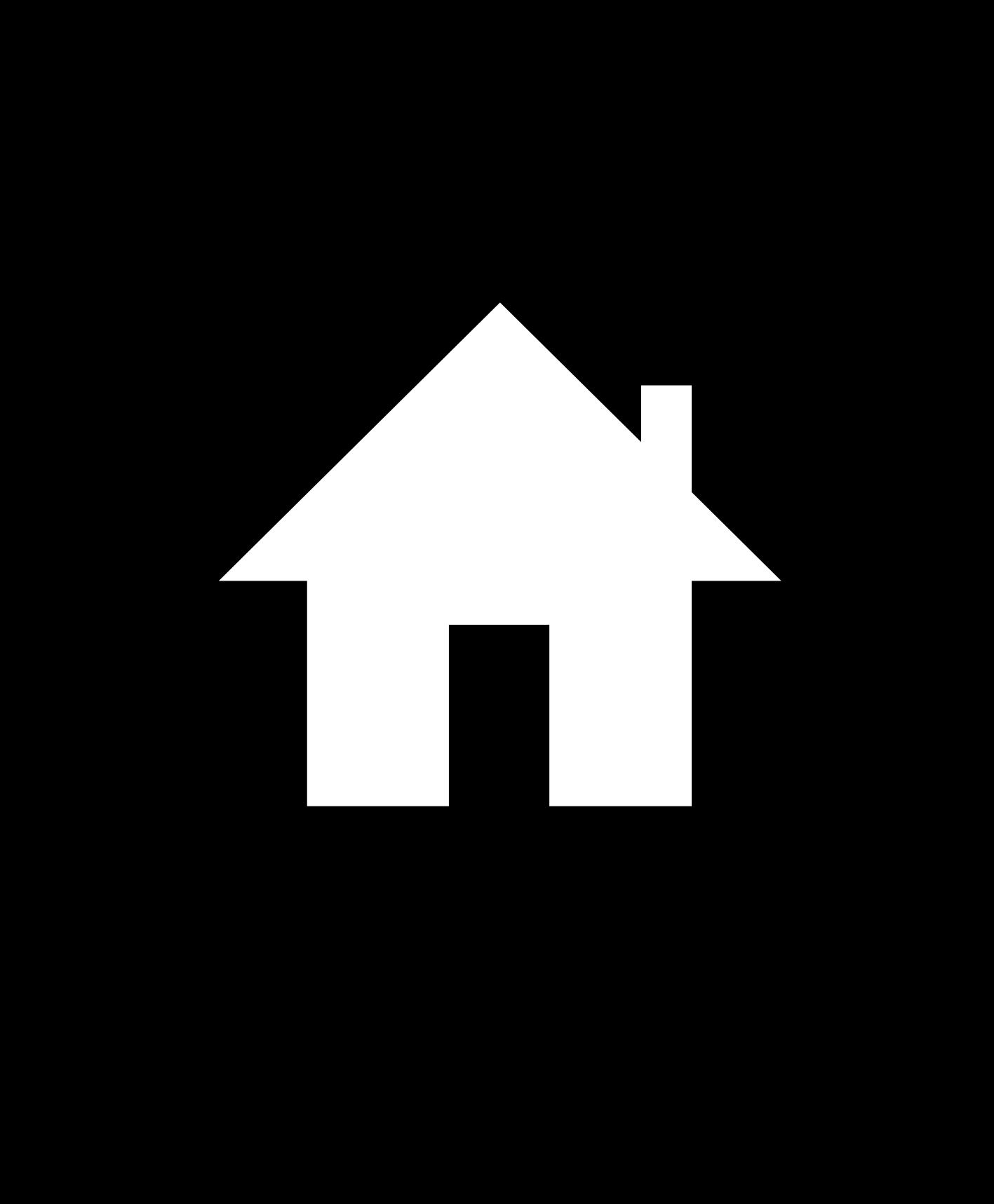




TELETRABAJO

Cómo implantar el teletrabajo de forma segura

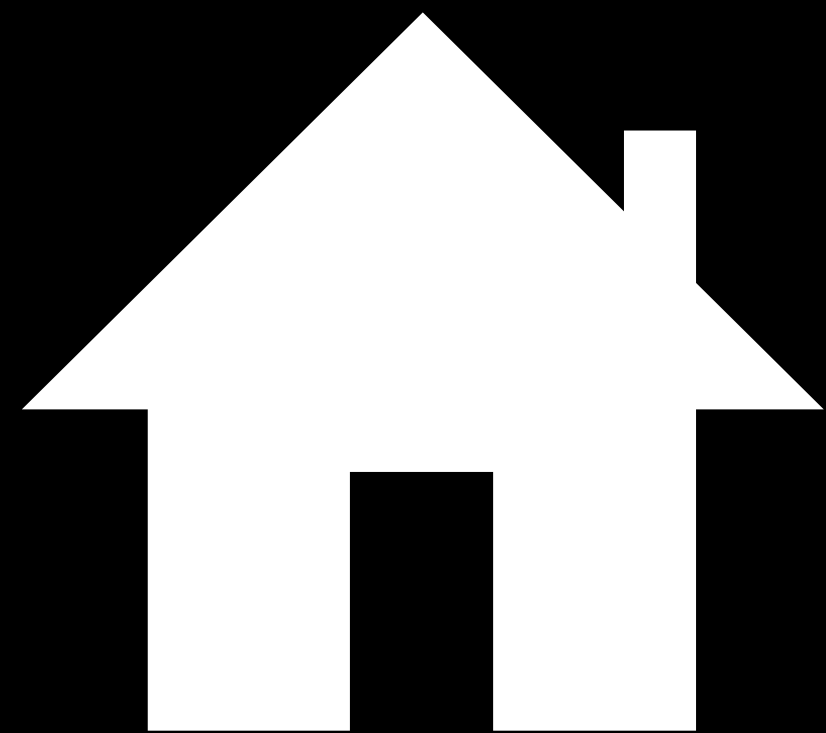
Safe



Este manual incluye una serie de medidas de seguridad para la movilidad en toda la empresa y también para concienciar a los empleados para que cumplan las directivas de seguridad.

Establece las condiciones y circunstancias en las que se permite el acceso remoto a los servicios corporativos siguiendo los consejos de este manual.

Safe



QUIÉN

Concediendo permisos

Debes llevar un registro de aquellos usuarios que disponen de permiso para trabajar desde fuera de las instalaciones corporativas y facilitarles instrucciones sobre las medidas de seguridad que deben aplicar durante la modalidad de teletrabajo.

El usuario con permiso deberá firmar un acuerdo en el cual se compromete a seguir ciertas directrices cuando utilice la modalidad de teletrabajo.

Haz clic sobre el botón para descargar el documento con las medidas de seguridad que deben cumplir los trabajadores que realicen su jornada o parte de su jornada en la modalidad de teletrabajo.

DESCARGAR



Safe





CÓMO

Definiendo unas pautas

Se deben implementar un conjunto de medidas de seguridad, que garanticen que sólo los dispositivos autorizados están conectados a la red y que éstos incorporan las medidas de seguridad apropiadas.

Además, debes implantar un método que te permita comprobar de manera periódica si se están aplicando en los dispositivos corporativos estas medidas.

Safe





DISPOSITIVOS

Autorizados y de confianza

Se debe limitar el acceso a los dispositivos de confianza, es decir aquellos que, aun siendo personales, están convenientemente protegidos.

- Deben tener instalado un antivirus y fijar una política de actualizaciones obligatorias, así como una política de aplicaciones autorizadas a instalarse en los mismos.
- Se deben establecer sistemas de acceso al dispositivos válidos: utilización de PIN o clave de acceso, además de medidas adicionales como el cifrado.
- Debes fijar unas normas para la conexión de dispositivos personales a dispositivos corporativos (a través del USB o bluetooth).



