VI Jornadas de Auditores Internos de Universidades Nacionales

Facultad de Ciencias Económicas UNER

SEGURIDAD DE TI
METODOLOGÍA DE REVISIÓN

EVIDENCIAS DIGITALES

Contenidos

- Conceptos
- Enfoques de riesgo
- Objetivos de protección
- Amenazas
- Estrategia de seguridad
- Herramientas (ejemplos)
- Políticas/estándares
- Rol de auditoría
- Una metodologías de revisión
- Procedimientos indagatorios – Check list base
- Evidencias digitales

Riesgo / Seguridad

Seguridad de la Información:

- Todas aquellas medidas **preventivas y reactivas** del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando mantener la **confidencialidad**, la **disponibilidad** y la **integridad**.

Ciberseguridad o seguridad informática:

- Es un conjunto de procedimientos y herramientas que se implementan para proteger los **datos e información que se genera y procesa a través de la infraestructura de sistemas** (Informe N° 25 FACPCE. Base COSO Ciberseguridad)

Integran el marco de la seguridad informática:

- Estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Comprende:

- Personas, infraestructura, software, bases de datos, metadatos, archivos, comunicaciones y todo lo que la organización valore (activo) de su sistema de información y signifique un riesgo si llega a manos de otras personas, se pierde, destruye o inutiliza... ***Entorno informático***

Seguridad Informática

El objetivo de un programa de seguridad de los sistemas de información es proteger la información de una organización reduciendo a un nivel aceptable el riesgo de pérdida de confidencialidad, integridad y disponibilidad de dicha información.

Un buen programa de seguridad de la información implica dos elementos principales: el análisis y la gestión de riesgos.

Para gestionar el riesgo cibernético es necesario identificar los sistemas de información de valor y en su caso llevar a cabo las evaluaciones de riesgo sobre incidentes para esos activos.

Esto corresponde a la parte responsable, el auditor valorará la valoración de riesgos en función a las circunstancias.

Un incidente se compone de tres elementos: la amenaza, la vulnerabilidad y el impacto. Vulnerabilidades son propiedad de los activos que pueden ser explotados por una amenaza e incluyen deficiencias

Enfoque para crear el inventario de SI y la evaluación de riesgos

Identificar los sistemas de información

- Identifique **las categorías de información** en función de los objetivos de la empresa y de la organización utilizando como guía lo siguiente:
  - Políticas corporativas
  - Normas del sector (por ejemplo, ISO)
  - Requisitos reglamentarios
  - Objetivos empresariales
  - Propiedad Intelectual
  - Datos financieros.
  - Datos de clientes o empleados.

Identificar procesos y propietarios de los sistemas de información

- Identificar cómo se recoge, utiliza, transfiere, almacena y archiva la información
- **Identificar a los propietarios** de la empresa, del sistema y de la aplicación para los activos de información
- **Crear flujos de datos** para comprender cómo se mueve la información dentro de los procesos empresariales, los sistemas y aplicaciones.

Comprender los riesgos asociados a los sistemas de información

- Analizar los **inventarios de activos** y los **flujos de datos** para identificar los riesgos de control
- Evaluar **los probables autores** de los ciberataques y sus probables métodos de ataque
- Identificar **los controles** para hacer frente a los riesgos identificados en función del perfil de riesgo del proceso, sistema o aplicación

¿QUÉ ES UN «ACTIVO» DESDE EL ENFOQUE DE SEGURIDAD DE TI?

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. ***(Magerit)***

CLASIFICACIÓN

La seguridad de la información requiere una valoración de los activos, fundamentalmente los DATOS

Los datos se puede clasificar en distintas categorías:

- **Críticos: indispensables para la operación de la empresa.**
- **Valiosos: Tienen un alto grado de utilidad, se requieren y son un componente de valor para SI, pero su pérdida puede ser costosa pero no terminal.**
- **Sensibles: Definidos por la legislación, su tenencia y utilización implica cumplimiento de disposiciones y riesgos.**

La información debe tener ciertas características o cumplir con ciertos criterios:

Requisitos de Calidad:

- **Calidad, Costo y Entrega.**

(mayor calidad, a menor costo y menor plazo)

Requisitos Fiduciarios: (Informe COSO)

- **Eficacia y eficiencia de las operaciones**
- **Confiabilidad de la información**
- **Cumplimiento de las leyes y reglamentaciones**

Requisitos de Seguridad

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

+

Requisitos de Seguridad

- **Autenticidad**
- **Legitimidad**
- **Consistencia**
- **Validación**

Requisitos Fiduciarios: (Informe COSO)

Eficacia y eficiencia de las operaciones

Eficacia: Relevancia y pertinencia de la información para el proceso de negocio ya su entrega en forma oportuna, correcta, consistente, completa y que pueda utilizarse.

Eficiencia: Provisión de información mediante le uso óptimo de recursos.

Confiabilidad de la información: Provisión de la información apropiada para que la gerencia maneje la entidad y ejerza su responsabilidades de presentación de informes financieros y de cumplimiento de las leyes y las reglamentaciones.

