Gestión de los controles de acceso según ISO 27001

"Los usuarios sólo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso". Así reza la introducción a la Sección A9 del Anexo A. En detalle, de acuerdo con cada una de las sub cláusulas, esto es lo que debemos hacer para gestionar los controles de acceso según ISO 27001:

A.9.1.1 Política de control de acceso

Se debe **establecer, documentar y revisar con periodicidad una política de control de acceso**, teniendo en cuenta los requisitos de la organización para los activos a su alcance.

Las reglas, derechos y restricciones de control de acceso, junto con la profundidad de los controles utilizados, deben reflejar los riesgos de seguridad de la información de la organización.

En pocas palabras, **el control de acceso debe ser concedido de acuerdo con quién necesita saber, quién necesita usar y a cuánto acceso requieren**. Los controles de acceso según ISO 27001 pueden ser **de naturaleza digital y física**: por ejemplo, restricciones de permisos en las cuentas de usuario, así como limitaciones sobre quién puede acceder a ciertas ubicaciones físicas. Para ello, la política debe tener en cuenta:

- Los requisitos de seguridad de las aplicaciones comerciales y su alineación con el esquema de clasificación de información en uso (A.8).
- Aclarar quién necesita acceder, saber quién necesita usar la información, todo ello con base en procedimientos documentados.
- Gestión de los derechos de acceso y derechos de acceso privilegiados, incluyendo la adición de cambios y las revisiones periódicas.
- **Reglas de control de acceso que deben estar respaldadas por procedimientos formales y responsabilidades definidas**.

Los controles de acceso según ISO 27001 deben revisarse en función del cambio de roles, y, en particular, durante la salida, para alinearse con el Anexo A.7.

A.9.1.2 Acceso a redes y servicios de red

El **principio de acceso mínimo** es el enfoque general para la protección, en lugar de acceso ilimitado y derechos de súper usuario sin una cuidadosa consideración. Como tales, los usuarios sólo deberían tener acceso a la red y a los servicios de red que necesitan usar o conocer para desarrollar su trabajo.

Por lo tanto, la política debe abordar:

- Las redes y los servicios de red.
- Procedimientos de autorización para mostrar quién tiene acceso a qué y cuándo.
- Controles y procedimientos de gestión para evitar el acceso.

A.9.2.1 Registro de usuarios y anulación de registro

Es preciso **implementar un proceso formal de registro y cancelación de registro de usuarios**. Un buen proceso para la administración de ID de usuario incluye la posibilidad de asociar ID individuales a personas reales y limitar las ID de acceso compartido, que deben probarse y registrarse donde se haga.

Un buen proceso de incorporación y salida, se vincula con A7, para mostrar el registro, y evitar la re-emisión de identificaciones antiguas. Una revisión periódica de las identificaciones ilustrará un buen control y reforzará la gestión continua.

A.9.2.2 Aprovisionamiento de acceso de usuario

Se debe **implementar un proceso – simple y documentado – para asignar o revocar derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios**. El proceso de aprovisionamiento y revocación debe incluir:

- Autorización del propietario del sistema o servicio de información para el uso de estos activos.
- **Verificar que el acceso otorgado sea relevante para el rol que se está realizando**.
- Proteger contra el aprovisionamiento antes de que se complete la autorización.

El acceso de los usuarios siempre debe estar dirigido por la organización y basado en los requisitos de la misma.

A.9.2.3 Gestión de derechos de acceso privilegiado

Se trata de **administrar niveles de acceso privilegiados, más altos y más estrictos**. La asignación y el uso de los derechos de acceso privilegiado deben ser controlados en forma muy estricta, dados los derechos adicionales que generalmente se transmiten sobre los activos de información y los sistemas que los controlan.

A.9.2.4 Gestión de información secreta de autenticación de usuarios

La información secreta de autenticación es una puerta de acceso para llegar a activos valiosos. Por lo general**, incluye contraseñas y claves de cifrado, por lo que debe controlarse mediante un proceso de gestión formal y debe ser mantenida en forma confidencial para el usuario**.

Esto generalmente está vinculado a contratos de trabajo y procesos disciplinarios, y obligaciones de proveedores.

