SEGURIDAD INFORMÁTICA

- ***Conjunto de medidas preventivas, de detección y corrección destinadas a proteger la integridad, la confidencialidad y la disponibilidad de los recursos informáticos.***
- ***Se ocupa de proteger la información de la organización en cualquier forma en que se encuentre.***

CONFIDENCIALIDAD → la información debe ser accedida sólo por personal autorizado.

INTEGRIDAD → toda modificación de datos/información es realizada por personas autorizadas, utilizando procedimientos específicos.

DISPONIBILIDAD → la información y los datos se encuentran disponibles cuando se los necesite.

IDENTIFICACIÓN → acto de proveer credenciales que permitan determinar la identidad de un sujeto.

AUTENTICACIÓN → comprobación de las credenciales recibidas para determinar si el sujeto es quien dice ser.

AUTORIZACIÓN → determinación de los permisos de acceso de un sujeto (ya identificado y autenticado) sobre un sujeto.

RESPONSABILIDAD → habilidad para determinar las acciones individuales de un usuario dentro de un sistema y para identificar a dicho usuario.

PRIVACIDAD → determina el nivel de confidencialidad y de protección de privacidad que se le brinda a un usuario dentro de un sistema.

NO REPUDIO – VALIDACIÓN DE IDENTIDAD → utilización de elementos de información única que permite validar la autenticidad de una persona.

SEPARACIÓN DE TAREAS → aquellas personas involucradas en la revisión y/o el análisis de uso no autorizado de activos no deben estar en condición de efectuar dicho uso no autorizado.

REGLA DE MÍNIMO PRIVILEGIO → un usuario/administrador/proceso/programa debe tener el mínimo privilegio necesario, y posible, para realizar su tarea → se deben otorgar aquellos permisos que aseguren que la tarea se pueda hacer, ni más ni menos.

Otros objetivos de la seguridad de la información:

- **EFICACIA** → sistemas de información correctos.
- **EFICIENCIA** → óptima utilización de recursos.
- **CUMPLIMIENTO** de normas y procedimientos.
- **CONFIABILIDAD** → brindando información correcta.

AMENAZA → todo hecho que pueda perjudicar bienes o personas.

RIESGO → la medida de la posibilidad que una amenaza se concrete.

VULNERABILIDAD → debilidades frente a las amenazas.

PLAN DE CONTINGENCIA → forma de actuar cuando una amenaza se ha concretado, de manera que dicho hecho impacte lo menos posible.

ANÁLISIS DE RIESGO → proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización.

GESTIÓN DE RIESGO → selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir y controlar los riesgos identificados.

NORMA ISO 27001 – *Objetivos de control y controles*

Política de seguridad

- Política de seguridad de información → proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.

Organización de la Seguridad de la Información

- Organización interna → manejar la seguridad de la información dentro de la organización.
- Entidades externas → mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o son manejados por entidades externas.

Gestión de activos

- Responsabilidad por los activos → lograr y mantener la protección apropiada de los activos organizacionales.
- Clasificación de la información → asegurar que la información reciba un nivel de protección apropiado.

Seguridad en los RRHH

- Antes del empleo → asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.
- Durante el empleo → asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.
- Terminación o Cambio de empleo → asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.

Seguridad física y ambiental

- Áreas seguras → evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
- Seguridad del equipo → evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

Gestión de las comunicaciones y las operaciones

- Procedimientos y responsabilidades operacionales → asegurar la operación correcta y segura de los medios de procesamiento de la información.
- Gestión de la entrega del servicio de terceros → implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.
- Planeación y aceptación del sistema → minimizar el riesgo de fallas en los sistemas.
- Protección contra software malicioso y código móvil → proteger la integridad del software y la información.
- Respaldo (*back-up*) → mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.
- Gestión de seguridad de redes → asegurar la protección de la información de redes y la protección de la infraestructura de soporte.
- Gestión de medios → evitar la divulgación, modificación, eliminación y/o destrucción no autorizada de los activos; y la interrupción de actividades comerciales.
- Intercambio de información → mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.

