Guía

CIBERSEGURIDAD

EN EL SECTOR DE LOS ADMINISTRADORES DE FINCAS

Guía de recomendaciones para los despachos de administración de fincas

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

Consejo de Colegios Administradores de Fincas Castilla y León

Administrador Fincas Colegiado

Índice

Índice

1. Introducción

Hoy en día es indudable que la **transformación digital** se encuentra cada vez más inmersa en los procesos de negocio de la administración de fincas. Su adopción permite a las empresas disponer de mayores y mejores ventajas competitivas en el mercado, aumentando también su productividad y rentabilidad.

En este escenario la gestión de la **ciberseguridad** cobra un papel fundamental para que el uso de la tecnología no suponga un riesgo para las empresas, por lo que la presente guía tiene como principal objetivo **promover la concienciación en ciberseguridad y unas medidas indispensables a implementar en el sector de la administración de fincas**, que permitan disponer de un negocio seguro y competitivo donde la digitalización y la ciberseguridad avancen de la mano.

- **En primer lugar**, se desarrolla una **caracterización de la ciberseguridad aplicada al sector,** detallando para ello la dependencia tecnológica y el perfil de ciberseguridad de las empresas que integran el mismo.

- **En segundo lugar**, se analizan las **principales amenazas de ciberseguridad** a las que están expuestas estas empresas, siempre teniendo en cuenta el alcance establecido.

- **Por último**, se abordan y detallan los **principales aspectos** a tener en cuenta **en materia de ciberseguridad dentro del sector**, destacando las distintas medidas necesarias para proteger la información que gestionan y transmitir de este modo una imagen positiva y competitiva de la organización entre sus clientes.

Dentro del objetivo marcado, y debido a la gran variedad de empresas pertenecientes a este sector, esta guía, realizada por **INCIBE**, en colaboración con el Colegio de Administradores de Fincas de León, se centra en las **microempresas, pymes y autónomos a nivel nacional**, excluyendo del presente estudio a las grandes empresas.

« La transformación digital se encuentra cada vez más inmersa en los procesos de negocio de la administración de fincas »

1.1. Glosario de términos

En el mundo de la ciberseguridad se emplean términos y acrónimos de perfil técnico que no se usan en el día a día, sobre todo en el caso de personas que no se dedican al ámbito de la ciberseguridad. Por este motivo, **INCIBE** pone a disposición de los usuarios un **glosario de términos [1]**, ayudando de este modo a todos los perfiles en la comprensión de esta guía.

1.2. Importancia de la seguridad en despachos de administración de fincas

Debido a su actividad, los despachos de administración de fincas gestionan una **gran cantidad de información confidencial**. Por tanto, si esta información se viera afectada por un incidente de seguridad, las repercusiones para el despacho podrían ser muy graves. La información que gestionan los administradores de fincas puede verse afectada principalmente por dos tipos de incidentes de seguridad: el ***ransomware* [2]** y las **fugas de información [3]**.

El ***ransomware*** es un tipo de código malicioso o *malware* diseñado para secuestrar la información de las víctimas y que estas no puedan acceder a su contenido. Este *malware* se encarga de cifrar todo archivo que pueda ser de valor para tu empresa, como hojas de cálculo, archivos de texto, imágenes, vídeos o bases de datos. Todo el tiempo de trabajo invertido en esos archivos no habrá servido de nada, ya que estarán bajo control de los ciberdelincuentes.

Las **fugas de información** son el otro tipo de incidente, cuyas consecuencias pueden ser muy perjudiciales. Ponte en el supuesto de que te robaran o perdieras información confidencial de tus clientes. ¿Seguirían confiando en tu empresa o se pasarían a la competencia? ¿Esa pérdida, además, podría tener consecuencias legales?

Las fugas de información se producen de tres formas distintas: **accidental**, **intencionada** por un miembro de la organización o *insider*, o por medio de un ataque externo llevado a cabo por **ciberdelincuentes**. Las causas pueden ser variadas, pero principalmente, cuando se produce una fuga, esta suele deberse a la **inexistencia o debilidad de los controles de seguridad** en el acceso a la información.

