PROTECCIÓN DEL PUESTO DE TRABAJO

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

A menudo invertimos una gran cantidad de recursos económicos en la implantación de medidas de seguridad para evitar fugas o pérdidas de información, como la mejora de la sala de servidores, la renovación de las aplicaciones corporativas, la implantación de sistemas de detección de intrusos mediante controles de acceso físico a las instalaciones, la replicación de datos entre distintas sedes, etc.

Sin embargo, es bastante habitual que se pase por alto un elemento vital en el proceso de implantación de medidas de seguridad: el **puesto de trabajo**. Gran parte de los incidentes de seguridad en la empresa se generan dentro de la propia organización, tanto de manera intencionada como accidental. Debemos tener en cuenta que un usuario no necesita realizar complejos ataques para acceder a la información: ha sido autorizado para utilizarla y la tiene a su alcance.

El concepto de **puesto de trabajo** va más allá de la ubicación «física» donde el usuario desempeña sus funciones diarias. Dentro de este entorno podemos identificar elementos con relación directa con la seguridad de la información: equipos de trabajo, *smartphones*, tabletas, dispositivos de almacenamiento extraíbles, impresoras, escáneres, documentación, archivadores, etc.

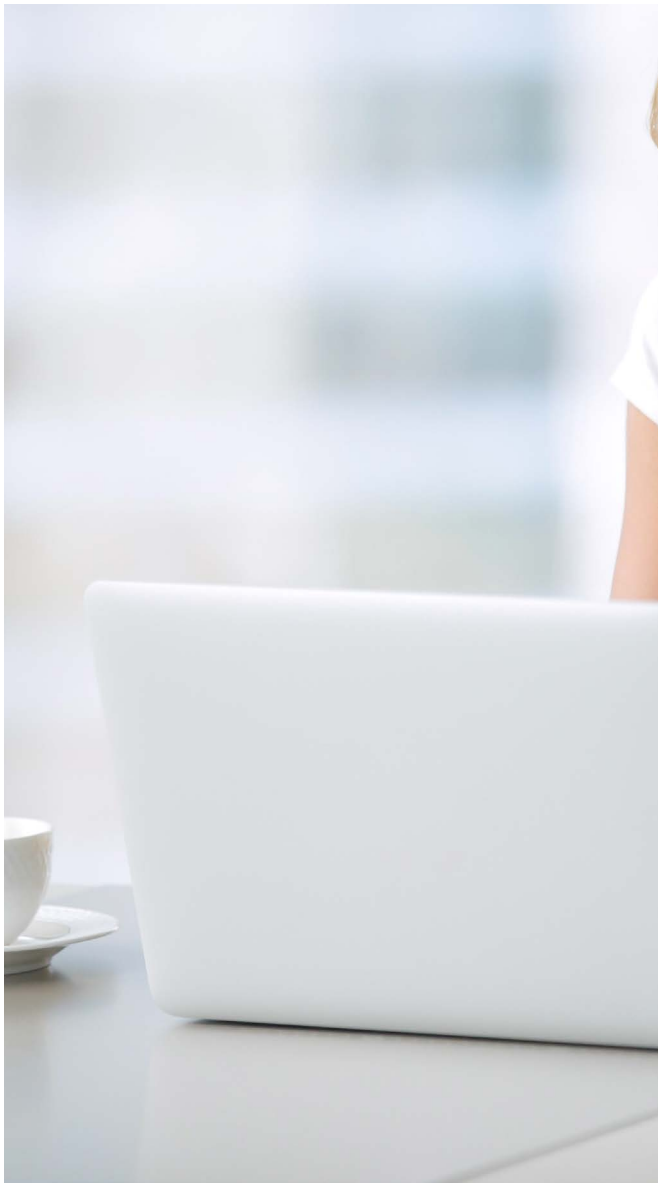
Debemos tener precauciones especiales con el uso de dispositivos personales en el ámbito corporativo, lo que se conoce como *BYOD (Bring Your Own Device).*

