# Seguridad y Auditoría Informática

## Auditoría de Seguridad

# Objetivos

- Comprender las implicancias de la Auditoría de Seguridad
- Diferenciar entre componentes Auditoría de Seguridad Física y Lógica
- Conocer las Consideraciones de Seguridad a incluir en el Informe de Auditoría
- Identificar las Vulnerabilidades más comunes en Redes
- Diferenciar entre elementos de Auditoría de Redes Física y Lógica

# Auditoría de Seguridad (1/2)

Debe evaluarse en la auditoría si los **modelos de seguridad** están en consonancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones.

Los grandes grupos de controles, que además de poderlos dividir en **manuales** y **automáticos**, o en **generales** y de **aplicación**, son los siguientes:

- Controles **directivos**
- Controles **preventivos**
- Controles **detectivos**
- Controles **correctivos**
- Controles **de recuperación**

# Auditoría de Seguridad (2/2)

El **sistema de control interno** debe basarse en políticas, y se implementa con apoyo de herramientas. Cuando existe un sistema de control interno adecuado, los procesos de auditoría, especialmente si son periódicos, son revisiones necesarias pero más rápidas, con informes más breves.

# Evaluación de Riesgos (1/4)

Se trata de identificar y cuantificar la **probabilidad e impacto** de los riesgos y analizar medidas que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

Para evaluarlos hay que considerar:

- El tipo de información almacenada, procesada y transmitida.
- La criticidad de las aplicaciones.
- La tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

Es necesario revisar si se han considerado las **amenazas** y, además, errores y negligencias en general que pueden traducirse en daños, en algunos casos irreversibles.

# Evaluación de Riesgos (2/4)

Es necesario evaluar las vulnerabilidades que existen, ya que la cadena de protección se podrá romper con mayor probabilidad por los eslabones más débiles.

El **factor humano** es el principal a considerar, salvo en algunas situaciones de protección física muy automatizados.

Es conveniente que haya cláusulas adecuadas en los contratos, sean de trabajo o de otro tipo, especialmente para quienes están en funciones más críticas.

Es necesaria una separación de funciones.

# Evaluación de Riesgos (3/4)

Además de reducirse, se pueden **transferir los riesgos** contratando seguros.

Otra posibilidad es **asumir los riesgos**.

En la auditoría externa se trata de saber si la entidad ha **evaluado de forma adecuada** los riesgos, si los informes han llegado a los destinatarios correspondientes y si se están tomando las medidas pertinentes, así como si el proceso se realiza con la frecuencia necesaria y no ha constituido un hecho aislado.

En estos casos se debe considerar la **metodología** que se sigue para evaluar los riesgos más que las **herramientas**, si se han considerado todos los riesgos y si se han medido bien.

# Evaluación de Riesgos (4/4)

Es necesaria la designación de **propietarios** de los activos.

Al hablar de seguridad siempre se habla de sus tres dimensiones clásicas y los controles buscan garantizar alguna de estas características:

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- Debe además existir **Autenticidad**

# Fases de la Auditoría de Seguridad

- Definición de los objetivos, alcance y profundidad de la auditoría.
- Análisis de posibles fuentes y recopilación de información.
- Determinación del plan de trabajo y comunicación a la entidad.
- Adaptación de cuestionarios y consideración de herramientas o perfiles de especialistas necesarios, sobre todo en la auditoría externa.
- Realización de entrevistas y pruebas.
- Análisis de resultados y valoración de riesgos.
- Presentación y discusión del informe provisional.
- Informe definitivo.

# Auditoría de la Seguridad Física (1/3)

Se evaluarán las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y personas.

Las **amenazas** pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, etc.

Desde la perspectiva de las **protecciones físicas** algunos aspectos a considerar son:

- Ubicación del centro de datos, servidores locales y cualquier elemento a proteger.
- Protección de computadoras portátiles, incluso fuera de las oficinas: aeropuertos, automóviles, restaurantes, etc.

# Auditoría de la Seguridad Física (2/3)

- Estructura, diseño, construcción y distribución de los edificios y de sus plantas.
- Riesgos a los que están expuestos por agentes externos como por accesos físicos no controlados.
- Amenazas de fuego; riesgos por agua; por accidentes atmosféricos o por averías en las conducciones; problemas en el suministro eléctrico, tanto por caídas como por perturbaciones.
- Controles tanto preventivos como de detección relacionados con los puntos anteriores.
- Además debe controlarse el contenido de carteras, paquetes, bolsos o cajas, ya que podrían contener explosivos, así como lo que se quiere sacar del edificio, para evitar sustituciones o sustracción de equipos, componentes, soportes magnéticos, documentación u otros activos.

# Auditoría de la Seguridad Física (3/3)

- Protección de soportes magnéticos (acceso, almacenamiento y posible transporte).
- Protección de documentos impresos y de cualquier tipo de documentación clasificada.
- Todos los puntos anteriores pueden estar además cubiertos por seguros.

