.

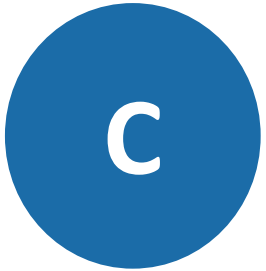
Ejemplo completo de la cadena de riesgo

Activo	Sistema académico universitario
Vulnerabilidad	Contraseñas débiles
Amenaza	Ataque de fuerza bruta
Riesgo	Acceso no autorizado a información académica

1.6 Principios Fundamentales · La Tríada CIA

¿Qué características debe conservar la información para que podamos considerarla adecuadamente protegida?
La respuesta se encuentra en los principios fundamentales de la seguridad, también denominados atributos de seguridad u objetivos de la seguridad.

Base conceptual de ISO/IEC 27001, 27002 y publicaciones del NIST



Confidencialidad

¿Quién puede acceder a la información?

Integridad

¿La información a sido modificada?

Disponibilidad

¿La información puede utilizarse cuando se necesita?

Los tres son igualmente importantes. La ausencia de cualquiera de ellos compromete la seguridad de la información

1.6.3 Confidencialidad

Es el principio que garantiza que la información solo pueda ser conocida, utilizada o divulgada por personas, procesos o sistemas debidamente autorizados.

Amenazas

- Accesos no autorizados
- Robo de credenciales
- Espionaje
- Interceptación de comunicaciones
- Pérdida de dispositivos

Mecanismos de protección

- Control de acceso (roles, permisos)
- Autenticación multifactor (MFA)
- Cifrado (almacenamiento y transmisión)
- Clasificación de la información (pública, uso interno, confidencial, secreta)
- Capacitación del personal

Solo deben acceder a la información quienes tienen autorización para hacerlo.

1.6.4 Integridad

Es el principio que garantiza que la información no sea modificada, destruida o alterada de forma no autorizada o accidental.

Características clave (según ISO/IEC 27000)

Exactitud	Completitud	Consistencia	Validez
Refleja fielmente la realidad	No faltan partes esenciales	Coherencia entre datos	Cumple las reglas establecidas

Amenazas: error humano, fallas de software, malware, ataques, fallas de hardware, errores de transmisión.

Mecanismos: validación de datos, control de cambios, copias de seguridad, auditoría.

Ejemplo crítico: modificar la dosis de un medicamento en una historia clínica puede poner en riesgo la vida del paciente.

Diferencias entre Confidencialidad e Integridad

Confidencialidad	Integridad
Protege el acceso a la información	Protege el contenido de la información
Evita divulgaciones	Evita modificaciones indebidas
Pregunta principal: ¿Quién puede verla?	Pregunta principal: ¿La información sigue siendo correcta?
Se protege con autenticación, autorización y cifrado	Se protege con validaciones, hash, firmas digitales y auditoría

1.6.6 Disponibilidad

¿De qué sirve que la información sea confidencial e íntegra si no puede utilizarse cuando se la necesita?

La disponibilidad es el principio que garantiza que la información, los sistemas y los servicios se encuentren accesibles y utilizables por los usuarios autorizados en el momento en que los necesiten.

Amenazas

Fallas de hardware

Discos, fuentes, memoria

Errores humanos

Configuración incorrecta

Cortes eléctricos

Sin UPS ni generadores

Desastres naturales

Incendio, inundación…

Ataques (DoS/DDoS)

Ransomware, sabotaje, ransomware

Fallas en Proveedores externos

ISP, nube, DNS

Mecanismos para garantizar la Disponibilidad

Redundancia	Copias de seguridad	Monitoreo
Servidores, enlaces, fuentes y discos (RAID) alternativos.	Permiten recuperar información ante pérdidas.	Detectar fallas antes de que se conviertan en interrupciones (uso excesivo de CPU, poco espacio en disco, etc).