A.9.2.5 Revisión de los derechos de acceso del usuario

Los propietarios de activos de a información deben **revisar los derechos de acceso de los usuarios a intervalos regulares**, tanto en torno al cambio individual – incorporación, cambio de rol y salida -, como a auditorías más amplias del acceso a los sistemas. **Las autorizaciones para derechos de acceso privilegiado deben revisarse a intervalos más frecuentes, dada su naturaleza de mayor riesgo.**

A.9.2.6 Eliminación o ajuste de los derechos de acceso

Cómo anotamos anteriormente, los derechos de acceso de todos los empleados y usuarios externos a las instalaciones de procesamiento de información, deben concluir al finalizar el vínculo laboral, el contrato o el acuerdo. Una buena política de salida garantizará que esto suceda.

A.9.3.1 Uso de información secreta de autenticación

Se trata simplemente de asegurar que los usuarios sigan políticas y asuman el compromiso de mantener confidencial cualquier información secreta de autenticación.

A.9.4.1 Restricción de acceso a la información

El acceso a la información **y las funciones del sistema deben estar vinculadas a la política de control de acceso**. Las consideraciones clave deben incluir:

- Control de acceso basado en roles.
- Niveles de acceso.
- Diseño de sistemas de menú, dentro de las aplicaciones.
- Leer, escribir, eliminar y ejecutar permisos.
- Limitación de la producción de información.
- Controles de acceso físicos y/o lógicos a aplicaciones, datos y sistemas sensibles.

El auditor verificará que se hayan hecho consideraciones para limitar el acceso dentro de los sistemas y aplicaciones que soportan políticas de control de acceso, requisitos comerciales, niveles de riesgo y segregación de funciones.

A.9.4.2 Procedimientos de inicio seguro

El acceso a los sistemas y aplicaciones debe controlarse mediante un procedimiento de inicio de sesión seguro, para demostrar la identidad del usuario. Esto puede ir más allá del enfoque típico de contraseña de múltiples factores, biometría, tarjetas inteligentes y otros medios de cifrado en función del riesgo que se está considerando.

A.9.4.3 Sistema de gestión de contraseñas

El propósito de un sistema de administración de contraseñas es **garantizar que estas sean de calidad, cumplan con el nivel requerido y se apliquen de manera consistente**. Los sistemas de generación y gestión de contraseñas proporcionan una buena forma de centralizar el suministro de acceso, pero como sucede con cualquier control, deben implementarse cuidadosamente para garantizar niveles óptimos de seguridad y protección.

A.9.4.4 Uso de programas de utilidad privilegiada

Los programas informáticos que tienen la capacidad de anular controles del sistema y de las aplicaciones, aunque resulten muy útiles, deben ser gestionados con mucha atención. Ellos pueden ser un objetivo atractivo para atacantes maliciosos. El acceso a ellos debe restringirse al menor número de personas.

A.9.4.5 Control de acceso al código fuente del programa

El acceso al código fuente de los programas debe estar restringido, al igual que a los elementos asociados como diseños, especificaciones, planes de verificación y de validación. **El código fuente de los programas informáticos, puede ser vulnerable a ataques si no está protegido en forma adecuada.**

10.1.1 POLÍTICA SOBRE EL EMPLEO DE CONTROLES CRIPTOGRÁFICOS

Los controles criptográficos están enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, se impone establecer un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad

En primer lugar en una política de implementación y administración de claves de cifrado de datos se debe identificar a un responsable de la política para su implementación y administración.

La clave de la política de controles criptográficos está en identificar

- Para que información y en qué circunstancias será necesario aplicar claves criptográficas
- Los medios a emplear
- La gestión, mantenimiento y actualización de dichos medios

A11 SEGURIDAD FISICA Y DEL ENTORNO

En coordinación con las medidas tecnológicas **ISO 27001** en este capítulo se centra en la necesidad de identificar y establecer medidas de control físicas para proteger adecuadamente los activos de información para evitar incidentes que afecten a la integridad física de la información o interferencias no deseadas

Este capítulo establece dos controles referidos a

- AREAS SEGURAS
- EQUIPAMIENTO

11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA

Control orientado a proveer protección contra la entrada no autorizada.

- Tanto los perímetros y controles o defensas previstas deben determinarse en un análisis o evaluación de riesgos
- **Seguridad perimetral:**
  Los requisitos para la seguridad física deben tener en cuenta los niveles de protección del perímetro de las instalaciones o elementos que contienen la información a proteger
    - Muros
    - Vallas
    - Alarmas
    - Suelos
    - Protección de ventanas
    - Cerraduras
    - Etc.