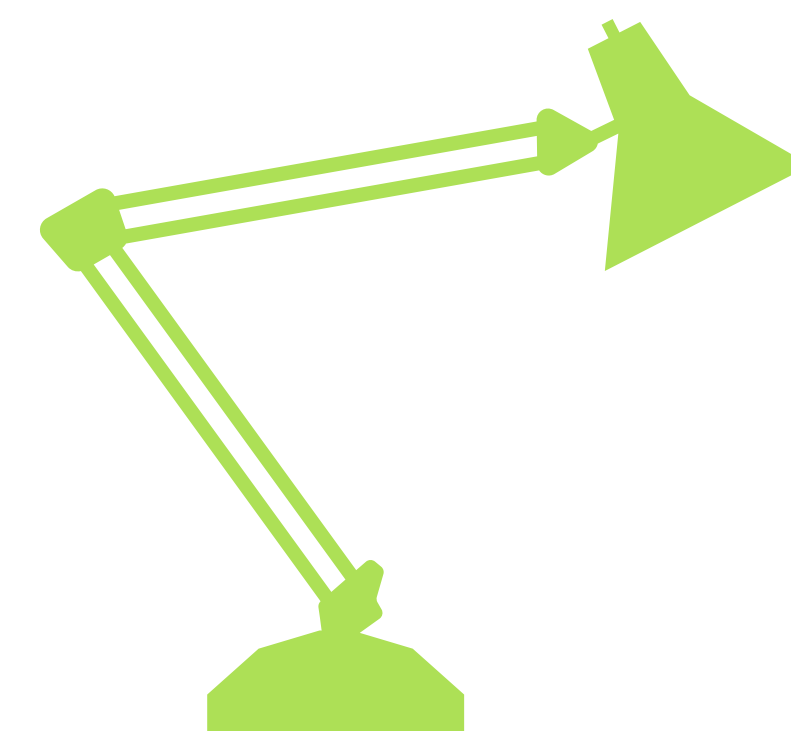


COPIAS DE SEGURIDAD

De dispositivos móviles

Las copias de seguridad no protegen de un ataque, sin embargo, garantizan que puedas recuperar la información importante si el dispositivo se vuelve inaccesible: pérdida o robo del terminal, fallo del material, borrado accidental...

- Las copia de seguridad se deben almacenar fuera del dispositivo móvil. Se pueden almacenar en los servidores corporativos o en la nube.
- Es más recomendable que las copias de seguridad sean almacenadas en repositorios gestionados por la organización, mejor que en equipos personales de los usuarios o en sistemas que no estén fuera del control del personal técnico.
- Se recomienda que las copias se realicen de manera automática, por ejemplo cada noche. Algunos servicios de almacenamiento en la nube disponen de la opción de realizar una copia de seguridad cada vez que se detecta un cambio en los archivos.
- La periodicidad de las copias depende de las necesidades propias de cada empresa en función del volumen y tipo de información que se gestiona.





APPS DE CONTROL REMOTO

Cómo usarlas de forma compliance

Se debe facilitar el uso de aplicaciones de control remoto, que ayuden a la localización del dispositivo en caso de pérdida y aporten la opción de borrado remoto de los datos.

- Tanto iOS como Android, como Windows Phone, tienen soluciones propias: "Find my iPhone, Device Manager y Encuentra mi teléfono".
- Recuerda que estas aplicaciones permiten realizar seguimientos en profundidad del dispositivo, por lo que su uso debe quedar restringido a causas justificadas ya que puede implicar la violación de la privacidad del usuario.
- Es recomendable deshabilitar el geoposicionamiento siempre que no sea estrictamente necesario pues se difunde más información de la necesaria de forma involuntaria.

Mantener el geoposicionamiento activado puede ayudar a recuperar un dispositivo robado o extraviado, antes de activar este servicio se debe informar al empleado y se debe firmar un acuerdo de conformidad, puede solicitarme que te redacte este acuerdo.