Los ciberdelincuentes pueden ser el origen de la fuga de información, mediante ***malware*** procedente de correos electrónicos o páginas **web de tipo *phishing***. Una vez esta información está en mano de ciberdelincuentes, lo más habitual es que sea vendida o extorsionen a las empresas, pidiendo dinero a cambio de no ser divulgada.

« Las fugas de información se producen de tres formas distintas: **accidental**, **intencionada** por un miembro de la organización o *insider*, o por medio de un ataque externo llevado a cabo por **ciberdelincuentes** »

2. Caracterización de la ciberseguridad aplicable al sector

En este apartado se pretende analizar, en primer lugar, la **dependencia tecnológica de las empresas del sector**, teniendo en cuenta los principales aspectos a considerar, como son la categorización de las empresas que se dedican a la administración de fincas y las diferentes soluciones que más utilizan para prestar sus servicios.

En segundo lugar, se obtienen los diferentes perfiles de ciberseguridad de las empresas del sector y el nivel de riesgo al que se encuentran expuestas.

2.1. ¿Qué es la ciberseguridad?

Aunque el término **ciberseguridad** representa un concepto bastante amplio, se puede definir en el **contexto** de esta guía, como la práctica de proteger nuestros sistemas de información y todo lo que engloban (redes de comunicación, dispositivos, aplicaciones, etc.) de posibles ataques malintencionados. Por lo general, a través de estos ciberataques se podría **acceder, modificar o destruir información confidencial**, extorsionar a los usuarios o llegar a interrumpir la continuidad del negocio.

La **dependencia tecnológica** aumenta a la par que el ingenio de los ciberdelincuentes por lo que la ciberseguridad es un factor fundamental en todas las empresas, ya sean pymes, autónomos o grandes corporaciones.

La ciberseguridad es un proceso, y como tal, los planes para abordarla deben revisarse y actualizarse periódicamente, ya que **las amenazas cambian y evolucionan constantemente**. Es esencial conocer medidas de seguridad que protejan la información de la organización, así como de los sistemas que la gestionan y, de esta forma, contribuir también a la generación de confianza en clientes y proveedores.

2.2. Dependencia tecnológica

Para empezar a implementar medidas de seguridad es necesario **conocer la dependencia tecnológica de nuestro despacho**, que está ligada a aspectos como el tamaño de la organización o los procesos que integra para ofrecer sus servicios.

2.2.1. Soluciones tecnológicas utilizadas

Los despachos de administración de fincas pueden utilizar un amplio conjunto de **soluciones tecnológicas**, con el objetivo de conseguir una mayor ventaja competitiva, una mayor productividad y/o una mejor rentabilidad de sus procesos.

A continuación, puede verse un **listado con algunas de las soluciones más utilizadas** habitualmente por el sector, clasificadas según el tipo de tecnología a la que pertenecen:

Tecnología	Soluciones
Infraestructura	▶ Soluciones de **almacenamiento externo.** ▶ **Equipamiento de oficina:** Portátiles, ordenadores de sobremesa, dispositivos móviles, etc. ▶ **Equipamiento auxiliar:** climatizaciones e iluminación. ▶ Sistemas de **videovigilancia.**
Red	▶ **Equipamiento para soluciones de redes internas:** servidores, *switch*, *firewall*, etc. ▶ Soluciones para **redes wifi.**
Cloud	▶ Soluciones para gestión de relación con clientes: **CRM.** ▶ Soluciones **ERP** para la gestión de administración de fincas. ▶ Soluciones de **pago electrónico.** ▶ Soluciones de **servicio de copias de seguridad.** ▶ Soluciones de **gestión documental.** ▶ Soluciones de **sistemas TPV.**
Aplicaciones	▶ Soluciones de **escritorio o cliente/servidor** para labores de administración de fincas. ▶ Soluciones para **contabilidad de la empresa**. ▶ Soluciones de **mensajería instantánea y videoconferencia** para comunicaciones internas y externas. ▶ Soluciones de **videovigilancia**. ▶ Soluciones de **firma y certificados digitales**. ▶ **Herramientas de productividad.** ▶ **Uso de redes sociales.**
Servicios de páginas web	▶ **Página web corporativa para administradores de fincas:** preparadas para ofrecer información y documentación. ▶ **Página web corporativa para gestión de alquileres turísticos:** pasarelas de pago seguras, calendarios interactivos de reservas, intercambio de información con el inquilino, etc.