Cumplimiento de las leyes y reglamentaciones: Cumplimiento de las leyes, reglamentaciones y disposiciones contractuales a las que esté sujeto el proceso de negocio, vale decir: criterios de negocios impuestos a nivel externo.

Triángulo CIA

Finalidad

- Confidencialidad
- Integridad
- Disponibilidad

- Autenticidad
- Legitimidad

Seguridad Informática

- **Objetivos**
- **Proteger los activos informáticos:**
  - **Información contenida**
    - Evitar el acceso no autorizado.
    - Asegurar el acceso autorizado en forma oportuna.
  - **Infraestructura computacional**
    - Proteger el equipamiento.
    - Prever hechos que atenten contra la infraestructura y su funcionamiento.
  - **Usuarios**
    - Personas que utilizan la infraestructura informática y gestionan la información.

Amenazas

Categorías

- **Interrupción:** ataque contra la disponibilidad
- **Intercepción:** ataque contra la confidencialidad
- **Modificación:** ataque contra la integridad
- **Fabricación:** ataque contra la integridad (autenticidad)

Provenientes de:

- Personas
- Malware
- Accidentes / Siniestros / Catástrofes

Amenazas Provenientes de Personas

- Insiders
- Ex empleados
- Piratas
- Intrusos remunerados
- Personal interno de Sistemas

Ingeniería Social: práctica de obtener información confidencial a través de la manipulación de usuarios legítimos:

- Trashing (buscar en la basura)
- Curiosidad (dejar un CD o pen)
- Suplantación (hacerse pasar por técnico o gerente)
- Shoulder Surfing (mirar sobre el hombro)
- Office Snooping (usuario deja un momento su sesión abierta)

Amenazas Provenientes de Malware

- **Virus:** código ejecutable que "infecta" otros archivos ejecutables para propagarse
- **Gusanos:** programa que se transmite a si mismo para infectar otros equipos de la red
- **Troyanos:** programa que se disfraza de algo inocuo o atractivo que invita al usuario a ejecutarlo
- **Sniffers:** programa que captura las tramas de una red (nivel de enlace)
- **Backdoors:** método para eludir los controles de autenticación al conectarse a una computadora
- **Rootkits:** técnicas que modifican el sistema operativo para permitir que un malware permanezca oculto
- **Adware:** programas que muestran publicidad de manera intrusiva
- **Spyware:** programas creados para recopilar información sobre las actividades desarrolladas por un usuario
- **Hijacking:** programas que realizan cambios en la configuración del navegador web
- **Keyloggers:** registran y almacenan todas las pulsaciones del teclado para su posterior envío al creador
- **Stealers:** buscan las contraseñas recordadas, las descifran y envían al creador
- **Rogue software**: hacen creer al usuario que la computadora está infectada, induciéndolo a pagar por un software inútil (que no necesita) para eliminar dicha supuesta infección

Amenazas Provenientes de Malware

- **Ransomware:** programas que encriptan archivos importantes del usuario, pidiendo un "rescate" para recibir la contraseña que permite recuperar el acceso al mismo.

Ampliemos el análisis

- 62,3 millones de ataques en mayo 2021.
- 14 millones más que los identificados en abril.
- 116 % de incremento con respecto a igual período de 2020.
- Records, sin antecedentes.
- Impacta en el enfoque de riesgo de las organizaciones por su efecto, interrupción de servicios y posible pérdida de datos.
- 2021: 318,6 millones más que en 2020.

El ransomware siguió cayendo en 2022, con un volumen de 493,3 millones, lo que supone un descenso interanual del 21 %.

Pero menos ransomware no equivale a menos ransomware: el volumen total de 2022 sigue eclipsando fácilmente los totales de 2018, 2019 y 2020, y asciende a más intentos de ransomware que 2019 y 2020 juntos.

Preocupante, el ransomware comenzó a aumentar de nuevo a finales de 2022, con el volumen de ataques del cuarto trimestre alcanzando los 154,9 millones, el más alto desde el tercer trimestre de 2021.

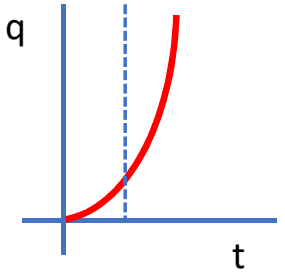
A pesar de la disminución global de 2022, no todas las regiones experimentaron una caída: el ransomware en Europa se disparó un 83%, incluyendo un aumento del 112% en el Reino Unido.

Las industrias de educación y finanzas también fueron fuertemente atacadas, con aumentos del 275% y 41% respectivamente.

Amenazas Provenientes de Malware

- **Man in the middle:** leer, insertar y modificar los mensajes entre dos partes
- **Pharming:** suplantar las direcciones DNS que usa el usuario para que visite páginas sustitutas
- **Fuerza Bruta:** prueba de todas las combinaciones posibles
- **Xploits:** programa que trata de sacar provecho de deficiencias o vulnerabilidades de otros programas
- **Spoofing:** técnica de suplantación de identidad (IP, DNS, web, mail)
- **Phishing:** suplantar la imagen de una empresa para obtener datos de la víctima

Comportamiento del phishing desde el inicio de las operaciones inmediatas en los bancos.