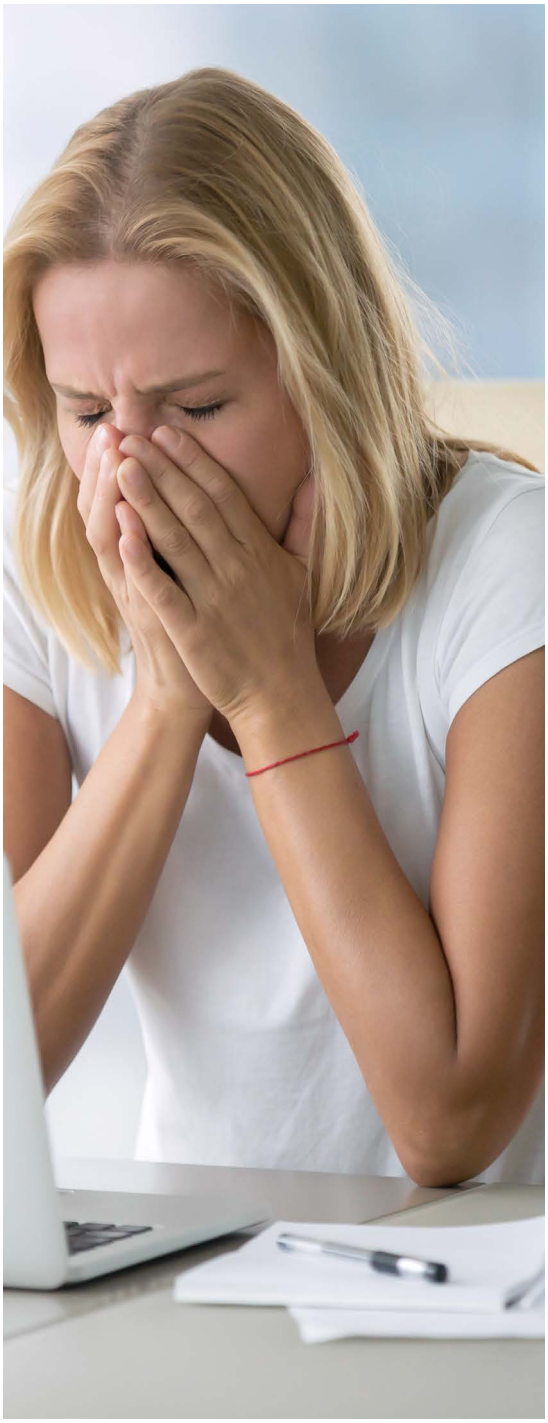
Cada puesto de trabajo está adecuado a un perfil profesional y por tanto las amenazas a las que está expuesto son distintas según las funciones que desempeñe el trabajador dentro de la organización. Un operario de planta no tendrá el mismo nivel de acceso que el director financiero, ni dispondrá de los mismos medios. Además de implantar medidas de seguridad transversales a toda la organización, debemos atender a la **casuística de cada puesto de trabajo** para evaluar la necesidad de medidas de seguridad adicionales a cada perfil de trabajo.

Mitigar los riesgos del puesto de trabajo de una forma significativa no requiere la implantación de grandes medidas técnicas, sino establecer una **cultura de la seguridad de la información** [1] y poner en marcha medidas técnicas que son en la mayor parte de los casos sencillas.

2. ESCENARIOS Y EJEMPLOS DE RIESGO

Fuga de datos, pérdida de información confidencial, infecciones por *malware* o deslices en el uso del correo electrónico o las redes sociales son algunos riesgos a los que nos enfrentamos en el puesto de trabajo.





2.1. ESCENARIOS DE RIESGO

Cuando hablamos de escenarios de riesgo en el puesto de trabajo podemos encontrarnos con situaciones como las siguientes:

	No siempre una fuga o pérdida de datos se produce por un usuario malintencionado. A menudo se trata de usuarios que llevan a cabo prácticas no recomendables, que pueden ser aprovechadas por un atacante externo o interno, o simplemente llevar asociadas consecuencias indeseables.
	Muchas fugas de información que se producen en las empresas 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.
	Las aplicaciones para gestionar el correo electrónico suelen tener la función de autocompletar la dirección del destino. Un descuido puede provocar el envío accidental de información confidencial a un destinatario inadecuado.
	En redes sociales profesionales es habitual que algunos usuarios incluyan información sobre clientes 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 sentido común a la hora de gestionar la información.
	Un puesto de trabajo sin las correctas medidas de seguridad, aunque no disponga de acceso a información, puede ser la puerta de entrada a la red corporativa para un atacante.
	Aunque el robo o fuga de información es una de las principales amenazas, existen otras como la infección por virus, que puede llevar a interrupción de las actividades de la empresa y a la pérdida de información.
	La ingeniería social tiene como objetivo a los empleados de nuestra organización y permite obtener información confidencial de las víctimas y su organización. Debemos aprender a detectar los ataques de ingeniería social.
	El *malware*/virus no puede discriminar entre «objetivos» y «accidentes». Aunque nuestra empresa no sea objetivo directo de los atacantes, el *malware* que existe en Internet puede hacer que nuestros sistemas estén afectados sólo porque tienen ciertas vulnerabilidades.
	La extensión del lugar de trabajo a los dispositivos portátiles ha llevado a la utilización en muchos casos de los dispositivos personales como si fuesen profesionales. No obstante, éstos carecen a menudo de los controles y protecciones de un entorno corporativo.
	La información no es el único elemento valioso del puesto de trabajo. La capacidad de procesamiento o la conexión a Internet son características que pueden ser explotadas como vías para cometer ataques sobre otras organizaciones.