Tabla 1. Soluciones tecnológicas más habituales del sector

2.2.2. Niveles de dependencia tecnológica

En función del **tipo de despacho**, caracterizado por el servicio que ofrece y/o actividad que realiza, y del tamaño del mismo, se puede determinar el **conjunto de soluciones tecnológicas** que serán necesarias para cumplir con su objetivo de negocio y, por tanto, su nivel de dependencia tecnológica. De forma general, para cualquier sector de actividad los niveles de dependencia se clasifican en bajo, medio o alto.

Las **3 tipologías de despacho de administración de fincas predominantes en España son las siguientes**:

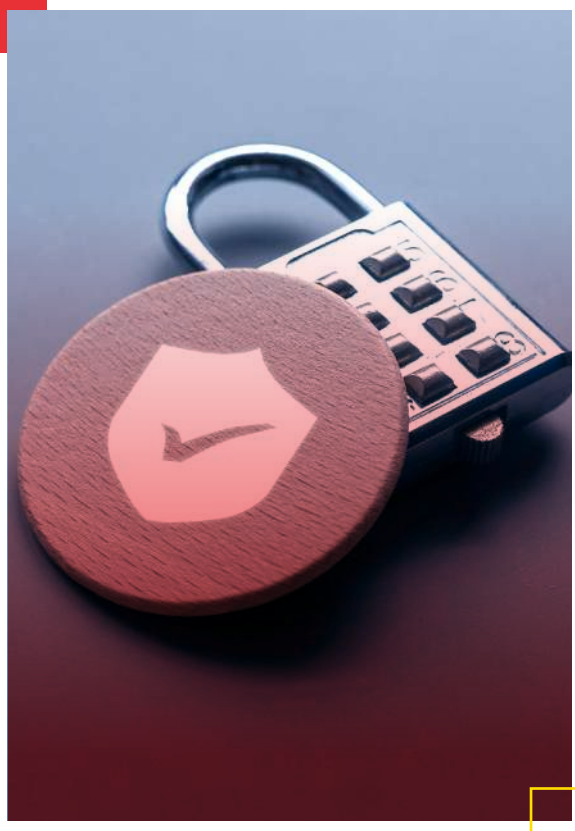
En torno al 90%:
despachos unipersonales y muy pequeños (1-4 personas).

Sobre el 8%:
despachos medianos (5-12 empleados).

El 2% restante:
despachos grandes más de 12 empleados.

Teniendo en cuenta las soluciones tecnológicas más habituales descritas en la tabla anterior y las tipologías de despachos, el alcance de esta guía excluye los grandes despachos y se centra en las **medidas de seguridad para los medianos, pequeños e unipersonales** con un nivel bajo o medio de dependencia tecnológica.

Además, existen diversas herramientas y servicios en el mercado, con el objetivo de que las empresas puedan evaluar su nivel de riesgo en ciberseguridad y, de esta forma, comenzar a mejorar su protección. Dentro de estos servicios **INCIBE** proporciona la **herramienta de autodiagnóstico [4],** que ofrece un primer punto de partida para determinar cómo es el estado actual de ciberseguridad en tu negocio, qué riesgos lo amenazan y qué aspectos debes mejorar.



2.3. Perfiles de ciberseguridad

El perfil de ciberseguridad está determinado por el **nivel de riesgo al que se encuentra expuesta una organización, pudiendo ser alto, medio o bajo**. Estos valores, a su vez, están definidos por varios factores, entre los que se encuentran el nivel de dependencia tecnológica y el tipo de soluciones utilizadas, teniendo en cuenta que no todas las soluciones están expuestas al mismo número o tipo de amenazas de ciberseguridad.