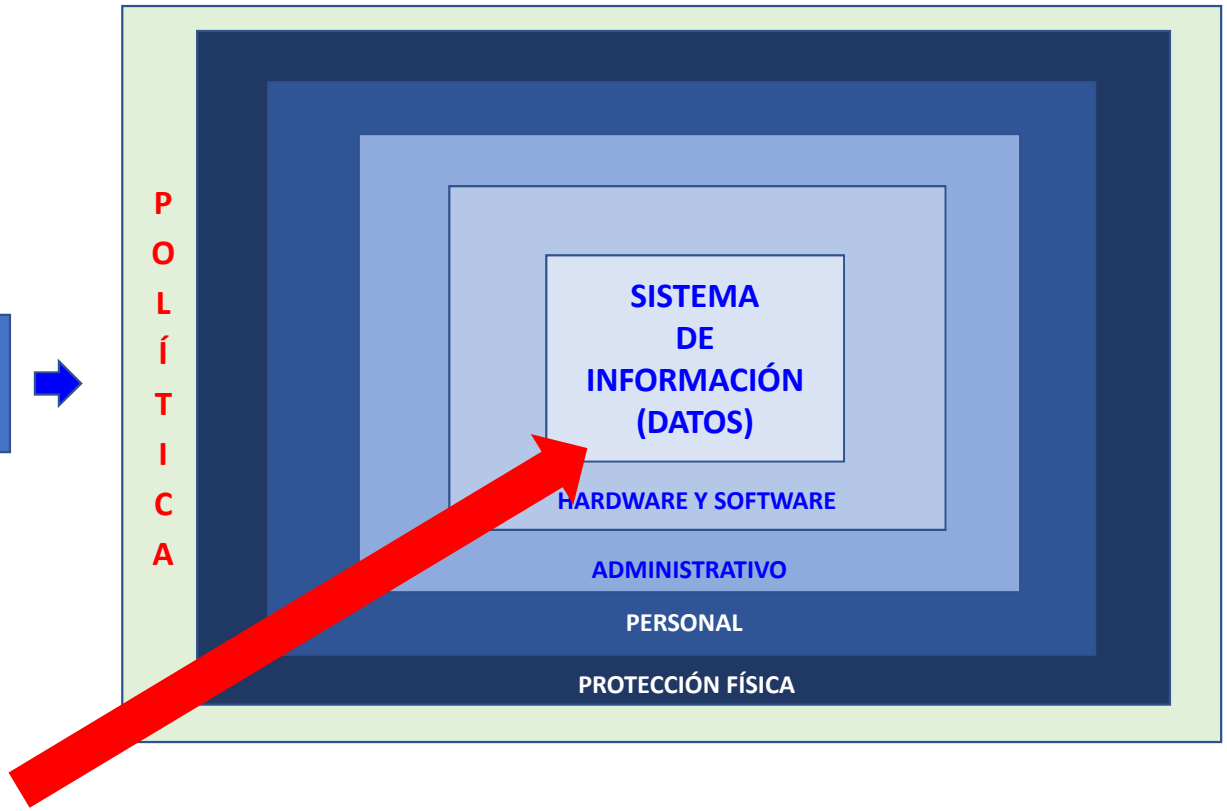


Amenazas Provenientes de accidentes, siniestros, catástrofes.

- **Accidentes**
  - Café derramado, tropiezo, …
- **Siniestros**
  - Incendio, inundación, …
- **Catástrofes**
  - Terremoto

Estrategia de Seguridad

PROTECCIÓN POR CAPAS COMPLEMENTARIAS



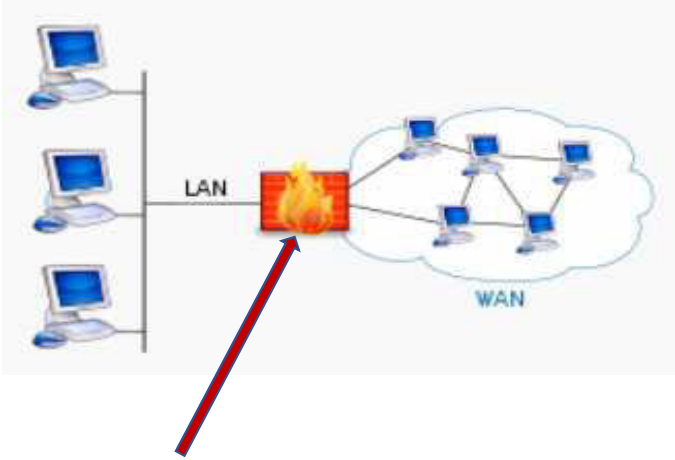
Estrategia en profundidad

Estrategia militar cuyo objetivo es hacer que el atacante pierda el empuje inicial debiendo superar varias barreras en vez de una