Ilustración 1
Escenarios de riesgo

2.2. EJEMPLOS DE RIESGO

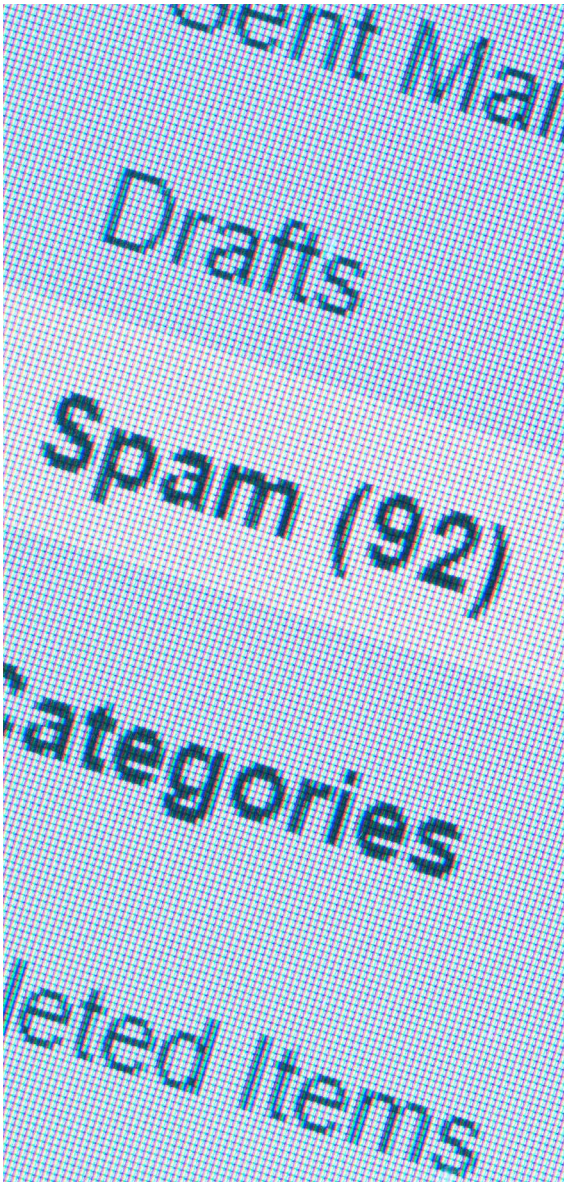
Veamos algunos ejemplos de riesgo que nos podemos encontrar, de forma muy habitual, en nuestros puestos de trabajo:

- Debido a la falta de gestión adecuada en los permisos de administración en los equipos de trabajo, un usuario instala en su equipo una aplicación de P2P[1]. Al ponerla en marcha, comparte por error con la red un directorio de su equipo donde almacena información corporativa: política salarial, datos personales de los usuarios, partes de baja, etc.
- Un usuario detiene el antivirus corporativo porque según indica le impide trabajar. Más tarde, ejecuta un archivo que le llega por correo electrónico, infectando su equipo y toda la red de la empresa.
- Un usuario tira a la papelera los *curriculum vitae* del último proceso de selección, que acaban en un contenedor y son recogidos por una tercera persona. Esto podría derivar en una sanción para la empresa de varios miles de euros según la legislación vigente de protección de datos de carácter personal **[2]**.
- Un **usuario descontento** coge de la impresora información sobre tarifas y márgenes de venta de la empresa. Esa tarde, cuando no queda nadie trabajando, los publica en Internet utilizando el ordenador de alguien que se ha dejado la sesión sin bloquear.
- Alguien accede a los recursos corporativos a través de la conexión remota en horario no laboral y elimina información de varios clientes. Debido a que se utilizan usuarios genéricos para los accesos remotos, no es posible identificar a la persona responsable, ni si se trata de un usuario o un atacante externo.
- Un usuario copia en un *pendrive* documentación confidencial de la oferta para concursar en una obra para un conocido edificio público, con la intención de continuar trabajando en casa. El *pendrive* se pierde en el autobús, con información de planos, oferta económica, etc. Alguien lo encuentra y los planos terminan publicándose en prensa.
- Un usuario instala en su equipo una versión «pirata» de un programa de edición de video. Éste lleva asociado un ejecutable para la generación del número de serie. Aunque el antivirus le alerta del peligro, lo desactiva temporalmente para continuar. Al ejecutarlo, instala en su equipo un control remoto

1 P2P (del inglés *Peer-To-Peer*) es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Algunos ejemplos son los sistemas de intercambio y búsqueda de ficheros: BitTorrent. Emule o eDonkey2000. También utilizan este modelo Skype y Bitcoin.

que es utilizado por un atacante para extenderse a otros equipos y realizar ataques de denegación de servicio contra grandes organizaciones.

- Un responsable de área vende su portátil personal en una tienda online de productos de segunda mano. Aunque no se trata de un elemento corporativo, era habitual que lo utilizase para gestionar y guardar información corporativa. Mediante un sencillo programa de recuperación, el comprador recupera la información y la publica en Internet.
- Un servidor de correo electrónico que está en una empresa no dispone de las medidas de seguridad adecuadas y termina siendo comprometido y utilizado por los atacantes para campañas de *spam*[2], ***phishing***[3], etc. Este hecho, además del daño a terceros que puede causar y de las implicaciones legales que pueda tener por formar parte de la cadena del delito, nos incluirá en muchos casos en la mayoría de listas negras de los sistemas antispam. Esta situación provoca que nuestro correo legítimo sea considerado como *spam*, lo que nos creará un trastorno al impedir comunicarnos con terceros de manera habitual.



