



El Lugar de Trabajo

El lugar de trabajo es el lugar en el que realizamos nuestras labores cotidianas, en donde requerimos acceder a diversos sistemas y manipular diferentes tipos de información. Como consecuencia directa, debemos tener en cuenta que el lugar de trabajo es un **punto clave** visto desde la **seguridad de la información**.

Por ello, es necesario que apliquemos un conjunto de medidas de seguridad que nos garanticen que la información, tanto impresa, como en formato electrónico, está correctamente protegida.

1. Gestión de la documentación

Habitualmente, cuando pensamos en un lugar de trabajo estándar, nos viene a la cabeza un lugar en una oficina, con una mesa de trabajo, archiveros, etc. Sin embargo, muchos de nosotros trabajamos también, de manera parcial o total, en lugares de trabajo ubicados en entornos abiertos. Este tipo de lugares son susceptibles a dañar la información impresa.

Para evitar esto, debemos tomar una serie de sencillas medidas preventivas:

-  **Almacenar o guardar nuestra información en una ubicación adecuada.** Evitar su cercanía a sistemas de refrigeración, canalizaciones de agua o instalaciones que puedan afectar al papel.
-  **Emplear elementos adecuados para almacenar la información impresa,** como por ejemplo armarios y archiveros que dispongan de dispositivos de cierre, o cajas fuertes o armarios ignífugos en caso necesario.
-  **Destruir la documentación de manera segura.** Dependiendo del volumen de papel, podemos utilizar destructoras de papel convencionales o subcontratar la retirada y destrucción a un proveedor. En este último caso no debemos olvidar firmar el acuerdo de confidencialidad pertinente y solicitar los certificados de destrucción segura.



2. Contraseñas seguras

Debemos hacer uso de una política de contraseñas seguras, que defina al menos los siguientes aspectos:

-  La longitud mínima de caracteres.
-  Utilizar siempre minúsculas, mayúsculas, números y símbolos.
-  Cambiar de manera periódica la contraseña.

Una contraseña segura sería una clave de acceso con longitud mínima de 12 caracteres, compuesta por una combinación de letras mayúsculas, minúsculas, números y símbolos; por ejemplo: yj4.0c2_3ZY@

También debemos recordar que las contraseñas son personales, secretas e intransferibles. No debemos apuntarlas en post-its, libretas, documentos de texto o cualquier otro medio que permita acceder fácilmente a ellas. En el caso de que necesitemos que un compañero acceda a la información que administramos, podemos poner en funcionamiento medidas alternativas, como utilizar repositorios compartidos o informar a los usuarios de un segundo contacto.

3. Métodos de autenticación

Un método de autenticación es la técnica o el procedimiento que un sistema utiliza para verificar que un usuario es quien dice ser.

Para llevar a cabo dicha verificación, existen distintos métodos:

-  Los basados en algo que sabemos, el caso más evidente es usar una contraseña.
-  Los basados en algo que poseemos, por ejemplo, una tarjeta de acceso magnética.
-  Los basados en una característica física personal, por ejemplo, huella dactilar, retina o rasgos faciales.

Cuantos más métodos combinemos para el acceso a un sistema, más robusto y fiable será éste. Es decir, más difícil será burlarlo o romperlo. Un ejemplo de método de autenticación combinado sería establecer un control de acceso al sistema en el que un usuario deba hacer uso de una tarjeta magnética (algo que tiene) y, adicionalmente, deba introducir un pin o contraseña (algo que sabe).



4. Política de escritorio limpio

A diario trabajamos con gran cantidad de documentación, que es habitual que esté distribuida encima del escritorio, para mayor comodidad o porque es necesaria para las tareas diarias.

Sin embargo, al acabar la jornada debemos guardar la documentación que se encuentre a la vista (información de la institución, alumnos, profesores, trabajadores, proveedores, etc.). Esto es especialmente importante si trabajamos en entornos compartidos con otros departamentos, o incluso públicos (área administrativa, área secretarial, por ejemplo). De esta manera evitaremos miradas indiscretas que puedan derivar en una fuga de información, además del robo de documentos que pueden contener información confidencial.

Una política de escritorio limpio requiere que:

-  El lugar de trabajo esté limpio y ordenado.
-  La documentación que no estemos utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando dejamos nuestro lugar de trabajo y al finalizar la jornada.
-  No haya usuarios ni contraseñas apuntadas en post-it o similares.