- Servicios de comercio electrónico → asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.
- Monitoreo → detectar actividades de procesamiento de información no autorizadas.

Control de acceso

- Requerimiento comercial para el control de acceso → controlar acceso a la información.
- Gestión del acceso al usuario → asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los SI.
- Responsabilidades del usuario → evitar el acceso de usuarios no autorizados y el compromiso o robo de la información y los medios de procesamiento de la información.
- Control de acceso a redes → evitar el acceso no autorizado a los servicios en red.
- Control de acceso al sistema de operación → evitar acceso no autorizado a los sistemas operativos.
- Control de acceso a la aplicación de información → evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.
- Computación móvil y teletrabajo → asegurar la seguridad de la información cuando se utilicen medios de computación móvil y teletrabajo.

Adquisición, desarrollo y mantenimiento de los SI

- Requerimientos de seguridad en los sistemas → asegurar que la seguridad sea una parte integral de los SI.
- Procesamiento correcto en las aplicaciones → evitar errores, pérdidas y/o modificación no autorizada o mal uso de la información en las aplicaciones.
- Controles criptográficos → proteger confidencialidad, autenticidad e integridad de la información a través de medios criptográficos.
- Seguridad de los archivos del sistema → garantizar la seguridad de los archivos del sistema.
- Seguridad en los procesos de desarrollo y soporte → mantener la seguridad del software e información del sistema de aplicación.
- Gestión de vulnerabilidad técnica → reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

Gestión de incidentes en la seguridad de la información

- Reporte de eventos y debilidades en la seguridad de la información → asegurar que la información de los eventos y debilidades en la seguridad de la información asociados a los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.
- Gestión de incidentes y mejoras en la seguridad de la información → asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad.

Gestión de la continuidad comercial

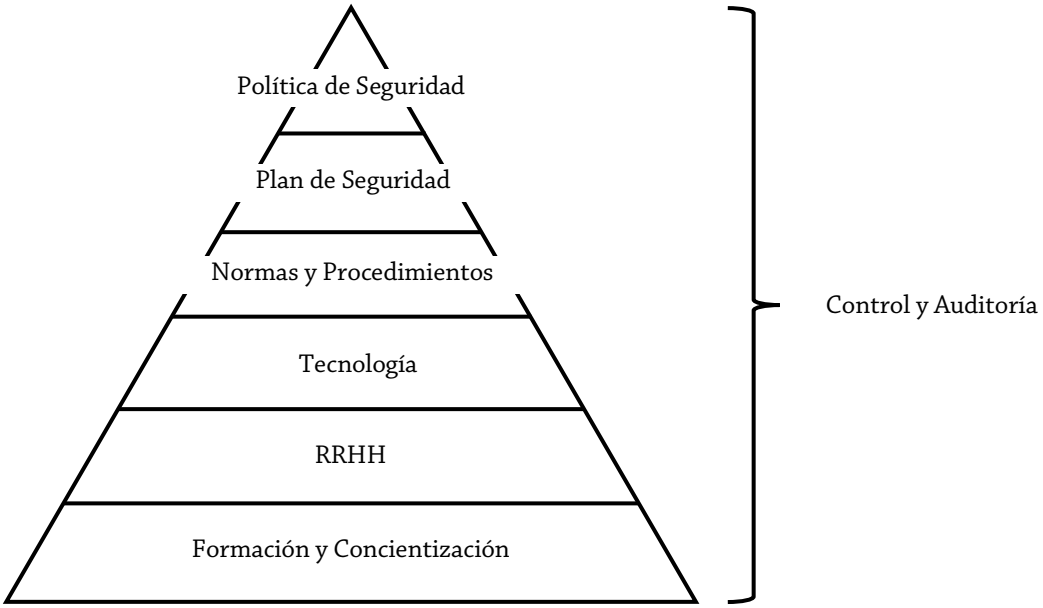
- Aspectos de la seguridad de la información de la gestión de la continuidad comercial → contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los SI y asegurar su reanudación oportuna.