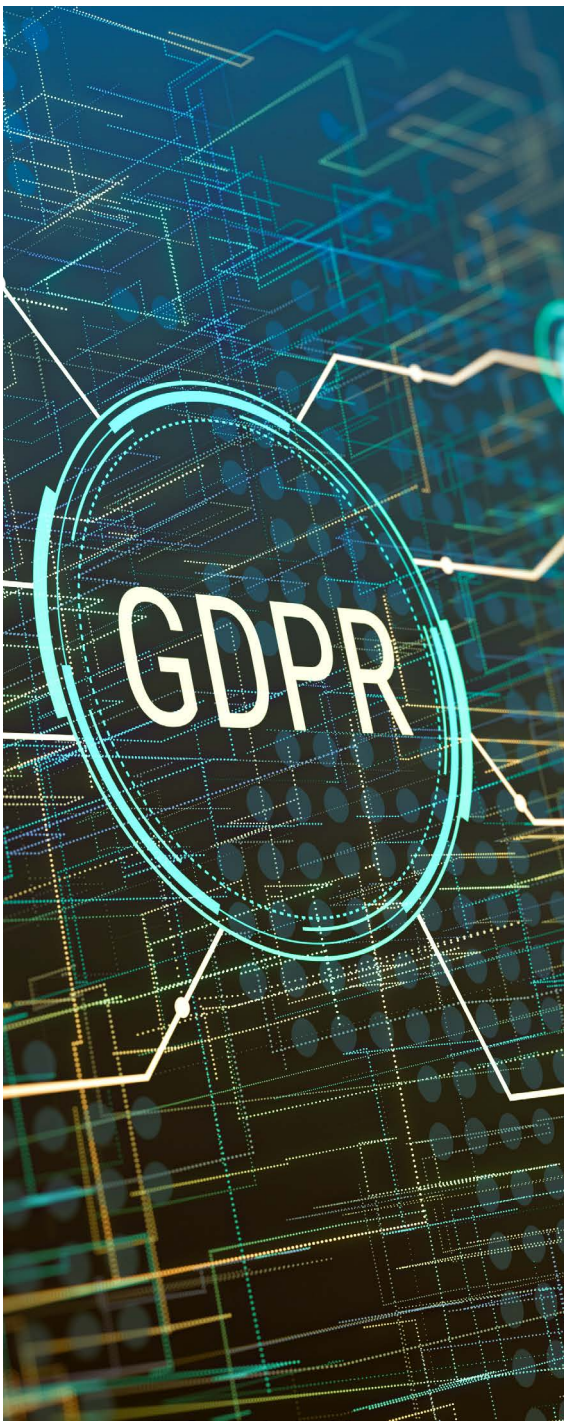
2 Se denomina ***spam*** a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor.

3 ***Phishing*** es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

3. MEDIDAS DE SEGURIDAD

Las medidas de seguridad que podemos aplicar para proteger el puesto de trabajo son innumerables y de diferente grado de complejidad. Sin embargo, existe un conjunto reducido de medidas con un coste de implantación y mantenimiento muy bajo, que nos aportarán una mejora sustancial en nuestro nivel de seguridad.

Así, nos vamos a centrar en aquellas medidas que se traducen en mayores beneficios sobre la seguridad del puesto de trabajo. Algunas de ellas son requisitos de la legislación de datos de carácter personal (para más detalles, puede consultarse el dosier temático de Cumplimiento legal **[3]**) y otras son recomendaciones establecidas por códigos de buenas prácticas en seguridad de la información.



3.1. MEDIDAS DE CARÁCTER ORGANIZATIVO

La primera y fundamental medida de carácter organizativo es implantar una **política de seguridad interna** de la organización, que transmita a los empleados las obligaciones y buenas prácticas en relación con la seguridad de la información.

Las medidas planteadas en la política y normativas de seguridad deben trasladarse a los usuarios de la manera adecuada. La información debe estar disponible para los usuarios, recordarse mediante comunicaciones de manera periódica, y firmarse al comienzo de la relación laboral.

Ni la política ni las normativas deben trasladarse al usuario como un descargo de responsabilidad de la empresa o como un medio con el fin exclusivo de adoptar medidas disciplinarias. Las principales consecuencias de una fuga o pérdida de información por negligencia son siempre para la empresa.

Estas medidas deben tener en cuenta los siguientes puntos:

1 **La obligación de mantener confidencialidad** en relación con cualquier información a la que el empleado tenga acceso durante su trabajo en la empresa, de manera indefinida.

Esto debe aplicarse tanto a información confidencial como a datos de carácter personal, y debe ir acompañado de un compromiso de confidencialidad.

No se debe publicar información corporativa sobre clientes o proyectos en las redes sociales.

2 **La obligación de notificar de cualquier incidente** de seguridad relacionado con el puesto de trabajo, ya sea en la propia empresa o en el exterior.

Específicamente, el empleado debe notificar de:

- alertas de virus/*malware* generadas por el antivirus;
- llamadas sospechosas recibidas pidiendo información sensible;
- correos electrónicos que contengan virus;
- pérdida de dispositivos móviles (portátiles, *smartphones* o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);
- cualquier actividad sospechosa que pueda detectar en su puesto de trabajo;
- borrado accidental de ficheros;
- alteración accidental de datos o registros en las aplicaciones con información crítica.

- comportamientos anómalos de los sistemas de información;
- hallazgo de información en ubicaciones no designadas para ello;
- evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes,...);
- evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros.

3 La prohibición de publicar o compartir contraseñas. Las claves son elementos confidenciales y deben permanecer en secreto, ya que sólo así se puede garantizar la confidencialidad y trazabilidad de las acciones. Por tanto, no deben compartirse ni apuntarse en documentos ni en cualquier otro tipo de soporte.