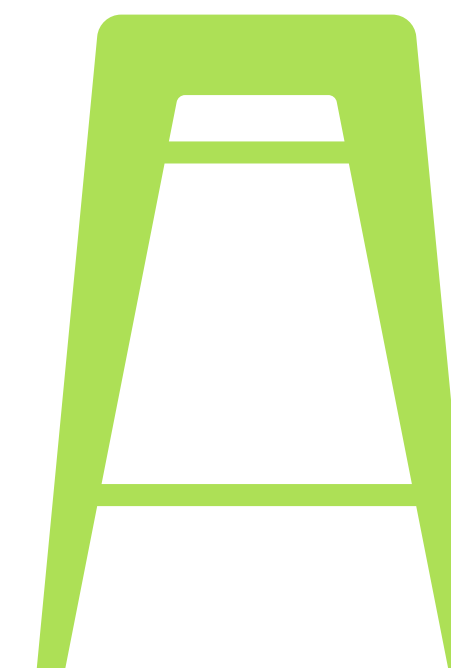


BYOD

Uso de equipos no corporativos

Se debe establecer una política de uso de BYOD corporativa en la que se establezcan los usos permitidos y las restricciones con respecto al uso de los dispositivos personales.

- Se deben incluir los dispositivos wereables: smartwatches, pulseras o gafas inteligentes que se conectan al móvil.
- Se debería prohibir por política el uso de **equipos ajenos** para conectarse a los activos de la empresa, especialmente si se trata de equipos públicos compartidos (centros comerciales, aeropuertos, hoteles..)
- Se deben incentivar medidas de seguridad en los dispositivos personales que permitan sacar el máximo partido al BYOD de una forma siempre segura.
- Se deben crear una política de seguridad del BYOD todos los requisitos de seguridad siempre que se haga uso del dispositivo personal para almacenar o acceder a información corporativa.
- Es necesaria la firma de un documento de conformidad y aceptación de estas normativas por parte del empleado antes del uso de sus propios dispositivos. Tienes un documento en KEYS que puedes utilizar.





COMUNICACIONES SEGURAS

Redes inalámbricas

A menudo, información confidencial de tu organización puede transmitirse a través de redes inalámbricas que no están bajo tu control, por lo que es recomendable que te asegures de que los datos viajan convenientemente protegidos.



REDES WIFI PROPIAS

En el caso de que quieras ofrecer movilidad poniendo en funcionamiento una red inalámbrica en tus dependencias, debes aplicar las siguientes medidas de seguridad:

- Utilizar un cifrado WPA2, actualmente se considera el más seguro para las redes WiFi.
- Crear una buena política de contraseñas que garantiza que se cambien periódicamente, longitud de al menos 8 caracteres y contenga mayúsculas, minúsculas y números.
- Modificar el nombre de la wifi por defecto para no dar pistas del tipo de router utilizado.

REDES WIFI DE TERCEROS

Es habitual que los usuarios utilicen redes públicas abiertas o pocas seguras para el intercambio de correo corporativo o acceder a apps de la organización.

Los motivos habituales para el uso de estas redes inseguras suelen ser la velocidad de la red, no disponer de conexión de datos en el portátil, ahorrar tarifa de datos o por el tipo de calidad o cobertura.

El uso de este tipo de redes se debe utilizar con algún tipo de seguridad adicional, mediante algún tipo de cifrado punto a punto como los sitios web SSL (los que empiezan con HTTPS y tienen un candado junto a la dirección o mediante una VPN.

REDES MÓVILES

Hoy en día las redes de telefonía móvil (3G,4G..) ofrecen una velocidad de transmisión que permite trabajar cómodamente desde cualquier lugar con cobertura telefónica móvil.

Los dispositivos como los smartphones y la mayoría de las tabletas traen por defecto conexión por red telefónica móvil.

Los consensos de seguridad a aplicar en este caso son los recomendados tanto para las redes wifi.



CONEXIONES REMOTAS

Red privada virtual VPN

El mejor sistema para la conexión remota a los equipos de tu organización es mediante el uso de una red privada virtual, también llamada VPN.

Esta tecnología de red proporciona un acceso seguro a las aplicaciones y sistemas corporativos a usuarios dispersos geográficamente, de una manera equivalente al tipo de acceso que tendrían en los locales de tu organización.

Estas son sus ventajas:

- Permite la conexión de manera totalmente segura, incluso desde redes abiertas o poco seguras.
- Funciona sobre conexiones 3G, 4G y wifi, de modo que es una capa de seguridad extra sobre la red que se esté utilizando.
- Limita el medio de acceso remoto a tu organización a un único punto con autenticación, lo que permite una mayor control de accesos.
- Reduce los servicios expuestos a Internet, disminuyendo la posibilidad de ser atacados.