- **Áreas atendidas:** las áreas restringidas a personal autorizado deberían contar con un área de recepción atendida o medios de control adecuados para limitar el acceso físico
- **Barreras:** Si es aplicable deberían considerarse barreras físicas que impidan el acceso no autorizado y protejan el área de agentes ambientales adversos
- **Sistemas Antiincendios:** contar con sistemas de protección contra el fuego cumpliendo con la legislación vigente
- **Detección de intrusión:** Se deben considerar sistemas de detección de intrusos (p ej. Alarmas)
- **Segmentación de espacios:** Deberían separarse físicamente las áreas de proceso de información que van a ser gestionadas por personal externo de las propias de la organización

No se debe subestimar la seguridad física

Asegurar su entorno físico, y especialmente sus áreas seguras, sigue el mismo enfoque que utilizamos para proteger la información digital:

- 1. definir el contexto,
- 2. Evaluar los riesgos
- 3. Implementar los controles de seguridad más adecuados: cuanto mayor sea el valor y el riesgo, mayor será nivel de protección.
- 4. Enfrentar las amenazas ambiéntale. En seguridad física, no es suficiente con enfrentar riesgos en cuento a la seguridad sino también se necesita asegurar los equipos e instalaciones para enfrentar las amenazas ambientales VER 11.1.4 Protección contra amenazas externas y del ambiente

11.1.2 CONTROLES DE ACCESO FÍSICO

Aquellas áreas que se consideran seguras deben estar protegidas por controles de entrada que permitan solo personal autorizado

- Los visitantes deben autenticarse: se debe registrar su fecha y hora de entrada / salida.
- Monitorización: La actividad debe ser monitoreada de acuerdo con la evaluación de riesgos.

- Comunicación: Se debe informar a los trabajadores que acceden sobre los procedimientos de seguridad y emergencia (especialmente en el caso de los centros de datos) y se les debe otorgar acceso para fines específicos.
- Personal Externo: Si hay personal externo autorizado y realizan el trabajo si ser acompañados por personal propio en una sala de servidores o centro de datos, debemos asegurarnos de que el acceso a otras áreas estén bloqueadas y que todo el cableado esté seguro. Se aconseja realizar una inspección física de las instalaciones al finalizar los trabajos.
- Identificaciones: Al personal que trabaje en áreas seguras se le debe exigir llevar identificación y cualquier persona que no use la identificación requerida debe ser notificada a los empleados de seguridad.
- Revisión de permisos: Los derechos de acceso deben revisarse periódicamente y revocarse según corresponda.

11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES

En cuanto a las instalaciones deben diseñarse para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes.

Se debe considerar la posibilidad de en uso de técnicas de enmascaramiento (“masking”) de datos referidos a nombres o actividades de clientes.

Supongamos por ejemplo el caso un centro de tratamiento de datos donde muchas líneas telefónicas están abiertas en cualquier momento o situaciones como la formación de usuarios o pruebas de software.

11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL AMBIENTE

En un mundo de crecientes inestabilidades y amenazas terroristas y de un clima impredecible, se debe considerar, diseñar y aplicar la protección física contra factores externos.

Si bien las leyes vigentes nos obligan a tener planes de protección y emergencias deberíamos ir más allá y si fuera necesario buscar asesoramiento especializado.

También podríamos pensar que las amenazas externas y del medioambiente quedan cubiertos con el desarrollo de "Planes de Continuidad del Negocio" y de "Recuperación ante desastres", sin embargo convendría considerar en este apartado las medidas de protección contra inundaciones, incendios y terremotos para mitigar sus efectos.