La necesidad de acceder al equipo de un compañero para poder seguir con su trabajo cuando éste se encuentre ausente puede solucionarse con medidas alternativas:

- utilización de repositorios de información departamentales compartidos;
- prohibición de almacenar información en los equipos personales.

4 La obligación de bloquear la sesión al ausentarse del puesto de trabajo. Dejar un equipo sin protección durante el almuerzo, la comida, o incluso por la noche, es equivalente a no utilizar contraseña de acceso.

Debe enseñarse al usuario cómo puede bloquear su equipo de manera sencilla. Asimismo, debemos indicar al empleado que debe apagar su equipo al acabar la jornada laboral.

Además, deberemos establecer las políticas de seguridad técnicas adecuadas para que el bloqueo del puesto de trabajo se realice de manera automática tras un tiempo prudencial sin actividad en el equipo. También se pueden establecer medidas para que se apaguen automáticamente los equipos cuando finalice la jornada laboral.

5 Limitación en el uso de servicios de almacenamiento online. Este tipo de servicios, denominados habitualmente «*cloud*», son muy útiles para almacenar copias de la información corporativa, facilitar el trabajo en equipo y permitir el trabajo desde fuera de la oficina.

Para hacer un uso seguro de este tipo de servicios, debemos tomar una serie de precauciones, como son:

- dar de alta perfiles de usuarios exclusivos corporativos para el manejo de información corporativa;
- prohibir utilizar el perfil de usuario corporativo para uso privado;
- utilizar algún mecanismo de cifrado antes de subir la información de la organización, siempre que no se trate de información pública;
- que el uso de este tipo de servicios venga autorizado por el personal de informática;
- debemos hacer uso de entornos *cloud* que estén autorizados por la organización;
- no utilizar estos servicios como repositorios permanentes sino temporales.

6 Realizar un uso adecuado de los medios de almacenamiento extraíble

. La utilización de *pendrives* y discos duros externos es una práctica habitual que conlleva un alto riesgo de pérdida y robo de información.

Existen diversos mecanismos para reducir la necesidad de este tipo de soportes y garantizar así la seguridad de la información. Podemos implementar alternativas a este tipo de dispositivos, como:

- la utilización de repositorios comunes para el intercambio de información;
- implantar la posibilidad de acceso remoto para el trabajo remoto desde fuera de la oficina;
- hacer uso de los servicios de almacenamiento online.

No obstante, en caso de que sea necesaria su utilización, debemos transmitir al empleado la necesidad de aplicar ciertas **precauciones**, como:

- utilizar mecanismos de cifrado que impidan el acceso a la información en caso de pérdida;
- utilizar dispositivos con mecanismo de acceso biométrico (huella digital) o protegido por contraseña;
- deshabilitar por defecto los puertos USB y habilitarlos en aquel personal que necesite dicha funcionalidad de manera periódica o gestione ficheros de gran tamaño: comercial, marketing, etc..

En la medida de lo posible, debemos evitar la aplicación de restricciones de manera masiva, y hacerla de manera gradual, para no dificultar el trabajo de los usuarios.

7 Prohibición de la alteración de la configuración del equipo y la instalación de aplicaciones no autorizadas.

El usuario final debe ser disuadido de modificar los dispositivos corporativos para instalar nuevas aplicaciones **[4]** o modificar la configuración del sistema. Aunque en los ordenadores de sobremesa esta medida es sencilla de aplicar, puede ser más difícil aplicarla en *smartphones*, tabletas e incluso portátiles.

En caso de ser necesaria la instalación de una aplicación o modificar la configuración original del equipo, ésta debe ser solicitada al personal de informática.

8 La obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral (Política de mesas limpias).

Toda la documentación que se haya gestionado durante el día debe guardarse de manera adecuada durante ausencias prolongadas.

Esto es especialmente importante si trabajamos en entornos compartidos con otras empresas, o incluso públicos (atención al cliente, 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.

9 La obligación de destruir la documentación mediante mecanismos seguros.

Debemos poner a disposición de los usuarios destructoras de papel para la destrucción de aquella documentación sensible obsoleta o que sea innecesaria.

Si hemos contratado un servicio de destrucción segura bajo demanda o mediante contenedores de reciclaje, debemos notifi-

car a los empleados de su existencia y obligación de uso.

Por otro lado, los empleados deben conocer los riesgos asociados a la utilización de papeleras comunes para documentos sensibles, como datos personales, información financiera, etc.

10 La obligación de no abandonar documentación en las impresoras o escáneres.

Es frecuente que un usuario envíe un documento a la impresora y lo recoja más tarde, o que lo imprima a través de la impresora de otro departamento, por cuestiones técnicas, mayor calidad o funcionalidades especiales (impresión en color, tamaño A3, etc.)

Durante ese tiempo la documentación permanece a disposición de otros usuarios, que pueden recogerla accidental o intencionadamente.

11 Normativa de utilización de Internet y el correo electrónico corporativo.

Debemos informar a los usuarios de las normas que regulan las condiciones y circunstancias en que puede utilizarse Internet y el correo corporativo, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

Debemos concienciar a los empleados sobre su uso responsable y, que debe ser utilizado únicamente para la actividad laboral. Si en nuestra empresa existe algún sistema de registro (proxy) que registre los accesos a Internet, debemos informar de éste al empleado.

