
# Seguridad y Auditoría Informática

## Auditoría Informática

Ing. Alfredo Pardo

Año 2021

# Tabla de Contenidos

# Auditoría de Seguridad y Redes

## Auditoría De Seguridad

Puede haber Seguridad sin Auditoría, puede existir auditoría de otras áreas, y queda un espacio de encuentro: la auditoría de la seguridad.

Si no existen suficientes y adecuadas medidas de protección se puede perder información vital, o al menos no estar disponible en el momento requerido, las decisiones tomadas pueden ser erróneas, o se pueden incumplir contratos e incluso la propia legislación, lo que puede traducirse en grandes multas en el caso de infracciones graves, o lo que es aún peor, la inmovilización de los archivos.

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 son los siguientes, además de poderlos dividir en manuales y automáticos, o en generales y de aplicación:

- Controles **directivos**, que son los que establecen las bases, como las políticas, o la creación de comités relacionados o de funciones.
- Controles **preventivos**, antes del hecho, como la identificación de visitas (seguridad física) o las contraseñas (seguridad lógica).
- Controles de **detección**, como determinadas revisiones de accesos producidos o la detección de incendios.
- Controles **correctivos**, para rectificar errores, negligencias o acciones intencionadas, como la recuperación de un archivo dañado a partir de una copia.
- Controles **de recuperación**, que facilitan la vuelta a la normalidad después de accidentes o contingencias, como puede ser un plan de continuidad adecuado.

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

Se trata de identificar los riesgos, cuantificar su **probabilidad e impacto**, y analizar medidas que los eliminen (lo que generalmente no es posible) o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

Para evaluar los riesgos hay que considerar, entre otros factores, 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. El problema es la adaptación de los puntos a cada caso y asignar el **peso** que puede tener cada uno de los puntos.

Desde la perspectiva de la auditoría de la seguridad es necesario revisar si se han considerado las **amenazas**, o bien evaluarlas si es el objetivo, y de otro tipo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a: personas, datos, programas, redes, instalaciones, u otros activos, y llegar a suponer un peor servicio a usuarios internos y externos, imagen degradada u otros difícilmente cuantificables, e incluso pérdida irreversible de datos, y hasta el fin de la actividad de la entidad en los casos más graves.

Es necesario evaluar las vulnerabilidades que existen, ya que la cadena de protección se podrá romper con mayor probabilidad por los eslabones más débiles, que serán los que preferentemente intentarán usar quienes quieran acceder de forma no autorizada.

El **factor humano** es el principal a considerar, salvo en algunas situaciones de protección física muy automatizados, ya que es muy crítico: si las personas no quieren colaborar de poco sirven los medios y dispositivos aunque sean caros y sofisticados.

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: es peligroso que una misma persona realice una transacción, la autorice, y revise después los resultados, porque podría planificar un fraude o encubrir cualquier anomalía, y sobre todo equivocarse y no detectarse; por ello deben intervenir funciones/personas diferentes y existir controles suficientes.

Además de reducirse, se pueden **transferir los riesgos** contratando seguros, aunque si se pierden los datos la entidad aseguradora abonará el importe estipulado pero la organización seguirá sin recuperar los datos.

Otra posibilidad es **asumir los riesgos**, pero debe hacerse a un nivel adecuado en la entidad, y considerando que puede ser mucho mayor el costo de la inseguridad que el de la seguridad, lo que a veces sólo se sabe cuando ha ocurrido algo.

En la auditoría externa se trata de saber si la entidad, a través de funciones como administración de la seguridad, auditoría interna, u otras 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, aunque sin dejar de analizar éstas, y si se han considerado todos los riesgos y si se han medido bien.

Es necesaria la designación de **propietarios** de los activos, sobre todo de los datos, que son quienes pueden realizar la clasificación y autorizar las reglas de acceso; un buen propietario se interesará por los riesgos que puedan existir, por lo que promoverá o exigirá la realización de auditorías y querrá conocer, en términos no técnicos, la sustancia de los informes.

Al hablar de seguridad siempre se habla de sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información, y algunos controles van más dirigidos a tratar de garantizar alguna de estas características.

