1.4.4. Salvaguardas y contramedidas más habituales

1. Seguridad de recursos humanos

Tanto antes del empleo, como durante el empleo, y a la terminación del mismo, conviene adoptar medidas, salvaguardas, o controles, para proteger la información que será accedida, e impactada por las personas. Se trata, por ejemplo, de establecer obligaciones y responsabilidades legales durante la contratación, o de establecer cómo actuar, de cara a la información, cuando una persona abandone la empresa. Dependiendo de cada circunstancia, podría corresponder aplicar, con mayor o menor exhaustividad, alguna de las siguientes salvaguardas habituales:

- Definición de roles y responsabilidades que contraerá el trabajador.
- Investigación de antecedentes.
- Formación y capacitación de los trabajadores en seguridad de la información.
- Definición de procesos disciplinarios.
- Definir las responsabilidades a la terminación del contrato.
- Devolución de activos.
- Retirada de derechos de acceso a la información.

2. Seguridad ambiental

Los equipos informáticos deben disponer de un entorno adecuado. Por ejemplo, no es óptimo que un servidor empresarial comparta las mismas condiciones de temperatura y suministro eléctrico que los ordenadores de usuario. De ser posible, hay que proporcionarle un espacio mejor, porque el riesgo de una amenaza actuando sobre él es mayor. Si existe la posibilidad, debe proporcionarse un sistema de alimentación eléctrica ininterrumpido, y unas condiciones de temperatura adecuadas (por ejemplo entre 20° y 25°, que reduzcan el deterioro de sus componentes si se vieran forzados a trabajar a temperaturas elevadas). Debe intentar ubicarse en un recinto separado, que se denominará en adelante Centro de Proceso de Datos o CPD.

Las amenazas vistas en el apartado anterior, en la categoría de “desastres naturales”, y amenazas “de origen industrial”, precisan de salvaguardas, de las que las más habituales son:

- Medidas que eviten el fuego, el humo o el agua: sistema anti-incendio y anti-inundaciones, bien solo de alarma, o incluso de extinción del incendio, o de evacuación del agua.
- Medidas que eviten las vibraciones, golpes, y caídas accidentales: como la fijación en armarios industriales para fijación de equipos informáticos, o armarios tipo rack).
- Medidas para proporcionar temperatura y humedad adecuadas, como equipos de aire acondicionado, y alarmas por exceso, o por defecto (riesgo de condensación).

- Medidas que eviten fallos de suministro eléctrico (corte del suministro, variaciones de tensión por encima o por debajo del suministro nominal, caídas de rayos, etc.).
- Seguridad del cableado, tanto en los materiales empleados, como en su disposición o tendido, siguiendo pautas de un sistema de cableado estructurado, que aseguren una correcta acometida al CPD, un trazado interior adecuado, y unas conexiones a los equipos correctas, de manera practicable, ordenada, e identificada.
- Un mantenimiento preventivo de los equipos, según indicaciones del fabricante, y al menos con chequeos periódicos generales (vías de salida de aire de los chasis, revisiones de temperatura de los procesadores y/o placa base, revisiones de leds, u otros indicadores del buen funcionamiento de discos duros, fuentes de alimentación, etc.).
- Asegurar condiciones de seguridad para desplazamientos del equipo fuera del CPD (vigilancia, exposición a campos electromagnéticos, condiciones de embalaje, y transporte).
- Seguridad al final del ciclo de vida del equipo, incluida su destrucción segura.

Recuerde

Las amenazas no pueden impedirse en su totalidad, por lo que deben contemplarse, anticipando la situación de que sucedan, más tarde o más temprano, según su probabilidad de ocurrencia.

Actividades

Investigue qué salvaguardas ambientales puede incorporar un ordenador en sus subsistemas: placa base, fuente de alimentación, discos duros, y chasis interno.

3. Seguridad física

El acceso físico a los ordenadores y equipos aumenta el riesgo de cualquier incidente. Debe aplicarse el criterio de conceder acceso exclusivamente a quien lo necesite por sus funciones y, a ser posible, concederlo solamente cuándo y cómo lo necesite (por ejemplo en un horario determinado, y/o en presencia de otra persona). Así, en general, los usuarios no deben tener acceso físico a servidores, o a equipos de comunicaciones; tampoco los desarrolladores de aplicaciones, ni administradores de bases de datos, ni la Dirección de la empresa, deberían tener acceso físico a servidores o equipos de comunicaciones, porque, en todos esos casos, su trabajo no lo exige.