12 Normativa de utilización de dispositivos personales o BYOD

(*Bring Your Own Device*). En la actualidad, es común que los empleados utilicen y conecten sus dispositivos personales (portátiles) **[5]**, *smartphones*, tabletas) a las redes corporativas desde su casa, la propia oficina o cualquier otro lugar, permitiéndose el uso «mixto» de estos dispositivos con los de uso corporativo.

El uso corporativo de estos dispositivos puede suponer riesgos importantes para la seguridad que hay que tener en cuenta. La principal medida de seguridad es la de involucrar y concienciar al usuario del correcto uso de estos dispositivos.

Los usuarios deben saber que aquellos dispositivos personales utilizados para acceder a recursos corporativos pueden requerir el uso de configuraciones de seguridad específicas y adaptarse a medidas de seguridad dictadas por la organización.

3.2. MEDIDAS DE CARÁCTER TÉCNICO

Las medidas organizativas vistas anteriormente deben complementarse con medidas técnicas. Éstas mejoran la eficacia, dificultan la realización de acciones dañinas e impiden la violación de las medidas organizativas.

Siempre que sea posible y adecuado, deben aplicarse las siguientes medidas, de coste muy reducido.

1 Implantar una política de contraseñas robusta a nivel del sistema, tanto para el acceso al sistema operativo como a las aplicaciones. Esto evita que algunos usuarios escojan claves demasiado sencillas o repitan la misma clave durante mucho tiempo.

Esta política debe contemplar los siguientes criterios:

- complejidad de contraseñas: número mínimo de caracteres, obligación de usar combinaciones de caracteres especiales y alfanuméricos, etc.;
- obligación de un cambio periódico;
- bloqueo del usuario por intentos de acceso fallido reiterado;
- cambio de la clave inicial forzado.

Una **recomendación de política de claves** podría ser la siguiente:

- longitud mínima de 8 caracteres;
- que contenga al menos un número, una mayúscula y una minúscula;
- que no contenga tres letras consecutivas del nombre de usuario;
- caducidad (cambio obligatorio) de seis meses;
- bloqueo del usuario tras cinco intentos de acceso fallidos;
- cambio obligatorio de la clave inicial.

2 **Implantar y configurar un antivirus** para todos los equipos de la empresa, incluyendo los dispositivos móviles. Entre otros aspectos, debemos tener en cuenta los siguientes elementos:

- el antivirus debe actualizarse de manera automática;
- aunque la mayoría de antivirus disponen de análisis en tiempo real, es recomendable realizar y planificar análisis periódicos;
- no debe ser posible desactivar el antivirus por el usuario final;

» si es posible, que contenga funcionalidades de análisis de páginas web.

3

Configurar los sistemas para la **actualización automática** del sistema operativo y las aplicaciones.

Los principales sistemas operativos y las aplicaciones más utilizadas (navegadores, suites de ofimática y programas de lectura de PDF) se actualizan periódicamente, corrigiendo problemas de seguridad e incorporando nuevas funcionalidades. Por tanto:

» cuando sea técnicamente posible, debemos configurar los sistemas para que las actualizaciones se instalen de manera automática en un horario en el que no afecten de manera grave al trabajo de los usuarios;

» si no es posible, debemos aplicarlas manualmente por el personal técnico.

4

Limitar la utilización de usuarios genéricos. Los usuarios genéricos impiden la posibilidad de llevar la trazabilidad de las acciones realizadas, además de que dificultan saber si puede haber una persona no autorizada utilizando un sistema.

Por ejemplo, si varios usuarios utilizan un mismo equipo con el usuario «personal», es imposible saber cuál de ellos ha accedido en un momento concreto. Además, cuando algo se modifica en un entorno compartido, es más normal atribuirlo a otro usuario autorizado, en lugar de a un intruso. Por ello, debemos:

» evitar los usuarios genéricos para las tareas cotidianas;

» utilizar usuarios genéricos únicamente cuando sea imprescindible. Por ejemplo, usuarios del funcionamiento interno de los sistemas o usuarios en portales web de consulta.

5

Limitar los permisos de administración. Un usuario que tiene en su equipo local privilegios de administración tiene múltiples problemas:

» si abre un virus, éste infectará su equipo y será difícil eliminarlo;

» puede instalar y desinstalar programas. Esto incluye la instalación de software no legítimo o la eliminación de restricciones en el funcionamiento de su equipo;

» puede desactivar el antivirus o incluso desinstalarlo.

Por tanto, debemos configurar los equipos de modo que:

- los usuarios habituales no tengan permisos de administración;
- el usuario «Administrador» o con privilegios avanzados debe estar en posesión del personal técnico especializado y ser utilizado únicamente para tareas de administración, tales como solucionar problemas técnicos o instalar, actualizar o desinstalar aplicaciones.

6 Configurar el bloqueo de sesión por inactividad en sistemas y aplicaciones.

Aunque el acceso a un equipo se realice con contraseña, si la sesión permanece abierta en aquellos momentos en los que el usuario no está trabajando con el equipo, la medida pierde toda su eficacia.

Los equipos deben ser configurados para que, tras un periodo breve de tiempo, se bloqueen automáticamente y requieran la clave de acceso para su desbloqueo.