11.1.5 EL TRABAJO EN LAS ÁREAS SEGURAS

Adicionalmente a las medidas de protección física en las áreas seguras deberíamos definir procedimientos de trabajo tales como

- Prohibición de trabajos sin supervisión por parte de terceros
- Revisión de las zonas a la finalización de las visitas
- Prohibición de uso de móviles / cámaras a no ser que estén expresamente autorizados

11.1.6 ÁREAS DE ENTREGA Y DE CARGA

Los puntos de carga suelen ser puntos sensibles para la seguridad física por lo que deberíamos tomar en cuenta algunos aspectos de control en nuestra evaluación de riesgos tales como:

- Horarios definidos de apertura y cierre
- Control de apertura y cierre de puertas externas e internas
- Control de personal
- Realización de inventarios de materiales entregados
- Revisión de mercancías entregadas para detectar materiales peligrosos
- Separar entregas entrantes y salientes
- Necesidad de informar de cualquier incidente a los responsables de seguridad
- Barreras adicionales de seguridad

OBJETIVO2: SEGURIDAD DE LOS EQUIPOS

Los daños en los equipos pueden causar interrupciones en la actividad de una organización o vulnerar la confidencialidad de la información causada por robos de activos

Veamos los controles que deberemos revisar en nuestra evaluación de riesgos para la seguridad de la información

11.2.1 UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO

Controles para proteger los equipos de daños ambientales y accesos no autorizados

- Evitar accesos no necesarios
- Proteger los equipos de áreas sensibles como centros de datos o salas de servidores
- Controles de protección en lugares de almacenamiento de equipos si estos contienen información
- Medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.)
- Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos
- Medidas de protección contra radiaciones
- Deben establecerse pautas para comer, beber y fumar cerca del equipo para evitar daños o simplemente evitar que los empleados estén en contacto con los equipos si no están trabajando en ellos.

11.2.2 ELEMENTOS DE SOPORTE

Se trata de establecer medidas de control para el suministro necesario para mantener operativas las instalaciones y los equipos

A menudo este capítulo se pasa por alto en pequeñas y medianas empresas pero conviene que tengamos en cuenta controles para garantizarnos según

nuestras posibilidades la cobertura ante fallos del suministro eléctrico y las comunicaciones.

Los controles de este apartado van enfocados a:

- Cumplir con las especificaciones del fabricante de los equipos en cuanto a suministros (electica, gas etc.)
- Cumplir los requisitos legales
- Establecer algún proceso de detección de fallos de suministro
- Mantener si es posibles alternativas a fallos de suministro (sistemas de alimentación ininterrumpida, rutas alternativas en comunicaciones etc.)

En este apartado deberemos ser imaginativos pues no siempre está a nuestro alcance poder duplicar las comunicaciones o los suministros de energía eléctrica o gas etc. A veces pasa por reforzar sistemas como Teletrabajo, soportes CLOUD o convenios con empresas más grandes como clientes importantes de confianza con mayor infraestructura en caso de desastres que no podamos asumir.

11.2.3 SEGURIDAD EN EL CABLEADO

Controles para protección del cableado de energía y de comunicaciones que afecta a los sistemas de información

Se trata de evitar tanto el posible daño de las infraestructuras como las posibles interferencias que corrompan los datos o el suministro

RECOMENDACIONES

Los cables deben estar bajo tierra hasta el punto de acceso dentro de la instalación, de o alternativamente debería pensarse en otro tipo de protección.

Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencias.

Los puntos de acceso del cableado a los equipos o a las salas deben asegurarse según corresponda y los cables deben estar protegidos.

Como medidas adicionales podríamos realizar barridos técnicos de los cables de comunicación para dispositivos no autorizados (bugs y sniffers) conectados al cableado.

El cableado alrededor de las salas de servidores y centros de datos debería estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.

Finalmente deberemos tener en cuenta siempre el acceso restringido y controlado a las sales de paneles de conexión

11.2.4 MANTENIMIENTO DEL EQUIPAMIENTO

Se trata de controles para garantizar que los equipos se mantienen adecuadamente para garantizar que no se deterioren y estén siempre disponibles.

Para ello deberíamos tener en cuenta

- Las recomendaciones del fabricante
- Solo personal autorizado debe mantener equipos críticos y se deben mantener registros.
- La información sensible debería removerse del equipo cuando sea necesario
- Cumplir con todos los requisitos de las pólizas de seguros

11.2.5 RETIRO DE BIENES

Cuando se trata de la retirada de un activo de información ya sea equipos, software u otros dispositivos de información deberíamos controlar

- La identificación y autorización de personal autorizado a retirar equipos o activos fuera de la organización
- Fijar límites de tiempo
- Llevar un registro de equipos retirados y de su retorno así como de la identificación de personal.