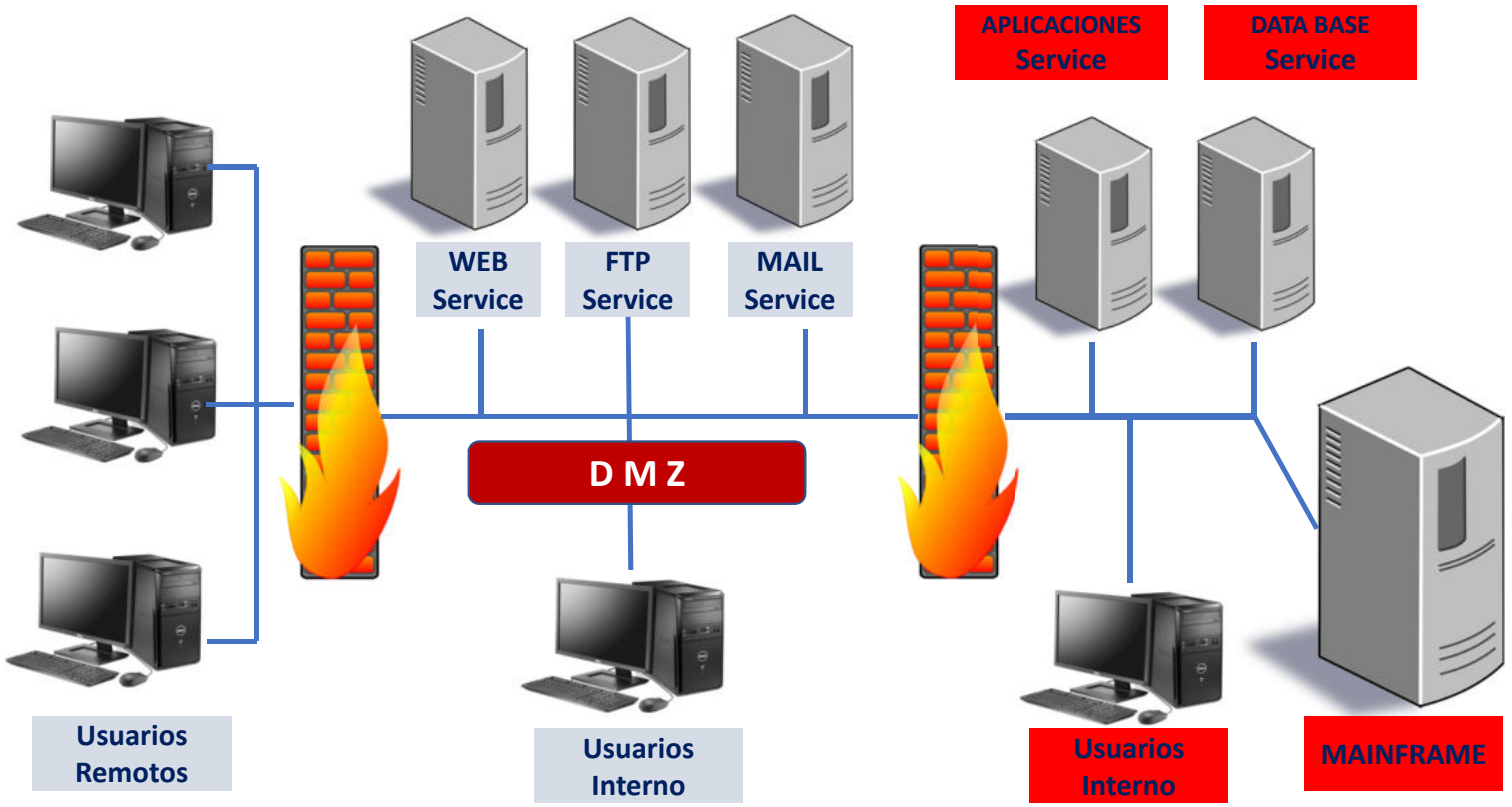
Herramientas de Seguridad – Perímetro -

Firewall

- Parte de un sistema o una red diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas
- Uno o más dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos



Herramientas de Seguridad – Perímetro -



Herramientas de Seguridad – Perímetro -

Pruebas de Penetración

Ataques del entorno

- ¿Qué grado de confianza posee la aplicación en su entorno local y en los recursos remotos?
- ¿Coloca la aplicación información confidencial en un recurso que pueda leerse por otras aplicaciones?
- ¿Confía en cada uno de los archivos o bibliotecas que carga sin comprobar el contenido?
- ¿Puede un atacante aprovechar esta confianza para obligar a la aplicación a hacer lo que éste desee?

Ataques de entrada

- ¿Se permiten las entradas consideradas seguras y se evitan las no seguras (por ejemplo, cadenas largas, paquetes formados incorrectamente, etc.)?