La **confidencialidad**: se cumple cuando sólo las personas autorizadas (o también sistemas) pueden conocer los datos o la información correspondiente.

La **integridad**: consiste en que sólo los usuarios autorizados puedan variar (modificar o borrar) los datos. Deben quedar pistas para control posterior y para auditoría.

La **disponibilidad**: se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas.

Debe además existir **autenticidad**: que los datos o información sean auténticos, introducidos o comunicados por usuarios auténticos y con las autorizaciones necesarias.

## Fases de la Auditoría de Seguridad

- Definición de los objetivos y delimitación del alcance y profundidad de la auditoría, así como del período cubierto en su caso, por ejemplo revisión de accesos del último trimestre; si no se especifica, los auditores deberán citar en el informe el período revisado, porque podría aparecer alguna anomalía anterior, incluso de hace mucho tiempo, y llegarse a considerar una debilidad de la auditoría.
- Análisis de posibles fuentes y recopilación de información: en el caso de los internos este proceso puede no existir.
- Determinación del plan de trabajo y de los recursos y plazos en caso necesario, así como de comunicación a la entidad.
- Adaptación de cuestionarios, y a veces 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

Se evaluarán las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y por supuesto habrá que considerar a las personas: que estén protegidas, que existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector.

Las **amenazas** pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores, negligencias, huelgas, epidemias o intoxicaciones.

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

- Ubicación del centro de datos, de los servidores locales, y en general de cualquier elemento a proteger especialmente en zonas de paso, de acceso público, o próximos a ventanas en plantas bajas. Protección de computadoras portátiles, incluso fuera de las oficinas: aeropuertos, automóviles, restaurantes, etc.
- Estructura, diseño, construcción y distribución de los edificios y de sus plantas.
- Riesgos a los que están expuestos, tanto por agentes externos, casuales o no, 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, así como de acceso basándose en la clasificación de áreas según usuarios, incluso según día de la semana y horario.
- Además del acceso en determinados edificios o áreas 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.
- Protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte, además de otras protecciones no físicas, todo bajo un sistema de inventario, así como 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

Es necesario verificar que cada usuario sólo pueda acceder a los recursos a los que le autorice el propietario, aunque sea de forma genérica, según su función, y con las

posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución, etc., trasladando a los sistemas lo que representaríamos en una **matriz de accesos** en la que figurarán los **sujetos**: grupos de usuarios o sistemas, los **objetos** que puedan ser accedidos con mayor o menor **granularidad**: un disco, una aplicación, una base de datos, una librería de programas, un tipo de transacción, un programa, un tipo de campo, etc., y las posibilidades que se le otorgan: lectura, modificación, borrado, ejecución.

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.

En cuanto a autenticación, hasta tanto no se abaraten más y generalicen los sistemas basados en la **biometría**, el método más usado es la contraseña, cuyas características serán acordes con las normas y estándares de la entidad, que podrían contemplar diferencias para según qué sistemas en función de la criticidad de los recursos accedidos.

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

- Quién asigna la contraseña: inicial y sucesivas.
- Longitud mínima y composición de caracteres.
- Vigencia, incluso puede haberlas de un solo uso o dependientes de una función de tiempo.
- Control para no asignar las “x” últimas.
- Número de intentos que se permiten al usuario, e investigación posterior de los fallidos: pueden ser errores del usuario o intentos de implementación.
- Si las contraseñas están cifradas, y bajo qué sistema, y sobre todo que no aparezcan en claro en las pantallas, listados, mensajes de comunicaciones o corrientes de trabajos.
- Protección o cambio de contraseñas iniciales que llegan en los sistemas, y que a menudo aparecen en los propios manuales.
- Controles existentes para evitar y detectar Troyanos: en este contexto se trata de un programa residente en un PC que emulando una terminal simula el contenido de la pantalla que recoge la identificación y contraseña del usuario, graba la contraseña y devuelve control al sistema verdadero después de algún mensaje simulado de error que normalmente no despertará las sospechas del usuario.
- La no-cesión, y el uso individual y responsable de cada usuario, a partir de la normativa.