Mantenimiento preventivo	Planes de contingencia	Recuperación ante desastres
Actualizaciones de software, reemplazo de componentes, limpieza de equipos, verificación del estado del sistema.	Procedimientos, responsables y recursos alternativos.	Restaurar la infraestructura después de eventos graves.

Diferencias entre Integridad y Disponibilidad

Integridad	Disponibilidad
Protege el contenido de la información	Protege el acceso oportuno a la información
Evita modificaciones indebidas	Evita interrupciones del servicio
Responde a la pregunta: "¿La información sigue siendo correcta?"	Responde a la pregunta: "¿La información puede utilizarse cuando se necesita?"
Se apoya en hash, firmas digitales, validaciones y auditorías	Se apoya en redundancia, respaldo, monitoreo y planes de contingencia

1.6.7 Autenticidad

¿Cómo se puede asegurar que una persona, un dispositivo o un sistema es realmente quien dice ser?

La autenticidad es la propiedad que garantiza que una entidad, un dato o un recurso es genuino y corresponde realmente a quien afirma ser.

Amenazas principales

- Suplantación de identidad (spoofing)
- Phishing
- Robo de credenciales
- Certificados falsificados

Mecanismos clave

- Usuarios y contraseñas
- Autenticación multifactor (MFA)
- Certificados digitales
- Firmas digitales

Ejemplo: el navegador verifica el certificado digital del banco antes de permitir el ingreso de credenciales. Si el certificado es inválido, muestra una advertencia.

1.6.8 No Repudio

¿Cómo puede demostrarse quién realizó realmente una acción?

El No Repudio es el principio que garantiza que una entidad no pueda negar posteriormente haber realizado una determinada acción.

Una vez realizada una acción y registrada mediante mecanismos adecuados, su autor no puede negar legítimamente haberla efectuado.

Acciones que requieren No repudio *(es importante cuando existen consecuencias legales o económicas)*

Firma de contratos	Aprobación de pagos	Emisión de facturas electrónicas
Declaraciones impositivas	Recetas médicas electrónicas	Actas de examen

Amenazas: Credenciales compartidas, contraseñas robadas, Ausencia de registros, falta de mecanismos criptográficos, manipulación de evidencias.
Mecanismos: Firma digital · Certificados · Sellado de tiempo · Registros de auditoría · Identidades únicas

Diferencia clave con autenticidad: la autenticidad verifica “¿quién es?”, el no repudio demuestra “¿quién realizó esta acción?” y evita que se niegue.

Diferencias entre Autenticidad y No Repudio

Autenticidad	No Repudio
Verifica quién es una entidad	Impide que una entidad niegue posteriormente una acción realizada
Se centra en la identidad	Se centra en la responsabilidad sobre una acción
Responde a la pregunta: "¿Quién es?"	Responde a la pregunta: "¿Quién realizó esta acción?"
Se implementa mediante autenticación y certificados	Se implementa mediante firmas digitales, certificados, sellos de tiempo y evidencias

1.6.9 Trazabilidad

¿Quién eliminó el archivo? ¿Cuándo ocurrió? ¿Desde qué equipo? ¿Qué usuario inició sesión? ¿Qué otros archivos modificaron?

*La **trazabilidad** es la capacidad de registrar y reconstruir las acciones realizadas sobre la información, los sistemas y los recursos tecnológicos, permitiendo identificar quién realizó una acción, cuándo la realizó, sobre qué recurso actuó y cuál fue su resultado.*

¿Qué debe registrarse?