Ataques de datos y de lógica

- Cuentas de usuario "soldadas" en el código
- Bypass
- Información mostrada en mensajes de error
- Acceso a funcionalidad por rutas no seguras

Prevenciones

SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

- Programa usado para detectar **accesos no autorizados** a una computadora o a una red
- Detecta, gracias a sensores virtuales (sniffers), anomalías que pueden ser indicio de la presencia de ataques
- Combinado con un firewall, puede reprogramarlo para bloquear el tráfico proveniente de la red del atacante

SISTEMAS DE PREVENCIÓN DE INTRUSOS (IPS)

- Dispositivo que ejerce el control de acceso en una red
- Toma decisiones de **control de acceso basados en los contenidos del tráfico,** en vez de direcciones IP o puertos

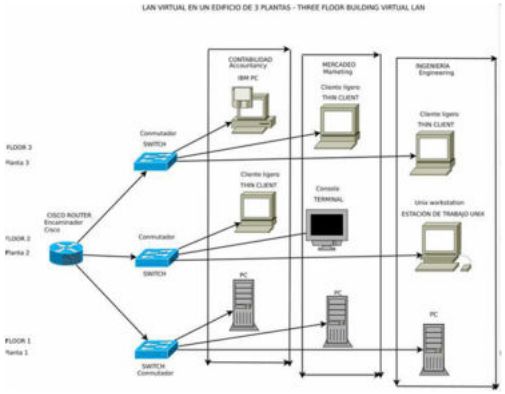
Herramientas de Seguridad Redes

–VPN- Red Privada Virtual.

- Tecnología de red que permite montar una red local (virtual) sobre una red pública o no controlada
- Para ello:
  - Autenticación (usuario, equipo y nivel de acceso)
  - Confidencialidad (cifrado)
  - Integridad (hash, digesto, firma)
  - No repudio (firma)
- Protocolos
  - IPSEC, PPTP, SSL/TLS, SSH

VLAN (virtual LAN)

- Método que permite crear redes lógicamente independientes dentro de una misma red física



ACL (access control list)

- Lista de reglas que detallan puertos de servicio o nombres de dominios que están disponibles en una terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio

Herramientas de Seguridad

HOST.

- Anti-malware
  - Anti virus, anti-spyware
- Control de Acceso
- Autenticación
- Actualización de sistemas operativos y navegadores
- Firewall
- Cuentas de usuario con privilegios limitados
- Limitar y controlar el uso de medios extraíbles

APLICACIONES

- Control de Acceso
- Autenticación
- Perfiles / roles / privilegios
- Pruebas

DATOS

CRIPTOGRAFÍA

- Técnicas que alteran las representaciones de mensajes para hacerlos ininteligibles a usuarios no autorizados

DATA LEAK PREVENTION (DLP)

- Mecanismos que intentan evitar que se filtre información confidencial

Protección: Políticas de Seguridad Integrales

Algunas medidas a modo de ejemplo:

- Establecer políticas de seguridad
- Respaldar la información
- Cifrar las comunicaciones
- Utilizar antivirus.
- Proteger todos los equipos conectados a la red.
- Adquirir herramientas de seguridad.

* Las medidas deben aplicarse en el marco de algún estándar de seguridad integral, por ejemplo: COSO, Series ISO 27.000, ITIL, COBIT, MAGERIT o los dispuestos por normas, por ejemplo circulares de BCRA.

Normas Generales de Control Interno para Tecnologías de Información –SIGEN -

NORMAS DE CONTROL INTERNO PARA TECNOLOGÍAS DE LA INFORMACIÓN 2021

IF-2021-106082452-APN-SNI#SIGEN

- ESTRUCTURA
- ASPECTOS RELEVANTES DE SU CONTENIDO

https://www.argentina.gob.ar/sites/default/files/2022/02/anexo_if-2021-106082452-apn-snisigen.pdf

Normas Generales de Control Interno para Tecnologías de Información –SIGEN -

ESTRUCTURA

1. Organización informática
2. Plan estratégico de TI
3. Arquitectura de la información
4. Políticas de seguridad y procedimientos de gestión de la TI
5. Cumplimiento de regulaciones externas
6. Administración de proyectos
7. Desarrollo, mantenimiento o adquisición de software de aplicación
8. Adquisición y mantenimiento de la infraestructura tecnológica
9. Servicios de procesamiento, soporte y/o almacenamiento prestado por terceros.
10. Publicación de información digital.
11. Monitoreo de activades de TI.
12. Auditoría interna de sistemas.

Protección: Políticas de Seguridad Integrales

Veamos un ejemplo: ISO 27002

Anexo DN N° 641/2021 !!!

14 Dominios

35 Objetivos de Control

114 Controles

NORMA

Rol del auditor con respecto a la seguridad de TI.

- El compromiso por la seguridad de TI le compete al «Responsable», el auditor sólo la evalúa en relación al tipo de encargo.
- Particularmente con respecto a la seguridad el auditor determinará si:

  - Existe un plan formal de seguridad
  - El plan ataca todos los riesgos identificados
  - El personal está informado del plan y de sus responsabilidades de seguridad
  - El personal clave ha sido entrenado
  - El plan esta actualizado
  - El plan está siendo cumplido
- En función a esta preevaluación definirá la estrategia y luego el programa de auditoría.