Siempre se ha dicho que la contraseña debe ser difícilmente imaginable por ajenos y fácilmente recordable por el propio usuario, y este último aspecto se pone en peligro cuando un mismo usuario debe identificarse ante distintos sistemas, para lo que puede asignar una misma contraseña, lo que supone una vulnerabilidad si la protección es desigual, por ser habitual que en pequeños sistemas o aplicaciones aisladas las contraseñas no están cifradas o lo están bajo sistemas más vulnerables; si opta por asignar varias contraseñas puede que necesite anotarlas.

La solución más adecuada por ahora puede consistir en utilizar **Sistemas de Identificación Únicos (Single Sign-on)** que faciliten la administración y el acceso, permitiéndolo o no a según qué usuarios/sistemas/funciones, o bien adoptar cualquier otro tipo de solución que, con garantías suficientes, pueda propagar la contraseña entre sistemas.

En la auditoría debemos verificar que el proceso de altas de usuarios se realiza según la normativa en vigor, y que las autorizaciones requeridas son adecuadas, así como la gestión posterior como variaciones y bajas, y que los usuarios activos siguen vigentes, y si se revisa cuáles son inactivos y por qué, por ejemplo contrastando periódicamente con la base de datos de empleados y contratados. Debería estar previsto bloquear a un usuario que no accediera por un período determinado.

Otra posible debilidad que debe considerarse en la auditoría es si pueden crearse **situaciones de bloqueo** porque sólo exista un administrador, que puede estar ausente de forma no prevista, por ejemplo por haber sufrido un accidente, e impedir la creación de nuevos usuarios en un sistema de administración centralizada y única; en más de una ocasión, según de qué entorno se trate hemos recomendado la existencia de algún usuario no asignado con perfil especial y contraseña protegida que pueda utilizar alguien con autoridad en caso de emergencia: todas sus operaciones deberán quedar registradas para control y auditoría.

## 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. El factor sorpresa puede llegar a ser necesario en las revisiones, según lo que se quiera verificar.

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, la simulación en paralelo con datos reales y programas de auditor o la revisión de programas.

## Consideraciones Respecto al Informe

En él se harán constar los antecedentes y los objetivos, para que quienes lean el informe puedan verificar de que ha habido una comunicación adecuada, así como qué metodología de evaluación de riesgos y estándares se ha utilizado, y una breve descripción de los entornos revisados para que se pueda verificar que se han revisado todas las plataformas y sistemas objeto de la auditoría.

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, especialmente en entidades grandes si existen responsables diferentes: en caso de duda será un punto a comentar previamente con quienes van a recibir el informe, ya que con frecuencia prefieren entregar, a cada uno la parte que más le afecta, así como planificar y controlar área por área o por departamentos la implementación de medidas.

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.

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

En muchos casos, bien en el propio informe o en otro documento, 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.

Los auditados siempre buscan un informe lo más benigno posible, mientras que los auditores nos proponemos llegar a un informe veraz y útil; estos diferentes puntos de vista a veces crean conflictos en el proceso de auditoría y en la discusión del informe.

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.

Con frecuencia quienes han pedido la auditoría, quieren conocer la **calificación respecto a seguridad**, además de disponer de un informe complementario o resumen en términos no técnicos; quieren saber si están aprobados en seguridad, así como los riesgos más destacados.

Es necesario, por tanto, 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, que pueden ser reconsideradas por la Dirección de la entidad a la hora de implementar las medidas, y en algunos casos, se puede llegar a entregar una lista provisional de proyectos de implementación.

En ocasiones, en el caso de la auditoría externa, los clientes que no conocen los límites habituales de la auditoría sobreentienden que una vez finalizada ésta los auditores darán asistencia más propia de consultores, y que incluso llevarán a cabo implementaciones, redactarán normas, o que al menos en los informes especificarán las soluciones, cuando a menudo esto requiere de un estudio que se sale de los límites e incluso de la independencia

propios de la auditoría. Por ello, es importante que se delimiten las responsabilidades y los productos a entregar que son objeto de auditoría externa en el contrato o propuesta.