Cumplimiento

- Cumplimiento con requerimientos legales → evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.
- Cumplimiento con las políticas y estándares de seguridad – Cumplimiento técnico → asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.
- Consideraciones de auditoría de los SI → maximizar la efectividad del proceso de auditoría de los SI y minimizar la interferencia de y/o desde el proceso de auditoría de los SI.

NORMA DE SEGURIDAD BANCARIA

Esquema básico de un plan de seguridad:



- Política de Seguridad:
  - El gerente de la empresa define qué tipo de seguridad se empleará.
  - El gerente de la empresa deberá tener la fuerza para que el plan se ejecute.
- Plan de seguridad → todos los actores del área protegida deben estar comprometidos con él.
  - Valoración de los bienes a proteger el valor de reposición y el valor de uso.
  - Identificación de riesgos.
  - Analizar medidas a tomar en relación costo–beneficio.
  - Implementar medidas para disminuir los riesgos.
  - Crear un plan de contingencia.
  - Documentar el plan de seguridad.
- Normas y Procedimientos → medidas y acciones que todos los integrantes del área protegida deben cumplir a efectos de disminuir los riesgos.
- Tecnología → referido a los sistemas de seguridad financiera.
- RRHH → referido al factor humano:
  - Identificación y/o autenticación sobre las personas.
  - Pacto de confidencialidad.
  - Verificación de antecedentes.
- Formación y Concientización → debe ser otra constante para todos los integrantes del área protegida y debe existir una continua capacitación.

Estructura del área de sistemas

- Debe ser independiente de los usuarios.
- Debe existir una segregación de tareas y control por oposición: desarrollo, operaciones, soporte técnico y supervisión.

Estrategias de seguridad

- Debe considerar las amenazas y vulnerabilidades asociadas a cada entorno tecnológico.
- Deberá contemplar el establecimiento de mecanismos de control para la detección, el registro, el análisis, la comunicación, la corrección, la clasificación y la cuantificación de los incidentes.

- En los nuevos proyectos informáticos se deberá contemplar los requerimientos de seguridad desde sus etapas iniciales.
- Se deben estandarizar: los procedimientos, las rutinas informáticas y las rutinas administrativas.

Política formal de Seguridad Informática

- Se deben detallar:
    - El nivel de confidencialidad de los datos.
    - El procedimiento de otorgamiento de claves de usuarios para el ingreso a los sistemas.
    - Estándares fijados para el acceso y la autenticación de usuarios.
- Se debe restringir el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción, dejando documentado cuando ello ocurra.
- El equipamiento informático debe estar inventariado, documentada su ubicación, la topología de las redes y el software instalado.
- Se deben implementar métodos de identificación y autenticación:
    - Cambio obligatorio de las contraseñas en el primer inicio de sesión.
    - Registro histórico de las últimas 12 contraseñas usadas.
    - Caducidad de las contraseñas a los 30 días.
    - Desconexión automática por inactividad a los 15 minutos.
    - Encriptación para el archivo de las contraseñas.
    - Identificación única de usuarios.

Sobre **las aplicaciones**, deberán existir:

- Documentación de los sistemas aplicativos.
- Operación de procesos informáticos.
- Procesos de recuperación y de resguardo de datos.
- Manuales de usuario.
- Procedimiento de transferencias de fondos.

Sobre **las operaciones**, debe existir una planificación y documentación adecuada (escrita y actualizada) de las actividades que se desarrollan normalmente en el centro de procesamiento de información.

Los sistemas de información computarizados deben tener incorporados en su programación validaciones y controles mínimos para asegurar la integridad y la validez de la información que procesan.

Sobre **el software malicioso**:

- Se deben implementar herramientas para su prevención, detección y eliminación.
- Se debe prevenir la presencia de código malicioso.
- Se debe impedir la instalación y utilización de software no autorizada.