La dependencia tecnológica viene derivada del conjunto de soluciones utilizadas en función de la actividad del negocio y el tamaño de la empresa, considerando la clasificación en autónomos, **microempresas (1-9 empleados)**, **pequeñas empresas (10-49 empleados)**, **medianas empresas (50-249 empleados)** y **grandes empresas (>250 empleados)**.

Por tanto, se considera que una empresa tiene un perfil de ciberseguridad con **nivel de riesgo alto** cuando tiene, por ejemplo, una **alta dependencia tecnológica**, con **tecnologías expuestas a un número moderado de amenazas**, o una **dependencia tecnológica media**, con **tecnologías expuestas a un gran número de amenazas**.

En la siguiente tabla se puede ver la **relación** existente entre la dependencia tecnológica, el nivel de amenazas a las que están expuestas las soluciones (que depende de los tipos y número de amenazas) y el nivel riesgo en ciberseguridad de las organizaciones.

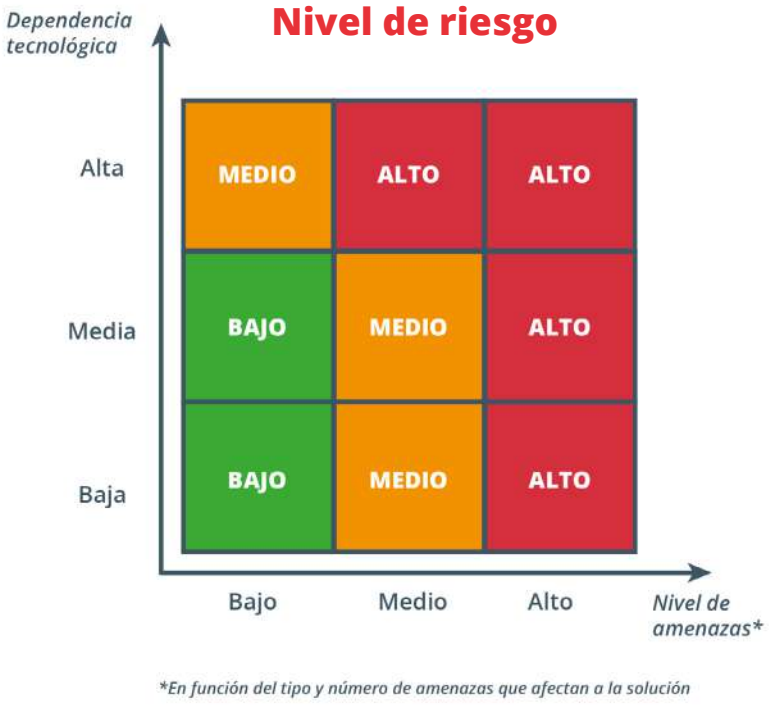


Ilustración 1. Nivel de riesgo de los perfiles de ciberseguridad

3. Principales amenazas de ciberseguridad en los despachos de administración de fincas

3.1. Amenazas a través de las comunicaciones

Las amenazas más comunes que afectan a los administradores de fincas tienen su origen en el **correo electrónico, mensajería y llamadas telefónicas** que, junto con la **ingeniería social** [5], se convierten en un instrumento muy eficaz para que los ciberdelincuentes se lucren a través del fraude, la estafa y la extorsión.

3.1.1. ¿Qué es la ingenería social?

En la ficción, generalmente se muestra a los ciberdelincuentes como prodigios de la informática y la ciberseguridad, capaces de vulnerar cualquier sistema **explotando sus vulnerabilidades**. En la realidad, y en la mayoría de ocasiones, los ciberdelincuentes atacan al eslabón más débil, pero de vital importancia en la cadena de la seguridad, es decir, al que gestiona la información, utilizando **técnicas no demasiado sofisticadas**. Los ataques basados en ingeniería social requieren mucho menos esfuerzo que otros tipos de ataques y, por lo tanto, el beneficio es mayor.

La ingeniería social consiste en **utilizar diferentes técnicas de manipulación psicológica**, con el objetivo de conseguir que las potenciales víctimas revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente, como revelar información confidencial o instalar *software* malicioso.