**Algunos de los puntos importantes** que pueden llegar a estar en los informes respecto a seguridad y, sin que se pueda generalizar porque depende de la entidad, sector y circunstancias, 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: en el caso de la legislación incluso pueden producirse sanciones.
- Diferenciación de entornos de desarrollo y producción, en cuanto a datos y programas, y control de accesos.
- Involucramiento de la Alta Dirección, preferentemente a través de algún comité.
- Motivación de los empleados y directivos en relación con la seguridad.
- Evaluación periódica y adecuada de riesgos.
- Segregación de funciones, así como una organización adecuada.

Es frecuente también que quienes han pedido la auditoría quieran conocer después en qué medida se han resuelto los problemas, a partir de las decisiones tomadas, a través de los informes de los auditores internos o de quienes implanten las medidas.

Otro deseo frecuente es querer conocer la **evolución de la situación** en el tiempo, ya que aparecen nuevos riesgos, se reproducen otros, y algunos pueden variar de clasificación en función del cambio de plataformas u otros.

Para ello es útil mostrar en algún informe -principalmente los auditores internos- algunos cuadros que muestren la evolución, que en algunos casos ha sido útil para demostrar la rentabilidad de una función como administración de la seguridad o auditoría interna o para evaluar la utilidad de un plan de seguridad.

## Contratación de Auditoría Externa

Si no se sigue un proceso de selección adecuado de auditores externos, no se pueden garantizar los resultados y se puede llegar al desencanto al recibir el informe, lo que puede suponer no llegar a conocer las posibilidades reales de la auditoría de sistemas de información, sobre todo en un tema tan delicado como la seguridad.

Algunas consideraciones pueden ser:

- La entidad auditora debe ser independiente de la auditada en el caso de una auditoría externa: si está ofreciendo otros servicios a la vez, o piensa ofrecerlos en el futuro, o incluso a veces si ha sido proveedora en el pasado, a menudo puede encontrar dificultades internas para entregar un informe veraz y completo.
- Las personas que vayan a realizar el trabajo deben ser independientes y competentes, según el objetivo: sistemas operativos o plataformas concretas, por lo que no está de

más examinar sus perfiles e incluso mantener alguna entrevista, sin descartar preguntar por sorpresa en una reunión qué aspectos revisarían y qué técnicas usarían en el entorno que se les describa.
- No es tan común pedir referencias de otros trabajos similares como en el caso de consultoría pero se puede hacer, aunque para ello los auditores deberían pedir permiso previo a sus clientes.
- La auditoría debe encargarse a un nivel suficiente, normalmente Dirección General o Consejero Delegado, y a este nivel recibir los informes, porque si no a veces no se cuenta con el respaldo suficiente en las revisiones, y en todo caso puede que si el informe no es favorable quede escondido, y se ha perdido el dinero y a veces la oportunidad.
- 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: sólo parte de una base de datos, epígrafes de algunas actas, o simplemente mostrarles documentación, que no pueden copiar o no pueden sacar de las instalaciones del cliente: se puede exigir una cláusula de confidencialidad, y raramente se les deben mostrar datos reales confidenciales de clientes, proveedores, empleados u otros.

# Auditoría De Redes

## Vulnerabilidades en Redes

En las redes de comunicaciones, por causas propias de la tecnología, pueden producirse básicamente tres tipos de incidencias:
- **Alteración de bits**. Por error en los medios de transmisión, una trama puede sufrir variación en parte de su contenido. La forma más habitual de detectar, y corregir en su caso, este tipo de incidencias, es agregar 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 en el mejor de los casos.
- **Ausencia de tramas**. Por error en el medio, o en algún nodo, o por sobrecarga, 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.

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. En redes LAN suelen utilizarse medidas de control de acceso al edificio y al cableado, ya que la criptografía es muy onerosa todavía para redes locales.

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.

En el propio puesto de trabajo puede haber peligros, como grabar/retransmitir la imagen que se ve en la pantalla, teclados que guardan memoria del 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 claro la información dentro de la red local, es imprescindible tener una organización que controle estrictamente los equipos de escucha, bien sean estos físicos ("sniffer") o lógicos ("traceadores"). Ambos escuchadores, físicos y lógicos, son de uso habitual dentro de cualquier instalación de cierto tamaño. Por tanto, es fundamental que este uso legítimo esté controlado y no devenga en actividad fraudulenta.