INTOSAI – Organización Internacional de las Entidades Fiscalizadoras Superiores

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

Análisis de los aspectos más relevantes

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

FASES

Análisis de riesgos: se realiza un **inventario** de todos los sistemas de información

Gestión del riesgo: consiste en seleccionar los controles y las medidas de seguridad que reducen la exposición de la organización al riesgo a **un nivel aceptable.**

Se hace hincapié en el **uso del sentido común** para equilibrar siempre el **coste de la seguridad** que debe incorporarse a un sistema con el **valor de la información** que soporta dicho sistema

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

PLANIFICACIÓN

- **Conocimiento del cliente y del entorno;**
- **Alcance de la revisión: ¿Qué sistemas de información, qué límites lógicos, físicos o geográficos?**
- **Recursos disponibles: Personal cualificado o consultores, presupuestos, plazos;**
- **Disponibilidad de estadísticas fiables sobre amenazas y cifras de costes, adecuadas a las condiciones locales; adaptación de los valores por defecto, en caso necesario;**
- **Requisitos del informe: Usuarios del informe, contexto de la revisión (Informe anual, informe especial, interno, externo, etc.), tipo de recomendaciones necesarias;**
- **Método de revisión: Enfoque descendente, análisis detallado o una combinación de ambos. Conocimiento del cliente y del entorno;**

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

- La norma plantea un método sencillo, **método descendente**, que se basa en:
  - evaluaciones cualitativas del **riesgo de que se produzcan amenazas,** y
  - el **grado de su impacto** si se producen.
- Las **amenazas** y los posibles **impactos** se evalúan primero individualmente y luego globalmente para determinar un **grado global de exposición al riesgo.**
- Estas evaluaciones son subjetivas y suelen expresarse en términos de riesgo, impacto y exposición altos, medios o bajos. **Una matriz**

- A partir de estas evaluaciones, se formulan **recomendaciones a la dirección** sobre la línea de actuación que debe seguirse o sobre el tipo de controles y medidas de seguridad específicos que deben establecerse.

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

Proceso de evaluación de la seguridad de la información:

- Evolución de la información
- Gestión de seguridad
- Equipo de seguridad
- Proceso
  - Declaración de sensibilidad
  - Evaluación del impacto empresarial
  - Evaluación de amenazas y riesgos
  - Clasificación de la exposición
- Decisiones de seguridad

▪La protección de la seguridad debe ser coherente con el valor de la información que se protege;
▪La protección de la seguridad debe permanecer con la información en todo momento mientras se traslada o procesa.
▪La protección de la seguridad debe ser continua en todas las situaciones.

▪La alta dirección debe comprometerse plenamente. Actualización!!!

▪Clasificación de acuerdo a la sensibilidad.

▪Efectos: Divulgación, amenazas, interrupción.

▪Determinar posibilidad de ocurrencia.

▪Evaluar el impacto. Exposición global

▪Minimizar riesgos identificados.

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

Declaración de sensibilidad, clasificación de seguridad:

- **Propiedad de las aplicaciones.**
  - ▪Inventario, identificación. (INTEGRIDAD)
  - ▪Las aplicaciones SON PROPIEDAD de un grupo de individuos
  - ▪Poca interacción entre operaciones > facilidad para identificarlos.
  - ▪Alta interacción > dificultad para identificarlos. **"Límite artificial"**

  → **Control de cambios**

- **Evaluación de la sensibilidad por parte del propietario.**
  - ▪El propietario evalúa la sensibilidad:
    - ▪Disponibilidad, integridad y confidencialidad
    - ▪Costos de sustitución y oportunidad
    - ▪Clasificación.

  → **Plan de continuidad**

- **Declaración de sensibilidad.**
  - ▪Documentación formal.

- **Descripción resumida de los sistemas.**
  - ▪Proporciona a la dirección una visión general de los sistemas bajo su responsabilidad y del valor de la información que transportan.

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

Evaluación del impacto empresarial y de las amenazas:

- **Amenazas**
  - Lo que puede ocurrir….
    - INTOSSAI: 80 % INTERNO (Insiders), 24% descuidos, 26% capacitación, 30 % EMPLEADOS DESHONESTOS.
- **Probabilidad de ocurrencia**
  - La probabilidad se mide para cada sistema
- **Evaluación del impacto empresarial.**
  - si la información se divulga,
  - su integridad se ve comprometida, o
  - hay una interrupción de los servicios
  - La evaluación tiene un componente de subjetividad.
  - Impacto global.
  - Aprobación por el responsable
- **Clasificación de la exposición a la seguridad**
  - Es el resultado de combinar el índice global de riesgo o probabilidad de amenaza (alto, medio, bajo) con el índice global de impacto en el negocio (muy grave, grave o menos grave). → **Matriz**

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

Resumen de la evaluación:

- **Visión**
  - ▪Proporciona una visión general de la seguridad de las aplicaciones en uso.
- **Obsolescencia**
  - ▪Naturaleza cambiante de las TI.
  - ▪La revisión pone de manifiesto políticas obsoletas.
- **Conocimiento**
  - ▪Todas las deficiencias graves de las políticas se ponen en conocimiento de la alta dirección en el informe final, junto con otras recomendaciones
- **Estrategias de seguridad**
  - ▪Es úitil y NECESARIO para establecer planes de seguridad a largo plazo.