Usuario

Quién realizó la acción

Fecha y hora

Cuándo ocurrió

Recurso

Sobre qué se actuó

Acción

Qué se hizo

Resultado

Éxito, rechazo o error

Origen

IP, equipo, dispositivo

***Amenazas**: borrado de logs, modificación de datos, inyección de comandos, inyección de eventos, ataques DoS a logs*

***Mecanismos**: registro de auditoria, sistemas de monitoreo, gestión centralizada de registros, protección de registros, sincronización horaria.*

Diferencias entre No Repudio y Trazabilidad

No Repudio	Trazabilidad
Impide que una entidad niegue una acción realizada	Permite reconstruir todas las acciones realizadas
Se centra en demostrar la autoría	Se centra en registrar la secuencia completa de eventos
Utiliza principalmente firmas digitales y certificados	Utiliza registros de auditoría, monitoreo y control de eventos
Responde a la pregunta: "¿Quién realizó esta acción?"	Responde a las preguntas: "¿Qué ocurrió?, ¿cuándo?, ¿dónde y cómo?"

1.6.10 Integración de los Principios

Principio	Pregunta clave	Objetivo
Confidencialidad	¿Quién puede acceder?	Evitar accesos no autorizados
Integridad	¿Sigue siendo correcta?	Evitar modificaciones indebidas
Disponibilidad	¿Puede utilizarse ahora?	Garantizar acceso oportuno
Autenticidad	¿Quién es realmente?	Verificar identidades y origen
No Repudio	¿Quién realizó la acción?	Impedir negar una acción
Trazabilidad	¿Qué ocurrió, cuándo y cómo?	Reconstruir la secuencia de eventos

1.7 Clasificación de medidas de seguridad

Seguridad Activa

Previene y evita daños.

- Firewall
- Antivirus / Antimalware
- Autenticación multifactor
- Control de acceso físico
- IDS / IPS
- Cifrado
- CCTV con monitoreo

Seguridad Pasiva

Reduce consecuencias y facilita la recuperación.

- Copias de seguridad
- UPS y generadores
- RAID
- Puertas cortafuego
- Materiales ignífugos
- Planes de recuperación
- Centros de datos alternativos

Comparación y complementariedad

Seguridad Activa	Seguridad Pasiva
Previene daños	Reduce las consecuencias de los daños
Actúa antes de que ocurra el daño	Actúa cuando el daño ya se produjo
Busca evitar interrupciones	Busca restablecer el funcionamiento
Ejemplos: firewall, antivirus, MFA	Ejemplos: backup, UPS, RAID

Ninguna es suficiente por sí sola. Una estrategia eficaz combina ambos tipos de medidas de forma complementaria.

Ejemplo: Centro de cómputos de la Facultad

Tarjetas + biometría	Activa
Firewall perimetral	Activa
MFA para administradores	Activa
Antivirus centralizado	Activa
Copias de seguridad diarias	Pasiva
UPS	Pasiva
Grupo electrógeno	Pasiva

Ejemplo de seguridad activa y pasiva con amenazas

Amenaza	Medidas de seguridad activa	Medidas de seguridad pasiva
Acceso no autorizado	Autenticación, MFA, control de acceso, biometría	Registros de auditoría, copias de seguridad, planes de recuperación
Malware	Antivirus, antimalware, firewall, actualización del software	Copias de seguridad, restauración del sistema
Falla del suministro eléctrico	Mantenimiento de la instalación eléctrica, monitoreo del suministro	UPS, generadores eléctricos, líneas redundantes
Incendio	Detectores de humo, alarmas	Puertas cortafuego, sistemas automáticos de extinción, copias de seguridad externas
Robo de equipos	CCTV, control de acceso, guardias, cerraduras	Cifrado de discos, copias de seguridad, equipos de reemplazo
Error humano	Capacitación, procedimientos, validación de datos	Copias de seguridad, control de versiones, recuperación de información
Falla de hardware	Monitoreo preventivo, mantenimiento	RAID, servidores redundantes, equipos de reserva
Desastres naturales	Selección adecuada de la ubicación, diseño resistente	Centro alternativo, copias externas, plan de recuperación ante desastres

Unidad 1 completada

Introducción a la Seguridad Informática

¿Preguntas?

Facultad de Ingeniería · Universidad Nacional de Jujuy