Sobre los mecanismos de **distribución de la información**:

- Se debe impedir la difusión de información a personas no autorizadas.
- Se deben realizar análisis para la implementación de los controles necesarios para limitar la pérdida de confidencialidad en la distribución de la información.

Sobre **la seguridad física**:

- Se debe permitir el acceso al área de procesamiento (en la cual debe haber detectores/aspiradoras de humo y elementos para extinguir incendios) solamente al personal autorizado.
- La documentación de datos debe estar resguardada, con medidas de seguridad adecuadas.

Por cada sistema aplicativo, se debe mantener actualizada **la documentación técnica** que contenga objetivos, alcances, diagramas del sistema, registro de modificaciones, lenguajes de programación y descripción del software y hardware utilizados.

CRIPTOGRAFÍA

- ***Rama de la informática que hace uso de métodos y técnicas con el objetivo de cifrar y proteger un mensaje o un archivo mediante un algoritmo usando una o más claves.***

Tipos de algoritmos

- Según la naturaleza del algoritmo:
  - Sustitución → se cambian unos símbolos por otros.
  - Transposición → cambia el orden o la ubicación de los símbolos.
- Según el número de bits cifrados a la vez:
  - Bloque → divide el texto en bloques de igual longitud para luego cifrar uno por uno por separado.
  - Flujo → se cifra cada símbolo (carácter) bit a bit.
- Según la clave utilizada:
  - Simétrico → se utiliza la misma clave para cifrar y descifrar.
    - De claves privadas. Emisor y receptor comparten la misma clave para cifrar y descifrar.
    - Requiere de un canal seguro para poder compartir la clave.
    - Mensaje y clave no deben ir en el mismo medio.
  - Asimétrico → se utilizan claves distintas para cifrar.
    - De claves públicas. Emisor y receptor tienen un par de claves: una pública y una privada.
    - El emisor cifra con la clave pública y el receptor descifra con la clave privada.
  - Irreversible → cifra un texto claro impidiendo su descifrado.

Función HASH → operación realizada sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado un "resumen" de tamaño fijo e independiente del tamaño original. Sirve para comprobar integridad.

- HASH → resultado de la función.
- Colisión → aquello ocurrido cuando 2 textos distintos tienen el mismo hash.
- "Un buen algoritmo de hash es aquel que no permita colisiones".
- Aplicaciones en: contraseñas, firmas digitales, integridad y autenticación.
- Una función hash debe:
  - Ser rápida de calcular.
  - Distribuir los elementos de manera uniforme en todo el rango de salida.
  - Devolver siempre el mismo hash para una misma entrada.

Protocolos seguros

- SSL (*Secure Socket Layer*) → protege los datos que se transmiten a través de la red.
- PGP (*Pretty Good Privacy*) → además de proteger los datos que se transmiten a través de la red, protege datos almacenados en discos, copias de seguridad, etcétera.

Firma digital

- Mecanismo criptográfico que le permite al receptor de un mensaje firmado digitalmente identificar al emisor confirmando la integridad del mensaje (por hash), es decir, confirmando que el mensaje no haya sido alterado.
- Avalada por el Estado.

Firma electrónica

- No avalada por el Estado.

VULNERABILIDADES WEB

1. **Inyección** → incluir comandos mal intencionados en los datos de una aplicación, los cuales son enviados a un intérprete, quien toma esos datos e interpreta los comandos como válidos.
   - Impacto típico: todos los contenidos de una base de datos pueden potencialmente ser leídos o modificados.

2. **Secuencia de comandos en sitios cruzados (XSS)** → ocurre cada vez que datos no validados de un atacante son enviados al navegador de una víctima.
   - Impactos típicos:
     - Robo tanto de la sesión del usuario como de datos sensibles.
     - Redireccionar un usuario hacia un sitio de malware o phishing.