11.1.2 CONTROLES DE ACCESO FÍSICO

Aquellas áreas que se consideran seguras deben estar protegidas por controles de entrada que permitan solo personal autorizado

- Los visitantes deben autenticarse: se debe registrar su fecha y hora de entrada / salida.
- Monitorización: La actividad debe ser monitoreada de acuerdo con la evaluación de riesgos.
- Comunicación: Se debe informar a los trabajadores que acceden sobre los procedimientos de seguridad y emergencia (especialmente en el caso de los centros de datos) y se les debe otorgar acceso para fines específicos.
- Personal Externo: Si hay personal externo autorizado y realizan el trabajo si ser acompañados por personal propio en una sala de servidores o centro de datos, debemos asegurarnos de que el acceso a otras áreas estén bloqueadas y que todo el cableado esté seguro. Se aconseja realizar una inspección física de las instalaciones al finalizar los trabajos.
- Identificaciones: Al personal que trabaje en áreas seguras se le debe exigir llevar identificación y cualquier persona que no use la identificación requerida debe ser notificada a los empleados de seguridad.
- Revisión de permisos: Los derechos de acceso deben revisarse periódicamente y revocarse según corresponda.

11.1.3 SEGURIDAD DE OFICINAS, DESPACHOS E INSTALACIONES

En cuanto a las instalaciones deben diseñarse para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes.

Se debe considerar la posibilidad de en uso de técnicas de enmascaramiento (“masking”) de datos referidos a nombres o actividades de clientes.

Supongamos por ejemplo el caso un centro de tratamiento de datos donde muchas líneas telefónicas están abiertas en cualquier momento o situaciones como la formación de usuarios o pruebas de software.

11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL AMBIENTE

En un mundo de crecientes inestabilidades y amenazas terroristas y de un clima impredecible, se debe considerar, diseñar y aplicar la protección física contra factores externos.

Si bien las leyes vigentes nos obligan a tener planes de protección y emergencias deberíamos ir más allá y si fuera necesario buscar asesoramiento especializado.

También podríamos pensar que las amenazas externas y del medioambiente quedan cubiertos con el desarrollo de “Planes de Continuidad del Negocio” y de “Recuperación ante desastres”, sin embargo convendría considerar en este apartado las medidas de protección contra inundaciones, incendios y terremotos para mitigar sus efectos.

11.1.5 EL TRABAJO EN LAS ÁREAS SEGURAS

Adicionalmente a las medidas de protección física en las áreas seguras deberíamos definir procedimientos de trabajo tales como

- Prohibición de trabajos sin supervisión por parte de terceros
- Revisión de las zonas a la finalización de las visitas
- Prohibición de uso de móviles / cámaras a no ser que estén expresamente autorizados

11.1.6 ÁREAS DE ENTREGA Y DE CARGA

Los puntos de carga suelen ser puntos sensibles para la seguridad física por lo que deberíamos tomar en cuenta algunos aspectos de control en nuestra evaluación de riesgos tales como:

- Horarios definidos de apertura y cierre
- Control de apertura y cierre de puertas externas e internas
- Control de personal
- Realización de inventarios de materiales entregados
- Revisión de mercancías entregadas para detectar materiales peligrosos
- Separar entregas entrantes y salientes
- Necesidad de informar de cualquier incidente a los responsables de seguridad
- Barreras adicionales de seguridad

OBJETIVO2: SEGURIDAD DE LOS EQUIPOS

Los daños en los equipos pueden causar interrupciones en la actividad de una organización o vulnerar la confidencialidad de la información causada por robos de activos

Veamos los controles que deberemos revisar en nuestra evaluación de riesgos para la seguridad de la información

11.2.1 UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO

Controles para proteger los equipos de daños ambientales y accesos no autorizados

- Evitar accesos no necesarios
- Proteger los equipos de áreas sensibles como centros de datos o salas de servidores
- Controles de protección en lugares de almacenamiento de equipos si estos contienen información
- Medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.)
- Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos

- Medidas de protección contra radiaciones
- Deben establecerse pautas para comer, beber y fumar cerca del equipo para evitar daños o simplemente evitar que los empleados estén en contacto con los equipos si no están trabajando en ellos.

11.2.2 ELEMENTOS DE SOPORTE

Se trata de establecer medidas de control para el suministro necesario para mantener operativas las instalaciones y los equipos

A menudo este capítulo se pasa por alto en pequeñas y medianas empresas pero conviene que tengamos en cuenta controles para garantizarnos según nuestras posibilidades la cobertura ante fallos del suministro eléctrico y las comunicaciones.