ISSAI 5310 – Metodología para la revisión de seguridad de un sistema de información.

Decisión de seguridad y acción recomendada:

Decisión de seguridad → **Acción de gestión recomendada**

Tasa de exposición	Decisión de seguridad	Acción recomendad
ALTA (9,8,7)	Controlar el riesgo	Aplicar políticas y medidas adicionales. (normas, procedimientos, herramientas)
MEDIA (6,5,4)	Controlar el riesgo Evitar el riesgo	Aplicar políticas y medidas adicionales. Cambiar/mejorar los procedimientos operativos.
BAJA (3,2,1)	Evitar el riesgo Limitar el riesgo Aceptar el riesgo	Cambiar/mejorar los procedimientos alternativos Obtener cobertura de seguros Ningún cambio

Metodología para la revisión de seguridad de un sistema de información.

Check list

Procedimiento indagatorio →

EVIDENCIAS DIGITALES - BREVE ANÁLISIS.

- **Conceptual,**
- **Soporte documental,**
- **Ciclo de vida y oponibilidad.**

https://www.youtube.com/watch?v=xX6klWu1wDA&t=35s

a) Análisis conceptual

Propuesta de norma de auditoría 500 (Revisada) IAASB – Definición en consulta.

Evidencia de auditoría - Información, a la que se han aplicado procedimientos de auditoría, que el auditor utiliza para extraer conclusiones que constituyen la base de la opinión y el informe del auditor.

Resolución N° 152/2002

Evidencias:

- **FÍSICAS**
- **TESTIMONIALES**
- **ANALÍTICAS**

DOCUMENTALES:

"…INFORMACIÓN CONTENIDA EN REGISTROS, ACTUACIONES, CARTAS, CONTRATOS, FACTURAS, INFORMES, EXPEDIENTES, ETC"

INFORMÁTICAS

"…LAS CONTENIDAS EN SOPORTES ELECTRÓNICOS, INFORMÁTICOS Y TELEMÁTICOS, , ASÍ COMO ELEMENTOS LÓGICOS, PROGRAMAS Y APLICACIONES UTILIZADAS POR EL AUDITOR"

Las «evidencias digitales» son en este contexto:

Elementos de juicio generados, almacenados o transmitidos por medios digitales,
entendiéndose por digital ***"…un dispositivo o sistema que crea, presenta, transporta o almacena información mediante la combinación de bits***

Constituyen la representación digital –intangible- ***de hechos, transacciones, relaciones, procesos, criterios, que se obtienen de bases de datos y todo tipo de documentos, tanto en formato numérico como de texto, imágenes, sonidos, videos, comunicaciones digitales u otros.***

Los procesos mediante los cuales la información se genera

⬆ ⬆ ⬆

Tecnología subyacente

Para tener en cuenta:

- La evolución de las evidencias *tradicionales* al formato digital no significa que modifiquen su fin principal.
- Mantienen los requisitos de **legitimidad[1], relevancia, validez y suficiencia.**

Simplemente…. Tienen distintas características por su intangibilidad:

- **MODIFICABLES:** La premisa que un registro electrónico es modificable determina su condición de volatilidad. **Impacta en la subsistencia de la fuente que queda en poder de terceros.**
- **ILEGIBLES:** Se requieren medios adecuados de acceso
- **PERDURABLES:** Están sujetos a **riesgos propios, distintos que el soporte papel** por ejemplo deterioro específico de los soportes y obsolescencia.
- **SENSIBLES:** **La fiabilidad de las evidencias digitales depende de la sofisticación de los sistemas, la tecnología subyacente y los controles de TI**

b) Soporte documental.

Evidencias digitales de acuerdo a su origen

Res. N° 152/2002.

- *# 8 El auditor debe realizar una planificación ordenada, sistemática y documentada de su labor.*
- *# 11 La tarea efectuada por el auditor debe documentarse en papeles de trabajo, de forma tal que permita respaldar las conclusiones y demás resultados de su labor*