El riesgo de interceptar un canal de comunicaciones, y poder extraer de él la información, tiene efectos relativamente similares a los de poder entrar, sin control, en el sistema de almacenamiento de una computadora.

Hay un punto especialmente crítico en los canales de comunicaciones que son las contraseñas de usuario. Mientras que en el sistema de almacenamiento las contraseñas suelen guardarse cifradas, es inhabitual que los equipos sean capaces de cifrar la contraseña cuando se envía al equipo central o al servidor.

Alguien que intercepte la información puede hacerse con las contraseñas en texto claro. Además, dado que los encabezados iniciales donde se teclea la contraseña son siempre los mismos, se facilita la labor de los agentes de interceptación, dado que proporcionan un patrón del paquete de información donde viaja la contraseña a interceptar.

# Auditando la Red Física

Se debe auditar hasta qué punto las instalaciones físicas del edificio ofrecen garantías y han sido estudiadas las vulnerabilidades existentes. Debe 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, sea total o parcial, debe comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y qué operatividad puede soportar. Dado que el tendido de cables es una actividad irrealizable a muy corto plazo, los planes de recuperación de contingencias deben tener prevista la recuperación en comunicaciones.

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

- Áreas controladas para los equipos de comunicaciones, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicaciones, para evitar accesos físicos.
- Controles de utilización de los equipos de pruebas de comunicaciones, usados para monitorear la red y su tráfico, que impidan su utilización inadecuada.
- 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.

## Lista de Control

Comprobar que:

1. El equipo de comunicaciones se mantiene en habitaciones cerradas con acceso limitado a personas autorizadas.
2. La seguridad física de los equipos de comunicaciones, tales como controladores de comunicaciones, dentro de las salas de equipos sea adecuada.
3. Sólo personas con responsabilidad y conocimientos están incluídas en la lista de personas permanentemente autorizadas para entrar en las salas de equipos de comunicaciones.
4. Se toman medidas para separar las actividades de electricistas y personal de tendido y mantenimiento de tendido de líneas telefónicas, así como sus autorizaciones de acceso, de aquellas del personal bajo control de la gerencia de comunicaciones.
5. En las zonas adyacentes a las salas de comunicaciones, todas las líneas de comunicaciones fuera de la vista.
6. Las líneas de comunicaciones, en las salas de comunicaciones, armarios distribuidores y terminaciones de los despachos, estarán etiquetadas con un código gestionado por

la gerencia de comunicaciones, y no por su descripción física o métodos sin coherencia.
7. Existen procedimientos para la protección de cables y bocas de conexión que dificulten el que sean interceptados o conectados por personas no autorizadas,
8. Se revisa periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.
9. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicación de datos deben tener propósitos y funciones definidos.
10. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados para monitorear líneas y fijar problemas incluyendo:
    a. Procedimiento restringiendo el uso de estos equipos a personal autorizado.
    b. Facilidades de traza y registro del tráfico de datos que posean los equipos de monitorización.
    c. Procedimientos de aprobación y registro ante las conexiones a líneas de comunicaciones en la detección y corrección de problemas.
11. En el plan general de recuperación de desastres para servicios de información se presta adecuada atención a la recuperación y vuelta al servicio de los sistemas de comunicación de datos.
12. Existen planes de contingencia para desastres que sólo afectan a las comunicaciones, como el fallo de una sala completa de comunicaciones.
13. Las alternativas de respaldo de comunicaciones, bien sea con las mismas salas o con salas de respaldo, consideran la seguridad física de estos lugares.
14. Las líneas telefónicas usadas para datos, cuyos números no deben ser públicos, tienen dispositivos/procedimientos de seguridad tales como retrollamada, códigos de conexión o interruptores para impedir accesos no autorizados al sistema informático.

## Auditando la Red Lógica

La red hace que un equipo pueda acceder legítimamente a cualquier otro, incluyendo al tráfico que circule hacia cualquier equipo de la red. Todo ello por métodos exclusivamente lógicos, sin necesidad de instalar físicamente ningún dispositivo. Si un equipo se pone a enviar indiscriminadamente mensajes, puede ser capaz de bloquear la red completa incluyendo al resto de los equipos de la instalación.

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.