3. **Pérdida de autenticación y gestión de sesiones:**
   - HTTP es un protocolo "sin estado": las credenciales tienen que viajar en cada pedido HTTP; debería usar SSL para todo contenido que requiere autenticación.
   - Impactos típicos:
     - Cuentas de usuario comprometidas.
     - Sesiones de usuario secuestradas.

4. **Referencia directa insegura a datos** → proteger el acceso a los datos forma parte de realizar una "autorización" apropiada.
   - Impacto típico → usuarios capaces de acceder a archivos o a datos sin autorización.

5. **Falsificación de petición en sitios cruzados (CSRF)** → ataque donde el navegador de la víctima es engañado para que emita un comando a una aplicación web vulnerable.
   - Impactos típicos:
     - Iniciar transacciones (transferencias de fondos, desconectar el usuario, cierre de cuenta, etcétera).
     - Acceder a datos sensibles.
     - Cambiar detalles de la cuenta.

6. **Configuración defectuosa de seguridad** → las aplicaciones web dependen de cimientos seguros: desde el sistema operativo hasta el servidor de aplicaciones (sin olvidar las librerías utilizadas).
   - Impactos típicos:
     - Instalación de código malicioso debido a un parche faltante en el sistema operativo o servidor.
     - Acceso no autorizado a cuentas por defecto debido a una configuración defectuosa del servidor.

7. **Almacenamiento criptográfico inseguro:**
   - Ocurre cuando:
     - No se identifican todos los datos sensibles.
     - No se identifican todos los lugares donde los datos sensibles son almacenados.
     - No se protege esta información en todas sus ubicaciones.
   - Impactos típicos:
     - Atacantes acceden y modifican información privada o confidencial.
     - Mala imagen para la empresa – Clientes insatisfechos – Pérdida de confianza.
     - Gastos para corregir el incidente.

8. **Falla de restricción de acceso a URL** → proteger el acceso a URLs forma parte de realizar una autorización apropiada.
   - Impactos típicos:
     - Atacantes invocan funciones o servicios a los cuales no se encuentran autorizados.
     - Acceso a otras cuentas de usuario y datos.
     - Realizar acciones privilegiadas (admin).

9. Protección insuficiente en la capa de transporte:

- Ocurre cuando:
  - No se identifican todos los datos sensibles.
  - No se identifican todos los lugares donde los datos sensibles son almacenados.
  - No se protege esta información en todas sus ubicaciones.
- Impactos típicos:
  - Atacantes acceden y modifican información privada o confidencial.
  - Mala imagen para la empresa – Clientes insatisfechos – Pérdida de confianza.
  - Gastos para corregir el incidente.

10. Redirecciones y destinos no validados:

- Las redirecciones en aplicaciones web son muy comunes:
  - Frecuentemente incluyen parámetros suministrados por el usuario en la URL destino.
  - Si no son validados, el atacante puede enviar a la víctima a un sitio de su elección.
- Impactos típicos:
  - Redireccionar a una víctima hacia un sitio de phishing o malware.
  - El pedido del atacante es ejecutado, pasando por alto los controles de seguridad.

MALWARE – SOFTWARE MALICIOSO

- ***Todo tipo de programa o código de computadora cuya función es dañar un sistema o bien causar un mal funcionamiento.***

Clasificación

- Virus propios → programas creados para producir algún daño en el sistema del usuario.
  - Tienen módulos de reproducción–ataque–defensa y precisan de un anfitrión.
  - Actúan de forma transparente al usuario.
- Bombas lógicas → no se reproducen hasta que se cumplen ciertas condiciones pre-programadas.
- Conejos.
- Gusanos → código malicioso que no infecta archivos.
  - Se reproducen fácil y eficientemente en otras computadoras.
- Troyanos → código malicioso que simula ser inofensivo y útil para el usuario.
  - Necesita del humano para propagarse.
- Hoax → mensajes con contenido falso y engañoso, normalmente distribuido en cadena.
- Zombis → PC infectada que es controlada a distancia por un hacker.
- De Active X.
- De HTML.
- Ransomware → restringen el acceso a archivos infectados pidiendo un rescate a cambio de quitar esa restricción. Algunos ransomware cifran archivos del sistema operativo inutilizando así el dispositivo.
- Spyware → aplicación cuyo fin es recolectar información del usuario sin su consentimiento. Son programas secundarios que se instalan por haber instalado otra cosa antes.
- Backdoors → troyano que abre puertos en el sistema.

