CIBERPROTECT

# MANUAL DE USUARIO

Los empleados son los encargados de gestionar, procesar, almacenar, modificar, transmitir y eliminar la información en una empresa. Son el engranaje principal para el buen funcionamiento, pero ¿conocen los riesgos en materia de seguridad?

Puede haber riesgos por desconocimiento y desinformación que sitúen a nuestra empresa en una situación crítica. Por eso ponemos a vuestro alcance este manual que incorpora múltiples acciones para mejorar la seguridad desde el corazón de su empresa, las personas.

CIBERPROTECT

## 1.- CONCIENCIACIÓN

Utiliza siempre los recursos que la empresa ha puesto a tu disposición y evita de los que no se haga copia y carezca de las medidas de seguridad adecuadas

Si vas a intercambiar información confidencial, es recomendable que utilices alguna herramienta para cifrar la información. Un fichero comprimido con contraseña puede ser suficiente

Evita utilizar USB para almacenar información confidencial ya que es fácil perderlos y que sean sustraídos o manipulados.

Hacer copias de seguridad periódicas de discos duros externos y USB

Utiliza el correo electrónico de forma segura y elimina o informa de todo correo sospechoso que recibas


No utilices wifi gratis del establecimiento al que vayas, suelen ser muy inseguras


Si tienes que trabajar desde fuera de la oficina, utiliza una VPN para trasmitir información confidencial

Utiliza contraseñas robustas, difíciles de adivinar y nunca las compartas o pongas a la vista

Bloquea tu equipo siempre que te ausentes de tu puesto de trabajo activando una contraseña y presionando + L

Mantén tu mesa libre de información confidencial como contraseñas o datos privados

Establece en tu dispositivo móvil una clave de acceso y la opción de bloqueo automático

Evita las fugas de información manteniendo conversaciones en lugares donde puedan ser oídas por terceros

Avisa al departamento de seguridad si detectas cualquier actividad sospechosa

## 2.- SUPLANTACIÓN DE IDENTIDAD

Para evitar riesgos es recomendable el uso del correo electrónico corporativo

Aprende a identificar correos sospechosos que contengan información confidencial

Verifica la fuente de información de los correos entrantes y sospecha de quien te pida datos confidenciales

No utilices los enlaces incluidos en correos, escribe la dirección directamente en el navegador

Mantén actualizado tu ordenador y todas las aplicaciones, sobre todo el antivirus y antispam

Asegúrate que las páginas donde entras son seguras. Han de empezar por https:// y tener un candado cerrado en el navegador

Una de las modalidades de suplantación suele legar por SMS intentando que visites un enlace fraudulento

Recuerda que este tipo de estafa no solo se centra en la banca online. Mantente alerta

Protege tu identidad desactivando el micrófono y tapando la cámara de tu ordenador

## 3.- LA INFORMACIÓN

Información Confidencial es todos aquellos datos que requieren medidas de seguridad para evitar su difusión

Firma siempre acuerdos de confidencialidad, restringe el acceso y cifra los datos cuando sea necesario

Haz copias de seguridad con regularidad. Su función es la de recuperarlos en caso de pérdida, fallo o ataque

Clasifica la información en base a nivel de riesgo y usuarios con permisos para poder establecer las medidas de seguridad adecuadas a cada información almacenada

Elimina los Metadatos de los ficheros que vayan a ser enviados a clientes o proveedores. Para eliminar los Metadatos hay que pinchar con el botón derecho en el archivo, ir a propiedades, detalles y pinchar en Quitar propiedades e información personal. Saldrá una nueva ventana y hay que pinchar en Quitar las siguientes propiedades de este archivo

## 4. - REDES SOCIALES

Usar redes sociales en entornos corporativos puede suponer un riesgo de fuga de información, así como riesgo para la empresa por actitudes impropias de los empleados

Conoce y cumple la normativa de la empresa antes de usar las redes sociales

Evita publicar información corporativa que pueda comprometer la seguridad de tu empresa

No mezcles los contactos personales con los corporativos

Ten cuidado en emitir juicios de valor a nivel personal que atañen a la empresa

No utilices el correo corporativo para unirte a una red social

No des información confidencial sobre tu trabajo o información que pueda usar la competencia

## 5.- SOPORTES

Todo soporte (discos duros, USB, tarjetas de memoria, cintas y discos) pueden sufrir pérdidas, robo, rotura, destrucción y avería

Debemos usar un proceso de borrado y destrucción segura para nuestros soportes cuando finalice su vida útil

Documenta el proceso seguro de borrado y destrucción de los soportes

Utiliza carpetas departamentales como métodos para compartir información en lugar de USB

El cifrado de los soportes es una de las medidas mas eficaces a la hora de evitar que la información sea comprometida

## 6.- PUESTO DE TRABAJO

Es necesario emplear mobiliario de contribuya a la protección de la información. Armarios con cierre, cajas fuertes o armarios ignífugos

Establecer políticas de contraseñas seguras y secretas. No debemos anotarlas ni compartirlas

Usar métodos de autenticación como contraseñas, tarjetas de acceso o de la huella dactilar para identificar que un usuario es quien dice ser

La ingeniería social tiene como objetivo a los empleados de una empresa y permite obtener información confidencial de las víctimas y su organización

Es fundamental que formarse y concienciarse en materia de seguridad de la información

La mayoría de las fugas de información se producen en el puesto de trabajo. Es recomendable ser muy cuidadoso para evitar esas fugas

## 7.- USO DE SOPORTES PERSONALES

Configura correctamente el dispositivo móvil y protégelo de forma adecuada. El departamento de informática puede ayudarte.

Diferencia entre correo personal y correo corporativo

Cifra las conexiones para proteger la información cuando trabajes fuera de la red corporativa

Cifra los dispositivos móviles para evitar la fuga de información en caso de pérdida o robo

Evita el uso de redes wifi públicas especialmente si acceder a cuentas bancarias o a la red corporativa

Usa la navegación de incognito que incluye la mayoría de los navegadores

Mantén el sistema operativo y todas tus aplicaciones siempre actualizadas

Los dispositivos móviles permiten habilitar y deshabilitar el geoposicionamiento. Es recomendable deshabilitarlo para evitar difundir más información de la necesaria