Además, aunque no sea una medida específica de escritorio limpio, si nos alejamos por un momento el lugar de trabajo, debemos bloquear nuestro equipo para evitar accesos no autorizados.

5. Ingeniería social

Los ataques de ingeniería social tienen como objetivo a cualquier personal, sin importar en el puesto que esté. A través de ellos una persona mal intencionada puede obtener información confidencial de las propias víctimas, o utilizar a ésta para acceder a otras personas de la institución de manera inadvertida.

Existen cuatro pilares de los ataques de ingeniería social, que permiten que en muchos casos éstos sean exitosos:

-  El deseo de ayudar a otras personas.
-  La confianza de que las personas actúan por buena voluntad.
-  El no querer decir que no a las peticiones de otras personas.
-  El deseo de ser halagado.





La mejor manera de entender lo que significa un ataque de ingeniería social es mediante un ejemplo: supongamos que un empleado del Departamento de Recursos Humanos sin responsabilidades relevantes recibe una llamada de una persona que le indica que le llama del departamento de informática, aunque en realidad se trata de una persona mal intencionada. Tras una breve conversación, la persona mal intencionada podría solicitar información sobre el equipo de cómputo, la política de actualizaciones, los programas instalados, o incluso solicitar su usuario y contraseña para realizar mantenimiento del equipo de cómputo de manera remota. A partir de este momento, la persona mal intencionada podría llevar a cabo acciones como intentar acceder a los sistemas institucionales, instalar un código malicioso, registrar todo lo escrito por el teclado, obtener datos de acceso a los sistemas.

Aunque parezca algo fruto de la casualidad, los ataques de ingeniería social se llevan a cabo de manera planificada, obteniendo información de múltiples fuentes, lo que permite simular un conocimiento similar al que tendría alguien que trabaje en la institución.

Uno de los medios más utilizados en la ingeniería social es el correo electrónico. Bajo cualquier pretexto o excusa invitan al usuario a enviarles información personal o de la institución, a hacer clic en algún enlace o al abrir un archivo adjunto infectado. El ataque por correo electrónico se realiza través de una cuenta falsa con características similares a las cuentas de correo personales o institucionales, para darle más credibilidad en caso de ser un ataque dirigido contra la misma. Por ejemplo, se envía un correo electrónico en el que se indica, que debido a una auditoría que se está llevando a cabo dentro de la institución, con un archivo adjunto infectado. Cualquier pretexto es bueno, para invitar al personal a ejecutar el archivo que se incluye en el correo electrónico.

Otra de las técnicas utilizadas y que podemos incluir dentro de este tipo de ataque a instituciones, es el uso de memorias USB «olvidadas» como ataque de ingeniería social. Consiste en dejar en lugares estratégicos USB con archivos infectados. Éstos están identificados con nombres atractivos como por ejemplo *Nomina*, *RenovacionContratos*, *auditoria_interna.exe* o similares, con el objetivo de atraer la curiosidad del personal y que éste ejecute el archivo.

Esto hace que este tipo de ataques sean los más difíciles de prevenir y, por lo tanto, los que mayor probabilidad tienen de éxito. Debemos estar alerta ante cualquier actividad o solicitud sospechosa. ¿Cuál es la mejor herramienta contra este tipo de ataques? **El sentido común.**





6. Fugas de información

La mayoría de las fugas de información que se producen en las instituciones tienen como origen el lugar de trabajo de la víctima. Pueden ser fruto tanto de actos malintencionados por parte de personal descontento como de errores al utilizar los sistemas con los que administramos la información.

Para evitar fugas de información, debemos ser muy cautelosos a la hora de usar el correo electrónico y las redes sociales. Por ejemplo, las aplicaciones para administrar el correo electrónico suelen tener la función de autocompletar la dirección del destino. Si no somos cautelosos, es posible que enviemos accidentalmente información confidencial a un destinatario inapropiado.

Por otro lado, en redes sociales profesionales es habitual que algunos usuarios incluyan información sobre alumnos o proyectos en los que están trabajando, proporcionando valiosa información que puede ser utilizada para organizar un ataque de ingeniería social entre otros.

Actualmente existen soluciones informáticas cuyo objetivo principal es reducir el riesgo de las fugas de información, sin embargo, debemos tener en cuenta que ninguna herramienta es capaz de sustituir al ya mencionado sentido común a la hora de administrar la información.