Herramientas de prevención

- Proxy → controla lo que sale.
- Firewall → controla lo que entra.

Mecanismos de detección de virus

- CheckSum.
- Firmas.
- Holístico.

EXPLOIT → programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta diferencia en beneficio del creador del mismo.

PHISHING → modalidad de estafa, basada en suplantación de sitios en Internet, diseñada con la finalidad de robar la identidad y obtener información personal de usuarios.

AUDITORÍA INFORMÁTICA

- ***Opinión profesional que determina si el objeto sometido a estudio refleja la realidad.***

INFORME TÉCNICO → opinión profesional sin necesidad de ratificar la auditoría (con alguna prueba) basada en la experiencia de la informática.

PERICIA INFORMÁTICA → opinión profesional que, en base al análisis de pruebas acortadas, emite un dictamen de lo acontecido.

AUDITORÍA → opinión profesional emitida tras haber buscado las pruebas que la ratifiquen.

Tipos de auditoría

- Auditoría financiera → veracidad de los estados financieros, prácticas y principios contables.
- Auditoría tributaria → observa el cumplimiento del código tributario.
- Auditoría de gestión → analiza los logros del proceso administrativo, funciones, métodos, etcétera.
- Auditoría ambiental.
- Auditoría gubernamental.
- Auditoría de sistemas → referida a la función informática.
    - Auditoría de la operación informática → la operación informática se ocupa de producir resultados informáticos de todo tipo.
    - Auditoría de desarrollo de proyectos → ciclo de vida de los sistemas; se usa metodología de desarrollo de proyectos informáticos.
    - Auditoría informática de sistemas → analiza la "técnica de sistemas" en todas sus facetas.
    - Auditoría informática de comunicaciones y redes → las comunicaciones con el soporte físico–lógico de la informática en tiempo real.
    - Auditoría de la seguridad física y lógica → sobre el hardware, los soportes de datos y sobre el uso del software.

Objetivos de la auditoría informática

- Optimizar el costo–beneficio de los sistemas.
- Asegurar integridad, confidencialidad y confiabilidad de la información.
- Conocer tanto la situación actual del área informática como las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones.
- Apoyo de la función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar los riesgos en el uso de tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los SI.

Clasificación de los controles

- Preventivos → reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
- Detectivos → detectan los hechos después de ocurridos.
- Correctivos → ayudan a la investigación y corrección de las causas del riesgo.

CASOS REALES DEL LIBRO "DELITOS INFORMÁTICOS"

Velocidad y origen de la información que nos llega

- *"Yuyo" estafó a SITA (Sociedad Internacional de Telecomunicaciones Aeronáuticas) haciéndose pasar por una compañía aérea que les compraría pasajes. SITA generaba las confirmaciones sin ningún problema.*

  SITA siempre daba por cierto la codificación que tenía como origen, nunca controlaba el origen de los requerimientos para el envío de pasajes.
- ***Siempre hay que constatar la veracidad y el origen de la información que nos llega.***

Control de insumos

- *Un cajero de peaje llamado Juan y su supervisor Hugo hacían figurar a camiones (por ejemplo) por vehículos oficiales (que no pagaban) y Juan y Hugo se quedaban con la diferencia.*

  Emitían vales (duplicados), cuyo papel era insumo de la empresa de peajes.
- ***Siempre hay que controlar los insumos en los sistemas informáticos.***

Control de operadores de un sistema informático

- *En una lista de sueldos, aparecía un empleado dado de baja hacía un año que cobraba más que cualquier gerente. Hubieron muchas liquidaciones fantasmas.*

  La lista era confeccionada por una auditoría, pero ésta nunca era controlada.
- ***Siempre hay que controlar los operadores de un sistema informático.***

  Si tenemos herramientas para auditar, hay que usarlas.