# Auditoría de la Seguridad Lógica (1/4)

Es necesario verificar que cada usuario sólo pueda acceder a los recursos a los que le autorice el propietario según su función, y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución, etc. lo que representaríamos en una **matriz de accesos** en la que figurarían los **sujetos**, los **objetos** que puedan ser accedidos con mayor o menor **granularidad** y las **posibilidades que se le otorgan**.

Desde el punto de vista de la auditoría es necesario revisar cómo se identifican y sobre todo autentican los usuarios, cómo han sido autorizados y por quién, y qué ocurre cuando se producen transgresiones o intentos: quién se entera, cuándo y qué se hace.

# Auditoría de la Seguridad Lógica (2/4)

En cuanto a autenticación el método más usado es la **contraseña**, cuyas características serán acordes con las normas y estándares de la entidad.

# Auditoría de la Seguridad Lógica (3/4)

Algunos de los aspectos a evaluar respecto a las **contraseñas** pueden ser:

- Quién asigna la contraseña.
- Longitud mínima y composición de caracteres.
- Vigencia.
- Control para no asignar las “x” últimas (Historial).
- Número de intentos fallidos que se permiten al usuario.
- Si las contraseñas están cifradas, y bajo qué sistema.
- Protección o cambio de contraseñas iniciales que llegan en los sistemas, y que a menudo aparecen en los propios manuales.

# Auditoría de la Seguridad Lógica (4/4)

- Controles existentes para evitar y detectar Troyanos.
- La no-cesión, y el uso individual y responsable de cada usuario, a partir de la normativa.
- Promover el uso de diferentes contraseñas para diferentes sistemas.
- La solución más adecuada por ahora puede consistir en utilizar **sistemas de identificación únicos (single sign-on)**.
- Verificar que el proceso de altas, variaciones y bajas de usuarios se realiza según la normativa en vigor. Debería estar previsto bloquear a un usuario que no accediera por un período determinado.
- Examinar **situaciones de bloqueo** por la existencia de un sólo administrador.

# Técnicas, Métodos y Herramientas

- En cada proceso de auditoría, se fijan los objetivos, ámbito y profundidad, lo que sirve para la planificación y para la consideración de las fuentes, según los objetivos, así como de las técnicas, métodos y herramientas más adecuados.

- Como métodos y técnicas podemos considerar los cuestionarios, las entrevistas, la observación, los muestreos, las CAAT (Técnicas de Auditoría Asistidas por Computadora), las utilidades y programas, los paquetes específicos, las pruebas y la simulación en paralelo con datos reales.

# Consideraciones Respecto al Informe (1/5)

- Se harán constar los antecedentes y los objetivos, qué metodología de evaluación de riesgos y estándares se ha utilizado, y una breve descripción de los entornos revisados.

- Debe incluirse un resumen **para la Dirección** en términos no técnicos.

- Dependiendo de los casos, será preferible agrupar aspectos similares: **seguridad física**, **seguridad lógica,** etc., o bien clasificar los puntos por centros o redes.

- En **cada punto** que se incluya debe explicarse por qué es un incumplimiento o una debilidad, así como alguna recomendación, a veces abarcando varios puntos.

# Consideraciones Respecto al Informe (2/5)

- El informe debe ser necesariamente revisado por los auditados, así como discutido si es necesario antes de emitir el definitivo.

- En muchos casos se recogen las respuestas de los auditados, sobre todo cuando la auditoría es interna.

- La entidad decide qué acciones tomar a partir del informe, y en el caso de los auditores internos éstos suelen hacer también un seguimiento de las implementaciones.

- En algunos casos los informes se han usado para comparar la seguridad de diferentes delegaciones, sucursales, o empresas de un mismo grupo, o bien filiales de una multinacional, pero si los entornos no son homogéneos las comparaciones pueden no ser útiles y llegar a distorsionar.

# Consideraciones Respecto al Informe (3/5)

- Es necesario diferenciar puntos muy graves, graves, memorables, u otra clasificación, en definitiva establecer algunas **métricas de seguridad** y clasificar los puntos según su importancia y prioridad.

- **Es importante que se delimiten las responsabilidades y los entregables** que son objeto de auditoría externa en el contrato o propuesta.

# Consideraciones Respecto al Informe (4/5)

- **Algunos de los puntos importantes** que pueden llegar a estar en los informes respecto a seguridad pueden ser la ausencia de:
  - Copias de activos críticos en cuanto a la continuidad, en lugar diferente y distante.
  - Cumplimiento de la legislación aplicable así como de las políticas y normas internas.
  - Diferenciación de entornos de desarrollo y producción.
  - Involucramiento de la Alta Dirección.
  - Motivación de los empleados y directivos en relación con la seguridad.
  - Evaluación periódica y adecuada de riesgos.
  - Segregación de funciones.

# Consideraciones Respecto al Informe (5/5)

- Es frecuente también que quienes han pedido la auditoría quieran conocer después en qué medida se han resuelto los problemas, conocer la **evolución de la situación** en el tiempo.