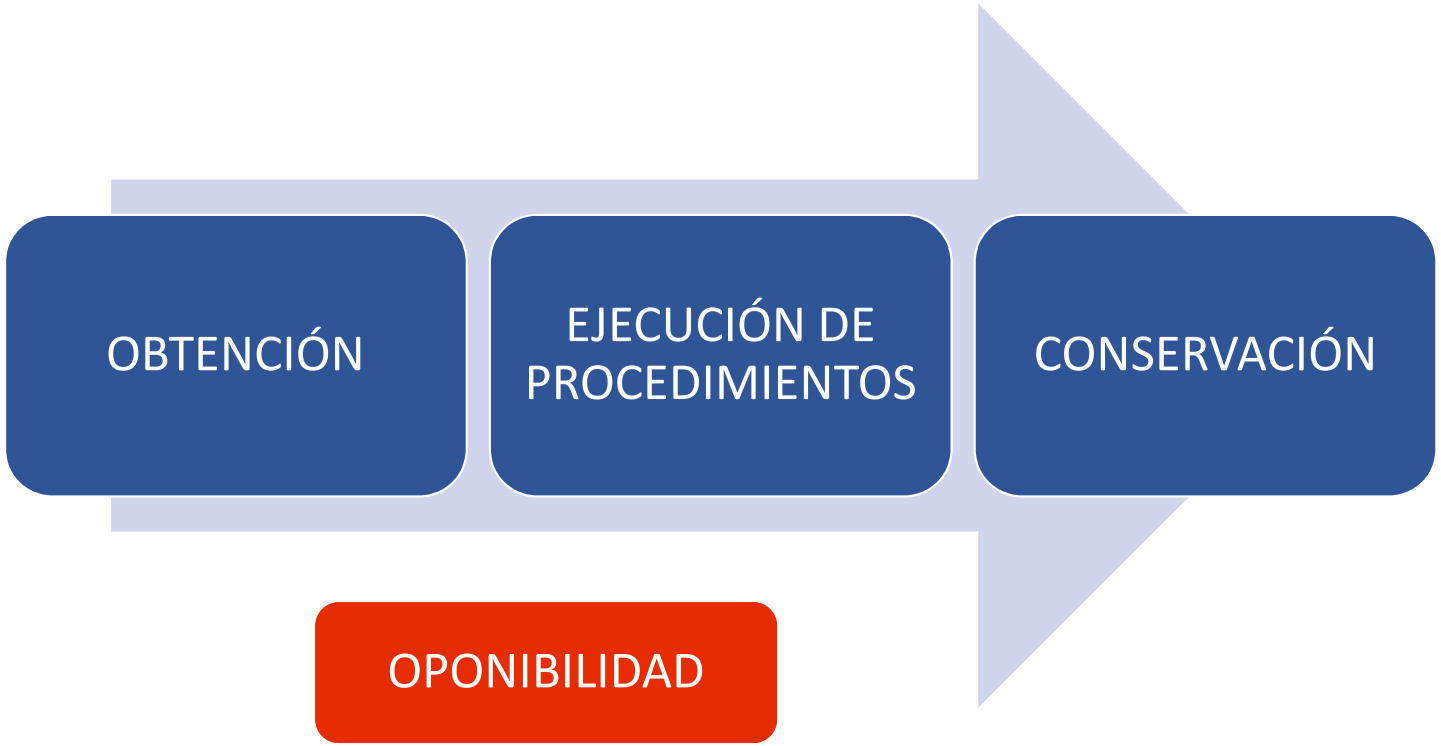
Res. N° 206/2023 (Res. N° 300/2022)

Evidencias según su soporte	
Soporte de origen	Transferido o conservado en
DIGITAL	DIGITAL
DIGITAL	PAPEL
PAPEL	DIGITAL

Los requisitos y métodos para su legitimación varían sustancialmente

Precauciones por la *oponibilidad*

c) Ciclo de vida de las evidencias digitales



OBTENCIÓN

¿Qué compone la evidencia digital y que se debe relevar?

- Los procesos mediante los cuales la información se genera
- La información correspondiente a la auditoría

¿Cuáles son los controles de TI que deben ser evaluados?

- Controles generales
- Controles de aplicación

¿Cuál es el alcance de la información a obtener?

- Relevancia
- Fiabilidad

¿Cómo se obtiene la evidencia?

- Formato en que están disponibles los datos
- Garantía de legitimidad y exactitud
- Posibilidad de repetir la prueba
- Preservación

Riesgos – DIGITALES –

EJECUCIÓN DE PROCEDIMIEN-TOS

La alteración de los datos de origen puede generar:

- Dificultades al momento de utilizarlos…
- Riesgo de conclusiones erróneas
- Invalidez de la oponibilidad

Algunos *Tips* (por si no dispone de una aplicación):

- **Nunca** operar sobre el archivo original. Crear carpeta de acceso restringido Resguardar
- Definir un diseño adecuado de resguardo de los documentos de trabajo
- Tener en cuenta que se trata de «toda» la documentación
- Aplicar el principio de saber-hacer

Riesgos – DIGITALES – **RESOL-2023-206-APN-SIGEN** → **Art. 12: Red de Trabajo o Disco Compartido**

CONSERVACIÓN

Riesgo de borrado, destrucción o acceso indebido. LDP-LDC –ANEXO B

- **Mala praxis**
- **Acceso indebido.**

Políticas Operación y acceso

Riesgo de inaccesibilidad. ANEXO B (7 Actualización) – ANEXO C. Back.

- **Obsolescencia técnica.**
- **Deterioro físico de los soportes.**
- **Resguardo en la nube.**

Backup

¿SON OPONIBLES?

Sí, tan oponibles como las evidencias «físicas», pero teniendo en cuenta su naturaleza digital.

OPONIBILIDAD

Garantizar que la información obtenida es copia legítima y exacta de la obrante en base del responsable.

Tipos según origen/resguardo: digital/digital - física/digital - digital/física.

Cadena de custodia.

Preguntas

carlosrumitti@yahoo.com.ar
carlosrumitti@gmail.com