Se recomienda que este tiempo no sea superior a 5 minutos.

7 Restringir los puertos USB a puestos determinados

Los *pendrives* se caracterizan por:

- ser elementos de poco tamaño que pueden sacarse fácilmente de una organización;
- su reducido tamaño los hace muy proclives a ser perdidos;
- a menudo, la información que contienen no es borrada una vez ha sido transportada;
- la conexión de un USB a un equipo se hace en muchas ocasiones sin pensar sobre su origen.

Por tanto, debemos:

- restringir el uso de USB a aquellos usuarios que lo necesiten para su trabajo;
- proporcionar a los usuarios herramientas para el cifrado de la información cuando ésta se transporte mediante USB;
- utilizar dispositivos con mecanismo de acceso biométrico (huella digital) o protegido por contraseña;
- aplicar herramientas de borrado seguro de manera periódica a los USB;
- poner en marcha herramientas alternativas para el acceso a la información

como la habilitación de repositorios comunes de trabajo, o el uso de almacenamientos en la nube.

Debemos tener en cuenta que una restricción excesiva en la gestión de estos dispositivos puede generar cierta resistencia por parte de los usuarios, ya que en muchos casos los sistemas de almacenamiento mediante USB ofrecen muchas ventajas en cuanto a la productividad y facilidad para los usuarios, como por ejemplo para llevar una presentación comercial a un cliente o para continuar con un trabajo en otro equipo.

Se hace más necesario concienciar al empleado sobre las medidas que debe adoptar en este sentido. En general, debe considerarse restringir estos dispositivos, en determinados equipos que contienen o pueden acceder a información crítica o confidencial, (por ejemplo servidores, maquinas con operaciones críticas,...), o determinados usuarios que por su actividad no va a requerir de su uso. Es recomendable buscar un equilibrio entre finalidad y seguridad.

Estas restricciones podrían aplicarse también a otro tipo de interfaces como CD, DVD, tarjetas de almacenamiento de SD, etc.

8 Adquirir destructoras de documentación. Debemos adquirir dispositivos que nos permitan destruir la documentación sensible que no sea necesaria: propuestas a clientes, datos personales, tarifas, currículos recibidos, etc.

En función del número de usuarios y el volumen de información que se gestione, necesitaremos más o menos dispositivos de este tipo.

Como medida alternativa, se puede optar por contratar un servicio de destrucción de información a una empresa especializada, exigiendo un certificado de destrucción que garantice la imposibilidad de su recuperación.

En este caso, en función del volumen de documentación que manejemos, para la destrucción podemos optar por la recogida de la documentación bajo demanda, o la instalación de contenedores de reciclaje propiedad del proveedor, cuyo contenido es recogido y destruido de manera regular.

Aunque siempre es recomendable establecer un procedimiento de destrucción de dispositivos de almacenamiento, es conveniente también disponer de herramientas de destrucción y borrado seguro de estos soportes (USB, Discos Duros, etc.).

9

Limitar la navegación a páginas **de ciertos contenidos**. El acceso a determinados sitios web puede conducir a la infección por virus, tener repercusiones legales o afectar a la imagen de la empresa.

Es recomendable que implantemos medidas que bloqueen el acceso a:

- sitios web considerados contrarios a la legislación vigente;
- sitios web con contenido «inadecuado»;
- plataformas de intercambio de archivos que pueden ser la fuente de virus e infecciones.

10

Controlar y prohibir el acceso remoto hacia la propia organización. Existen herramientas que haciendo uso del protocolo HTTPS permiten el acceso no controlado a equipos de usuarios finales.

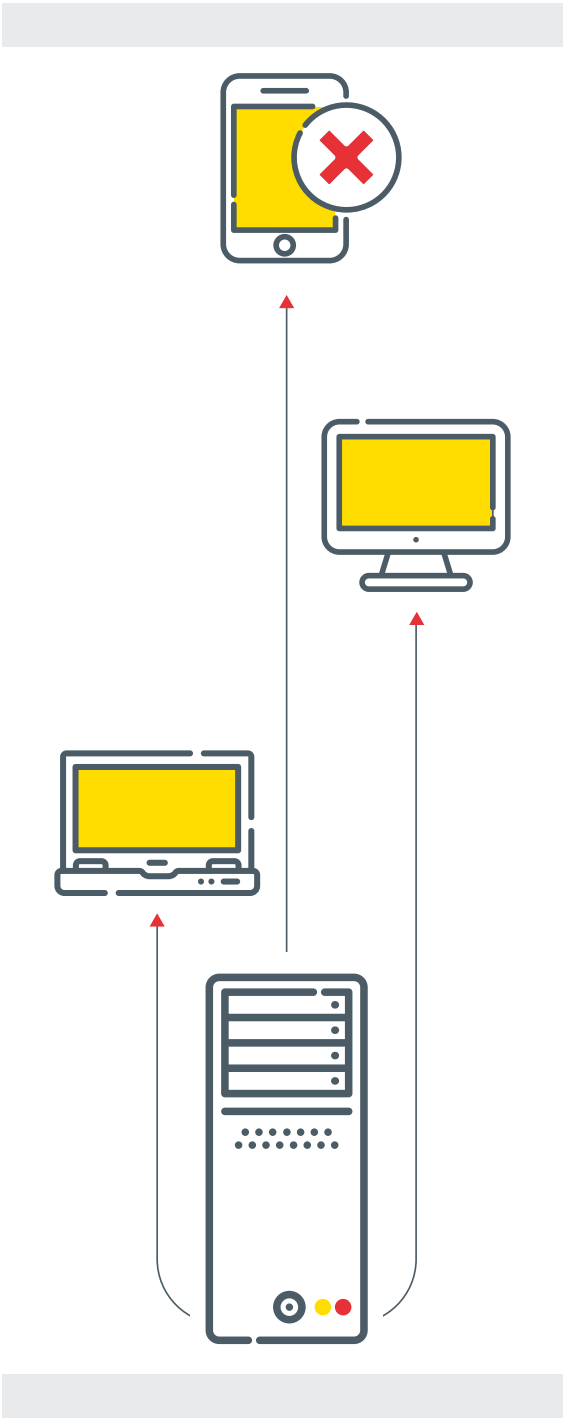
La utilización de este tipo de herramientas puede suponer el acceso incontrolado desde el exterior a nuestra organización. Se recomienda el filtrado de este tipo de aplicaciones y sistemas En su lugar es posible la instalación sistemas de acceso remoto del estilo de VPN que garanticen la seguridad y trazabilidad de todos los accesos remotos.