Los ataques basados en ingeniería social se pueden categorizar en **dos tipos diferentes en función del número de comunicaciones** que debe realizar el ciberdelincuente hasta conseguir su objetivo:

Hunting

Mediante **una única comunicación**, los ciberdelincuentes buscan obtener su propósito. Generalmente, la técnica del *hunting* es utilizada en ataques de *phishing* [6] o campañas de distribución de *malware* [7]**.** Este tipo de campañas maliciosas son enviadas por los ciberdelincuentes de manera masiva, es decir, sin objetivos concretos.

Farming

En este caso, los ciberdelincuentes emplean **más de una comunicación** con la víctima hasta conseguir su objetivo. El *farming* es comúnmente utilizado en campañas de extorsión, fraude del CEO o fraude de RR.HH. [8]

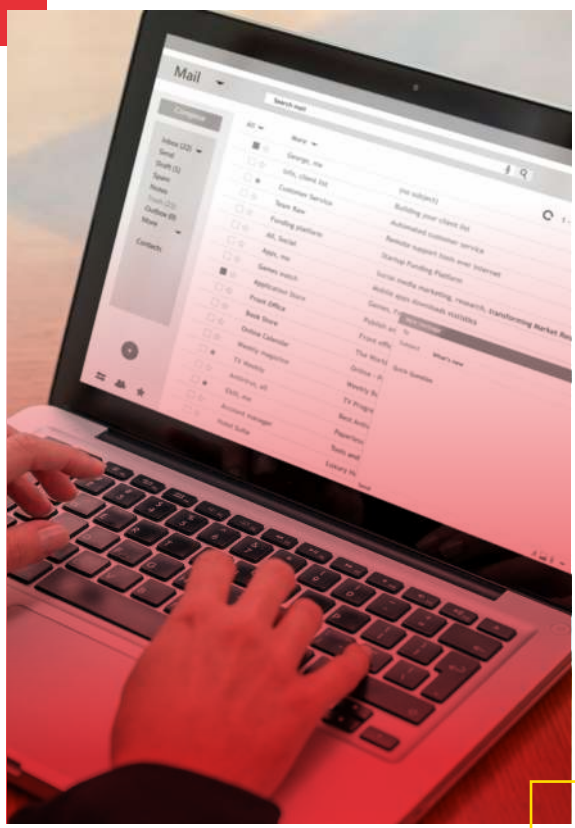
La gran mayoría de incidentes de seguridad que afectan a los administradores de fincas tienen en común dos factores: el **correo electrónico** y comunicaciones que utilizan diferentes técnicas de **ingeniería social**, por lo que analizaremos estos incidentes más en profundidad.

3.1.2. Amenazas a través del correo electrónico

Los ciberdelincuentes utilizan la combinación de la ingeniería social y las herramientas tecnológicas para engañar tanto a empresarios como a empleados. Este tipo de estafas, por lo general, se realizan a través del correo electrónico y tienen principalmente una motivación económica para el ciberdelincuente.

Los incidentes más comunes en los despachos de administración de fincas son los relacionados con el ***phishing*** y sus variantes (***smishing*** y ***vishing***) **[9]**, ***ransomware*** y el fraude del email comprometido (BEC) **[10]**.

A continuación, se describen en profundidad estos **tres tipos de incidentes** con sus correspondientes ejemplos de casos reales. Además, se detallan otro tipo de ataques que, aunque con menos incidencia en este sector, también es necesario conocer y saber identificar.



3.1.2.1. Phishing y sus variantes smishing y vishing

¿Alguna vez has recibido en tu correo algún mensaje que parece ser de una empresa o entidad de las que eres cliente o usuario, instándote a realizar una acción con urgencia como un inicio de sesión o cambio de contraseña? Presta siempre atención a estos correos, pues no son lo que parecen.

Se trata de **correos de tipo *phishing***, un tipo de fraude cometido generalmente a través del correo electrónico, aunque se pueden utilizar otros medios, como **mensajes SMS** (***smishing***), redes sociales, aplicaciones de mensajería instantánea o **llamadas telefónicas** (***vishing***), cuyo objetivo principal es robar credenciales de acceso e información confidencial.