Claves de acceso

- *Un empleado de una financiera (Ignacio) aprovechó que los cajeros descuidaran por unos minutos la computadora con el sistema abierto para transferir dinero a su cuenta.*

  No era necesaria ninguna clave para el ingreso al sistema.
- ***No alejarse de la computadora cuando el sistema está abierto.***

  Nunca dar las claves de acceso a los sistemas.

  No anotar las claves de acceso cerca de la computadora.

Confidencialidad de los datos en sistemas informáticos

- *"Carlos" y "el Negro" compraron bases de datos de personas de alto poder poder adquisitivo. Tiempo después, se hicieron pasar por una empresa de turismo para estafarlos ($100 en aquel momento a cada "cliente").*

  Falló el control y el resguardo de las bases de datos con información de personas.
- ***Regla básica: la confidencialidad de los datos en los sistemas informáticos.***

  Los datos de las personas son muy codiciados.

Instalación de software de origen desconocido

- *Un disquete tenía un troyano, el cual se hacía pasar por un software con información sobre el SIDA. Al ejecutarse, el virus imprimía una factura que debía pagarse a una cuenta en Panamá.*

  Nunca descubrieron al troyano.
- ***No instales software ni ingreses datos en tu computadora si desconoces el origen.***

La seguridad informática y el personal de seguridad

- *Billetes de lotería ganadores que iban sospechosamente a un mismo lugar. Un tipo, usando a amigos y a parientes, los retiraba de las agencias.*

  Si bien el jefe de seguridad no dio con el mentor del plan, sí pudieron hacerlo los técnicos informáticos.
- ***Las políticas y normas de seguridad informática deben ser desarrolladas por personas de informática. El personal de seguridad sólo debe colaborar.***

Módulos informáticos de evasión fiscal

- *Jesús y Francisco instalaron un módulo de evasión en sus computadoras del restaurante para hacerle creer al fisco que facturaban poco y, de esa manera, tributar menos.*
- ***Los módulos informáticos no sólo evaden al fisco sino que también pueden vulnerar el patrimonio de quien los usa.***

Control de reimpresión de comprobantes

- *Francisco (analista) y Patricia (cajera) idearon un sistema para que siempre, de alguna forma, quedara un sobrante en caja, que luego Patricia retiraría.*
- ***Siempre se debe controlar la reimpresión de comprobantes y documentos contables en los sistemas informáticos.***

Hackers: ¿cómo descubrirlos?

- *[Varias historias de cómo atraparon a diversos hackers].*

  La mayoría de los policías los atrapan por basarse en el hecho de que los hackers necesitan contar su accionar, su ego les exige publicidad.

Back-up

- *[Tres ejemplos referentes al ambiente en donde se resguarda la información].*
- ***Siempre hacer back-up bajo un ambiente seguro.***

Sistemas informáticos de los cajeros informáticos

- *[Diferentes casos de empleados de sistemas que se aprovecharon de los sistemas de cajeros automáticos para extraer montos mayores al permitido].*
- ***Es común que se quieran vulnerar los sistemas informáticos de los cajeros automáticos.***

El peligro del home banking

- *Hackers que ingresaron a las cuentas de banco de usuarios (las contraseñas eran muy débiles) extrajeron dinero y bloquearon el ingreso a las demás cuentas.*
- ***El home banking tiene sus peligros.***

Control de acceso como herramienta de seguridad

- *Secuestraron a 3 empleados que tenían claves de acceso para girar dinero.*

  Los ladrones no lograron su cometido porque ignoraron el uso de dígitos verificadores, de manera que no pudieron realizar las transferencias.
- ***El control de acceso también forma parte de la seguridad informática.***