Safe



VPN

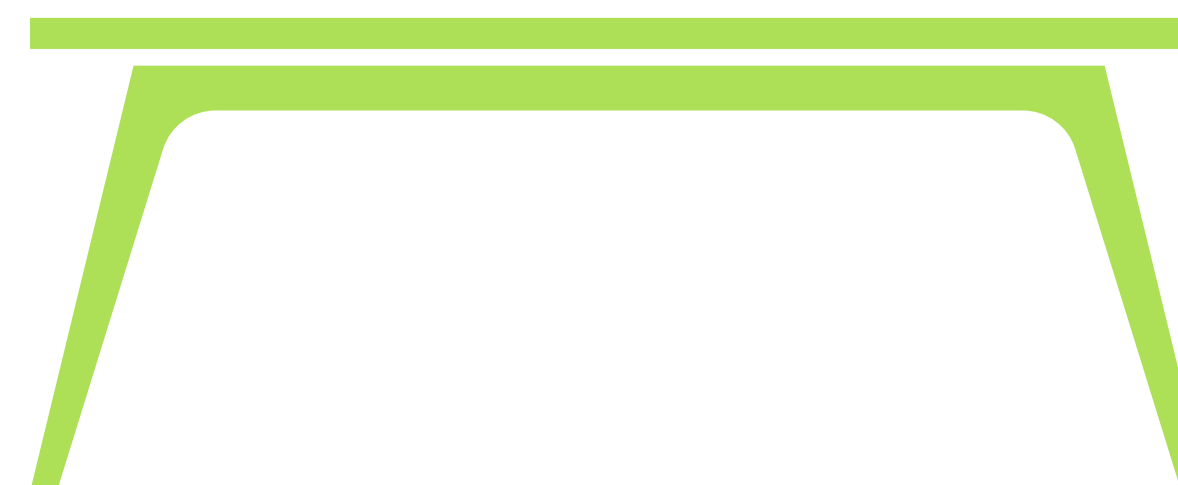
OPCIONES DE SEGURIDAD

Si la contraseña de acceso a una VPN resulta comprometida por un atacante, éste dispone de un acceso a la red interna de nuestra empresa, por lo que puede resultar peligroso.

Existen opciones de seguridad ofrecidas en los sistemas VPN que pueden minimizar o anular estos riesgos:

- El uso de certificados para la autenticación mutua que confiere protección frente al riesgo de que alguien se pueda hacer pasar por el usuario de uso legítimo.
- La doble autenticación utilizando un certificado y contraseña hace muy difícil robar las credenciales de acceso, ya que se necesitan dos elementos para autenticarse.

Safe





LA NUBE

Servicios de almacenamiento

Una opción alternativa al almacenamiento de información en el equipo es utilizar los sistemas de almacenamiento en la nube. De este modo el robo o pérdida del dispositivo no implica la pérdida de la información almacenada.

Sin embargo, antes de empezar a utilizar estos servicios, debemos tener en cuenta algunos aspectos:



- Debe estudiarse la disponibilidad del servicio y las posibles restricciones de privacidad o confidencialidad. Es necesario escoger un servicio que cumpla la normativa de protección de datos personales.
- Este tipo de servicio puede requerir que haya que utilizarlo también en los equipos de escritorio de la empresa, para mantener la sincronización con la información utilizada en la organización. Es implica un estudio en profundidad de aquellos repositorios que se consideren susceptibles de ser subidos a la nube.
- Aunque es poco frecuente que se produzcan incidentes de seguridad en los principales proveedores de estos servicios, debe valorarse esa posibilidad.
- Los dispositivos no pueden tener habilitado el acceso por defecto, debe ser necesario que se solicite una clave cada vez para acceder al servicio. De otro modo, el uso de esta alternativa no proporcionaría una seguridad adicional.



673 248 261
safe@safe-lopd.com
www.safe-lopd.com

Safe