El Puesto de Trabajo

El puesto de trabajo es el lugar en el que realizamos el trabajo diario. Como parte de las tareas cotidianas, cualquier usuario requiere acceder a diversos sistemas y manipular diferentes tipos de información. Como consecuencia directa, debemos tener en cuenta que el puesto de trabajo es un **punto clave** desde el punto de vista de la **seguridad de la información**.

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

1. Gestión de la documentación

Habitualmente, cuando pensamos en un puesto de trabajo estándar, nos viene a la cabeza un puesto de trabajo en una oficina, con una mesa de trabajo, cajoneras, etc.

Sin embargo, muchos de nosotros trabajamos también, de manera parcial o total, en puestos de trabajo ubicados en entornos susceptibles de dañar la información en soporte papel.

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 el papel**, como por ejemplo armarios y cajoneras 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 de las claves que utilicemos:

- La longitud mínima de las claves.
- La obligación de utilizar minúsculas, mayúsculas y símbolos.
- La periodicidad con la que se debe cambiar la contraseña.

Un ejemplo de contraseña segura podría ser una clave de acceso con una longitud mínima de 12 caracteres, compuesta por una combinación de letras mayúsculas, minúsculas, números y símbolos.

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 nuestras claves. En el caso de que necesitemos que un compañero acceda a información que gestionamos, 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 la utilización de contraseñas.
- Los basados en algo que poseemos, como por ejemplo, una tarjeta de acceso magnética.
- Los basados en una característica física de la persona, como por ejemplo, su 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 falsearlo y romperlo.

Un ejemplo de método de autenticación combinado sería establecer un control de acceso al sistema en el que el 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 mesas limpias

A diario trabajamos con gran cantidad de documentación, que es habitual que esté distribuida encima de la mesa, 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 organización, usuarios, proveedores, etc.). Esto es especialmente importante si trabajamos en entornos compartidos con otras organizaciones, o incluso públicos (atención al usuario, 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 mesas limpias requiere que:

- El puesto de trabajo esté limpio y ordenado.
- La documentación que no estemos utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando dejamos nuestro puesto 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 mesas limpias, si abandonamos el puesto de trabajo, debemos bloquear nuestro equipo para evitar accesos no autorizados.

5. Ingeniería social

Los ataques de ingeniería social tienen como objetivo a cualquier empleado, sin importar en el puesto que esté. A través de ellos un atacante puede obtener información confidencial de las propias víctimas, o utilizar a ésta para acceder a otras personas de la organización de manera inadvertida.

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

1) El deseo de ayudar a otras personas.
2) La confianza de que las personas actúan por buena voluntad.
3) El no querer decir que no a las peticiones de otras personas.
4) El deseo de ser halagado.

La mejor manera de entender lo que significa un ataque de ingeniería social es mediante un ejemplo, que vemos a continuación.

Supongamos que un empleado del Departamento de RRHH sin responsabilidades relevantes recibe una llamada de una persona que le indica que le llama del departamento de informática, aunque en realidad se trata del atacante. Tras una breve conversación, el atacante puede solicitarle información sobre su equipo, la política de actualizaciones, los programas instalados, o incluso solicitarle su usuario y contraseña para realizar mantenimiento del equipo. A partir de este momento, el atacante podría llevar a cabo acciones como intentar acceder a los sistemas corporativos, instalar un troyano o registrar todas las pulsaciones del teclado.

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 trabajase en la organización.

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 organización, a hacer clic en algún enlace o a abrir un fichero infectado adjunto. El ataque por correo electrónico se realiza través de una cuenta falsa con características similares a las cuentas de correo de la organización, 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 organización en ese momento. Cualquier pretexto es bueno, para invitar al empleado 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 organizaciones, es el uso de memorias USB «extraviadas» como ataque de ingeniería

social. Consiste en dejar en lugares estratégicos USB con ficheros infectados. Éstos están identificados con nombres atractivos como por ejemplo *NóminasFeb2014*, *auditoria_interna.exe* o similares, con el objetivo de atraer la curiosidad del empleado y que éstos ejecuten el fichero.

Esto hace que este tipo de ataques sean los más difíciles de prevenir y, por lo tanto, los que mayor probabilidad de éxito tienen. 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 organizaciones tienen como origen el puesto de un empleado. Pueden ser fruto tanto de actos malintencionados por parte de empleados descontentos como de errores al utilizar los sistemas con los que gestionamos 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 gestionar 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 destino inapropiado.

Por otro lado, en redes sociales profesionales es habitual que algunos usuarios incluyan información sobre usuarios 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 gestionar la información.