Los controles de este apartado van enfocados a:

- Cumplir con las especificaciones del fabricante de los equipos en cuanto a suministros (electica, gas etc.)
- Cumplir los requisitos legales
- Establecer algún proceso de detección de fallos de suministro
- Mantener si es posibles alternativas a fallos de suministro (sistemas de alimentación ininterrumpida, rutas alternativas en comunicaciones etc.)

En este apartado deberemos ser imaginativos pues no siempre está a nuestro alcance poder duplicar las comunicaciones o los suministros de energía eléctrica o gas etc. A veces pasa por reforzar sistemas como Teletrabajo, soportes CLOUD o convenios con empresas más grandes como clientes importantes de confianza con mayor infraestructura en caso de desastres que no podamos asumir.

11.2.3 SEGURIDAD EN EL CABLEADO

Controles para protección del cableado de energía y de comunicaciones que afecta a los sistemas de información

Se trata de evitar tanto el posible daño de las infraestructuras como las posibles interferencias que corrompan los datos o el suministro

RECOMENDACIONES

Los cables deben estar bajo tierra hasta el punto de acceso dentro de la instalación, de o alternativamente debería pensarse en otro tipo de protección.

Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencias.

Los puntos de acceso del cableado a los equipos o a las salas deben asegurarse según corresponda y los cables deben estar protegidos.

Como medidas adicionales podríamos realizar barridos técnicos de los cables de comunicación para dispositivos no autorizados (bugs y sniffers) conectados al cableado.

El cableado alrededor de las salas de servidores y centros de datos debería estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.

Finalmente deberemos tener en cuenta siempre el acceso restringido y controlado a las sales de paneles de conexión

11.2.4 MANTENIMIENTO DEL EQUIPAMIENTO

Se trata de controles para garantizar que los equipos se mantienen adecuadamente para garantizar que no se deterioren y estén siempre disponibles.

Para ello deberíamos tener en cuenta

- Las recomendaciones del fabricante
- Solo personal autorizado debe mantener equipos críticos y se deben mantener registros.
- La información sensible debería removerse del equipo cuando sea necesario
- Cumplir con todos los requisitos de las pólizas de seguros

11.2.5 RETIRO DE BIENES

Cuando se trata de la retirada de un activo de información ya sea equipos, software u otros dispositivos de información deberíamos controlar

- La identificación y autorización de personal autorizado a retirar equipos o activos fuera de la organización
- Fijar límites de tiempo
- Llevar un registro de equipos retirados y de su retorno así como de la identificación de personal.

11.2.7 SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE EQUIPOS

Para los equipos que van a ser reutilizados deberíamos garantizar

- La información que contenían se ha destruido o sobre escribido correctamente antes de su reutilización
- Garantizar que las información se ha eliminado completamente considerando que los formateos estándar no realizan esta tarea de forma adecuada
- Los equipos averiados deben estar sujetos a una evaluación de riesgos antes de disponer de ellos para una reparación

11.2.8 EQUIPAMIENTO DESATENDIDO POR EL USUARIO

Los usuarios no deben dejar las sesiones abiertas mientras el equipo no este atendido.

Además de los procedimientos de bloqueo de pantalla, la sesión de la aplicación y de la red debe cerrarse cuando las conexiones no se utilizan.

Esto debería aplicarse tanto a los dispositivos móviles como a los equipos fijos.

11.2.9 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Una de las políticas de seguridad más fácilmente reconocidas y que más se incumple en la práctica y que podríamos decir que se aplica a todas las personas en todas las organizaciones.

Las pantallas no deben mostrar información cuando el equipo no esté en uso y los escritorios deben estar libres de papeles cuando no estén en uso o desatendidos.

Dependiendo de la clasificación de los documentos en papel y la cultura de la organización, el papel y los medios extraíbles deben asegurarse según la política cuando no estén en uso.

Las evaluaciones de riesgos deberían considerar el uso de tecnologías que permitan realizar copias de la información tales como: Impresoras, fotocopiadoras, escáneres y cámaras (especialmente en teléfonos)

Las impresoras se pueden configurar de modo que solo el creador pueda acceder a las copias una vez que se haya ingresado un código en la máquina para evitar el acceso no autorizado.

-