# Contratación de Auditoría Externa

- Si no se sigue un proceso de selección adecuado de auditores externos, no se pueden garantizar los resultados.
- Algunas consideraciones pueden ser:
  - La entidad auditora debe ser **independiente** de la auditada en el caso de una auditoría externa.
  - Las personas que vayan a realizar el trabajo deben ser independientes y competentes, según el objetivo.
  - La auditoría debe encargarse a un nivel suficiente alto, normalmente Dirección General o Consejero Delegado.
  - Puede ser necesario dar o mostrar a los auditores todo lo que necesiten para realizar su trabajo, pero nada más, e incluso lo que se les muestre o a lo que se les permita acceder puede ser con restricciones.

# Fundamentos de Auditoría de Redes

# Vulnerabilidades en Redes (1/4)

En las redes de comunicaciones, por causas propias de la tecnología, pueden producirse básicamente tres tipos de incidencias:

- **Alteración de bits**. Una trama puede sufrir variación en parte de su contenido. Se agrega un sufijo a la trama con un Código de Redundancia Cíclico (CRC) que detecte cualquier error y permita corregir errores que afecten hasta unos pocos bits.

- **Ausencia de tramas**. Alguna trama puede desaparecer en el camino del emisor al receptor. Se suele atajar este riesgo dando un número de secuencia a las tramas.

- **Alteración de secuencia**. El orden en el que se envían y se reciben las tramas no coincide. Unas tramas han adelantado a otras. En el receptor, mediante el número de secuencia, se reconstruye el orden original.

# Vulnerabilidades en Redes (2/4)

Teniendo en cuenta que es físicamente posible interceptar la información, los tres mayores riesgos a atacar son:

- **Indagación**. Un mensaje puede ser leído por un tercero, obteniendo la información que contenga.
- **Suplantación**. Un tercero puede introducir un mensaje adulterado que el receptor cree proveniente del emisor legítimo.
- **Modificación**. Un tercero puede alterar el contenido de un mensaje.

Para este tipo de actuaciones, la única medida prácticamente efectiva en redes MAN y WAN (cuando la información sale del edificio) es la criptografía.

# Vulnerabilidades en Redes (3/4)

El cableado que va desde el armario distribuidor a cada uno de los potenciales puestos, suele llamarse de “**planta**” suele ser de cobre y es propenso a escuchas (“pinchazos”) que pueden no dejar rastro.

El cableado **troncal** (conexión entre armarios y salas de equipos) y el de **ruta** (conexión desde sala de equipos hacia los transportistas de datos) se tienden frecuentemente mediante fibra óptica, que son muy difíciles de interceptar, debido a que no provocan radiación electromagnética y a que la conexión física a una fibra óptica requiere una tecnología delicada y compleja.

# Vulnerabilidades en Redes (4/4)

En el propio **puesto de trabajo** puede haber peligros, como grabar/retransmitir la imagen que se ve en la pantalla, teclados que memorizan el orden en que se han pulsado las teclas, o directamente que las contraseñas estén escritas en papeles a la vista.

Dentro de las **redes locales**, el mayor peligro es que alguien instale una "escucha" no autorizada. Al viajar en texto plano la información dentro de la red local, es imprescindible tener una organización que controle estrictamente los equipos de escucha, bien sean estos físicos ("sniffers") o lógicos ("traceadores").

# Auditando la Red Física (1/2)

- Deben comprobarse que efectivamente los accesos físicos provenientes del exterior han sido debidamente registrados y que desde el interior del edificio no se intercepta físicamente el cableado (“pinchazo”).

- En caso de desastre, debe comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y qué operatividad puede soportar.

- Como objetivos de control, se debe marcar la existencia de:

  - Áreas controladas para los equipos de comunicaciones.

  - Protección y tendido adecuado de cables y líneas de comunicaciones.

# Auditando la Red Física (2/2)

- Controles de utilización de los equipos de pruebas de comunicaciones, usados para monitorear la red y su tráfico.

- Atención específica a la recuperación de los sistemas de comunicación de datos en el plan de recuperación de desastres en sistemas de información.

- Controles específicos en caso de que se utilicen líneas telefónicas normales con acceso a la red de datos para prevenir accesos no autorizados al sistema o a la red.

# Auditando la Red Lógica (1/2)

- Se debe controlar que un equipo no pueda enviar indiscriminadamente mensajes ya que puede bloquear la red completa.

- Es necesario monitorear la red, revisar los errores o situaciones anómalas que se producen y tener establecidos los procedimientos para detectar y aislar equipos en situación anómala. Una solución totalmente efectiva es el cifrado de las comunicaciones.

- Como objetivos de control, se debe marcar la existencia de:

    - Contraseñas y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado a la red de comunicaciones.

# Auditando la Red Lógica (2/2)

- Facilidades para detectar errores de transmisión y establecer las retransmisiones apropiadas.
- Controles para asegurar que las transmisiones van solamente a usuarios autorizados.
- Registro de la actividad de la red.
- Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.
- Controles adecuados que cubran la importación o exportación de datos a otros sistemas informáticos.

# ¿Preguntas?

# ¡Muchas Gracias!