11

Habilitar mecanismos de seguridad en la impresión de documentos. Si el tamaño o la disposición de nuestra organización facilita que los documentos residan en la impresora durante un tiempo hasta que son recogidos, se deben establecer mecanismos de seguridad, tales como el uso de tarjetas o códigos personales antes de la impresión.

12

Limitar el acceso a la red corporativa a los equipos que no estén debidamente protegidos. La conexión de determinados dispositivos a la red como *smartphones* personales, equipos de proveedores o portátiles de personal esporádico pueden implicar un serio riesgo de infección por virus, entre otras amenazas. Debemos prestar especial atención a la utilización de los *BYOD*, manteniendo una base de datos de estos dispositivos y los usuarios que los utilizan.



Antes de conectar cualquier equipo a la red interna, debemos asegurarnos que están configurados correctamente y que son seguros para nuestra organización, comprobando cuestiones como:

- que tiene instalado y actualizado un antivirus y que se realizan análisis periódicos;
- que tiene instaladas las principales actualizaciones del sistema operativo;
- que, salvo que sean necesarias, no dispone de herramientas utilizadas para la evaluación técnica de los sistemas o la identificación de vulnerabilidades.

Es imprescindible que la wifi esté debidamente configurada y securizada **[6]** para el caso en que la conexión a la red corporativa se realice a través de ella. Por ello debemos cifrar el canal mediante SSL para garantizar la seguridad de la información que se trasmita.

3.3. PROGRAMA DE FORMACIÓN Y CONCIENCIACIÓN

Hay una medida de seguridad por encima de todas las descritas anteriormente, que es la de la **involucración y concienciación** de los usuarios que hacen uso de los activos de la empresa en materia de ciberseguridad.

Deben llevarse a cabo programas periódicos de concienciación (como los indicados en el «Kit de Concienciación de INCIBE» **[7]**), que incidan sobre la importancia de las medidas incluidas dentro de la **política de seguridad interna** de la empresa para conseguir que los empleados las interioricen y acepten.

Se recomienda que la realización de sesiones de formación se realice de forma periódica, y que traten los principales elementos de la **política de seguridad interna**. Se debe realizar un seguimiento de las sesiones para evaluar el nivel de implantación de estos conceptos en el usuario, identificando los puntos débiles donde se debe incidir en próximas sesiones **[8]**.

Para su aplicación, pueden ponerse en marcha las siguientes iniciativas:

Ilustración 2
Iniciativas de concienciación

Podrás encontrar información más detallada sobre este aspecto en el apartado del portal Protege tu empresa - ¿Qué te interesa? «Desarrollar una cultura de seguridad» **[1]**.

3. REFERENCIAS

[Ref - 1]. **INCIBE, Desarrollar cultura en seguridad -** https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf

[Ref - 2]. **BOE, Protección de Datos de Carácter Personal -** https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2

[Ref - 3]. **INCIBE, Cumplimiento Legal -** https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf

[Ref - 4]. **INCIBE, «Normativa corporativa de uso de software legal» -** https://www.incibe.es/sites/default/files/contenidos/dosieres/proteccion-puesto-trabajo/proteccion-puesto-trabajo-normativa-corporativa-de-software-legal.pdf

[Ref - 5]. **INCIBE, «Normativa corporativa de portátiles» -** https://www.incibe.es/sites/default/files/contenidos/dosieres/proteccion-puesto-trabajo/proteccion-puesto-trabajo-normativa-corporativa-de-portatiles.pdf

[Ref - 6]. **INCIBE, Seguridad en redes wifi: una guía de aproximación para el empresario -** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

[Ref - 7]. **INCIBE, Kit de Concienciación -** https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[Ref - 8]. **INCIBE, «Checklist básico para la protección del puesto de trabajo» -** https://www.incibe.es/sites/default/files/contenidos/politicas/fichas/proteccion-puesto-trabajo.pdf


GOBIERNO
DE ESPAÑA
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD


protege
tuempresa