Las consecuencias de un ataque con acceso físico, serán normalmente de máxima gravedad, porque se puede lograr el máximo nivel de acceso posible a toda la información. Entre los infractores, se pueden encontrar los propios usuarios o trabajadores de la empresa, antiguos empleados que conserven sistemas de acreditación que les den acceso, y personas externas, como ladrones, salteadores, o hackers.

Habitualmente, el incidente más frecuente por acceso físico es accidental o no intencionado: se trata de errores humanos protagonizados por personal del departamento de informática o TIC, por personal de servicios auxiliares (limpieza, seguridad o mantenimiento), o incluso por proveedores o visitas.

Se trata, por tanto, de proteger a los equipos de accidentes que ocurren cuando hay acceso humano a los equipos. Entre las salvaguardas más habituales para proteger el acceso físico, se encuentran las siguientes:

- Establecer un perímetro de seguridad física (local, habitaciones), con elementos constructivos acordes (puertas, paredes, ventanas, techos, suelos, etc.).
- Mecanismos de control de ingreso físico (acreditaciones, cerraduras automáticas, etc.).
- Establecer y definir áreas de acceso público, de entrega, de carga, etc.
- Protección contra locales o actividades cercanas (incendios, explosiones, vías de vehículos, o cargas en movimiento).

Actividades

Reflexione sobre el riesgo de que el local donde se alojan los equipos informáticos de una entidad financiera esté ubicado junto a una gasolinera, disponga de ventanas (protegidas o no), incluya muchas cámaras de seguridad, y rótulos con el nombre de la entidad financiera en la fachada.

4. Seguridad de acceso lógico

El acceso lógico se refiere al acceso a la información de manera remota, es decir, sin emplear un periférico conectado directamente al equipo. Por ello, interviene forzosamente una red de comunicaciones, que extiende el acceso al servidor más allá del CPD, donde estén confinados sus periféricos de entrada y salida.

Las principales medidas de seguridad que se pueden interponer para reducir el riesgo de un incidente de seguridad, aprovechando una vulnerabilidad en el acceso lógico, son las siguientes:

- Definir una política de control de acceso, que identifique la información relacionada con actividades comerciales, los responsables de conceder-configurar-revocar los accesos, el procedimiento de solicitud, etc.
- Existencia de un registro de usuarios, y de los servicios a los que acceden.
- Nota: Es importante mantener un registro actualizado de los usuarios, de los servicios, y de los accesos autorizados de los usuarios a los servicios.
- Gestión de privilegios de acceso, sobre la base de "solo lo que necesitan saber".
- Gestión de claves de usuario, tanto de las características técnicas o de complejidad, como de la prohibición de divulgación de las mismas.
- Revisiones periódicas de los derechos de acceso de los usuarios.
- El establecimiento de responsabilidades del usuario, en cuanto al uso de claves secretas, equipos desatendidos, políticas de "mesas" y pantallas "limpias" (que no muestren información que no sea de carácter público).
- La existencia de una política de uso de los servicios de red (internet, correo electrónico, etc.).
- Mecanismos de autenticación y registro para las conexiones externas a la empresa o remotas, como técnicas de redes privadas virtuales (VPN).
- Separaciones de redes, por ejemplo, en base a servicios de información, o grupos de usuarios o sistemas.
- Controles de las conexiones que realizan los usuarios hacia fuera de la empresa.
- Controles de acceso al sistema operativo, como la identificación y autenticación del usuario, un sistema automático de gestión de contraseñas, la restricción del uso de las utilidades del sistema operativo, el cierre de sesiones por inactividad, y la limitación de los periodos válidos para los inicios de sesión.
- Controles de acceso a las aplicaciones y la información, como controles de lectura, escritura, modificación de archivos, y carpetas; o el aislamiento de la información confidencial, por ejemplo, en sistemas con cifrado integrado.
- Establecimiento de una política para trabajo en movilidad, que incluya las comunicaciones móviles y el teletrabajo.

Actividades

Plantee un hipotético registro de usuarios y de los servicios a los que acceden, en una empresa con 10 trabajadores, 3 departamentos, y 5 servicios entregados por los equipos informáticos (acceso a internet, correo electrónico, impresión, base de datos de contabilidad, y base de datos de clientes).