En general, si se quiere que la información que viaja por la red no pueda ser espiada, la única solución totalmente efectiva es el cifrado.

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.

- Facilidades de control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas.
- Controles para asegurar que las transmisiones van solamente a usuarios autorizados y que los mensajes no tienen por qué seguir siempre la misma ruta.
- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.
- 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 través de puertas, en cualquier punto de la red, a otros sistemas informáticos.

## Lista de Control

Comprobar que:

1. El software de comunicaciones, para permitir el acceso, exige código de usuario y contraseña.
2. Revisar el procedimiento de conexión de usuario y comprobar que:
    a. Los usuarios no pueden acceder a ningún sistema, ni siquiera de ayuda, antes de haberse identificado correctamente.
    b. Se inhabilita al usuario que sea incapaz de dar la contraseña después de un número determinado de intentos infructuosos.
    c. Se obliga a cambiar la contraseña regularmente.
    d. Las contraseñas no son mostradas en pantalla cuando se teclean.
    e. Durante el procesamiento de identificación, los usuarios son informados de cuándo fue su última conexión para ayudar a identificar potenciales suplantaciones o accesos no autorizados.
3. Cualquier procedimiento del fabricante, mediante hardware o software, que permita el libre acceso y que haya sido utilizado en la instalación original, debe haber sido inhabilitado o cambiado.
4. Se toman estadísticas que incluyan tasas de errores y de retransmisión.
5. Los protocolos utilizados, revisados con el personal adecuado de comunicaciones, disponen de procedimientos de control de errores con la seguridad suficiente.
6. Los mensajes lógicos transmitidos identifican el originante, la fecha, la hora y el receptor.
7. El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdidos, o retrasados.
8. La arquitectura de comunicaciones utiliza indistintamente cualquier ruta disponible de transmisión para minimizar el impacto de una escucha de datos sensibles en una ruta determinada.
9. Existen controles para que los datos sensibles sólo puedan ser impresos en las impresoras asignadas y vistos desde los terminales autorizados.
10. Existen procedimientos de registro para capturar y ayudar a reconstruir todas las actividades de las transacciones.

11. Los archivos de registro son revisados, si es posible, a través de herramientas automáticas, diariamente, vigilando intentos impropios de acceso.
12. Existen análisis de riesgos para las aplicaciones de proceso de datos a fin de identificar aquellas en las que el cifrado resulte apropiado.
13. Si se utiliza cifrado:
    a. Existen procedimientos de control sobre la generación e intercambio de claves.
    b. Las claves de cifrado son cambiadas regularmente.
    c. El transporte de las claves de cifrado desde donde se generan a los equipos que las utilizan sigue un procedimiento adecuado.
14. Si se utilizan canales de comunicación uniendo diversos edificios de la misma organización, y existen datos sensibles que circulen por ellos, comprobar que estos canales se cifran automáticamente, para evitar que una incerceptación sistemática a un canal comprometa a todas las aplicaciones.
15. Si la organización tiene canales de comunicación con otras organizaciones se analice la conveniencia de cifrar estos canales.
16. Si se utiliza la transmisión de datos sensibles a través de redes abiertas como Internet, comprobar que estos datos viajan cifrados.
17. Si en una red local existen equipos con módems, se han revisado los controles de seguridad asociados para impedir el acceso de equipos foráneos a la red local.
18. Existe una política de prohibición de introducir programas personales o conectar equipos privados a la red local.
19. Todas las “puertas traseras” y accesos no específicamente autorizados están bloqueados. En equipos activos de comunicaciones, como puentes, encaminadores, conmutadores, etc., esto significa que los accesos para servicio remoto están inhabilitados o tienen procedimientos específicos de control.
20. Periódicamente se ejecutan, mediante los programas actualizados y adecuados, ataques para descubrir vulnerabilidades, que los resultados se documentan y se corrigen las deficiencias observadas. Estos ataques deben realizarse independientemente a:
    a. Servidores, desde dentro del servidor.
    b. Servidores, desde la red interna.
    c. Servidores Web, específicamente.
    d. Intranet, desde dentro de ella.
    e. Cortafuegos, desde dentro de ellos.
    f. Accesos desde el exterior y/o Internet.