Para lograr engañar a la víctima, los ciberdelincuentes suelen **suplantar la identidad de empresas y organizaciones reconocidas**, comúnmente aquellas de las que pretenden **robar la información**, como, por ejemplo, entidades bancarias, empresas del sector de la energía, de logística, etc.

Como técnica principal, los ciberdelincuentes suelen **falsear la dirección del remitente para que simule proceder de la entidad legítima, cuando en realidad el mensaje procede de otra fuente**. A esta técnica se la denomina ***email spoofing*** **o suplantación de la dirección correo electrónico [11]**.

Además, estos correos comúnmente contienen un **enlace en el cuerpo del mensaje** que lleva a una página web fraudulenta que tiene la misma estética que la página web legítima a la que intenta suplantar. En dicha web fraudulenta se solicita la **información confidencial** que se quiere sustraer, generalmente información personal, credenciales de acceso e información financiera. Para ofrecer más veracidad, dicha web suele utilizar un **nombre de dominio similar al legítimo**, siempre buscando como objetivo que las potenciales víctimas caigan en el engaño.

Una vez que la víctima del ataque ha facilitado toda la información que los ciberdelincuentes solicitan, el usuario suele ser **redirigido a la página web legítima de la entidad suplantada**, con el fin de que el fraude pase el mayor tiempo desapercibido antes de que la víctima denuncie el hecho.

Como adelantábamos, uno de los tipos de *phishing* que más afectan a este sector son los ***phishing* bancarios**, cuya apariencia suele ser la siguiente. Puedes encontrar más casos reales **aquí.**

Ilustración 2. Correo de tipo phishing suplantando a una entidad bancaria

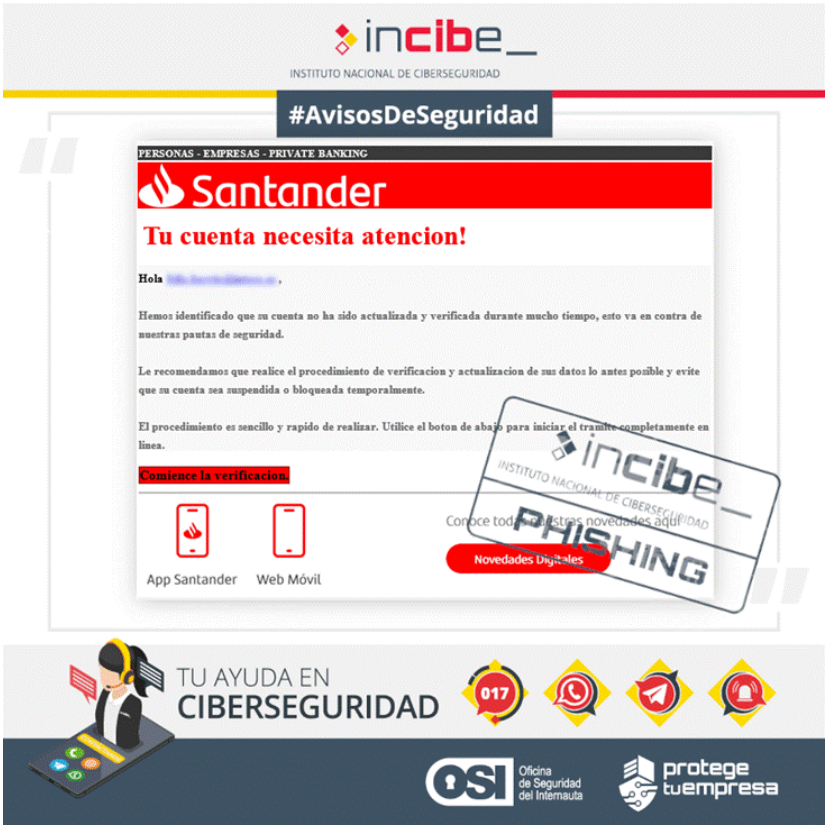


Ilustración 3. Correo de tipo phishing suplantando a una entidad bancaria

Otros son los que suplantan a distintas entidades, como, por ejemplo, la **Agencia Tributaria** o la **DGT**:

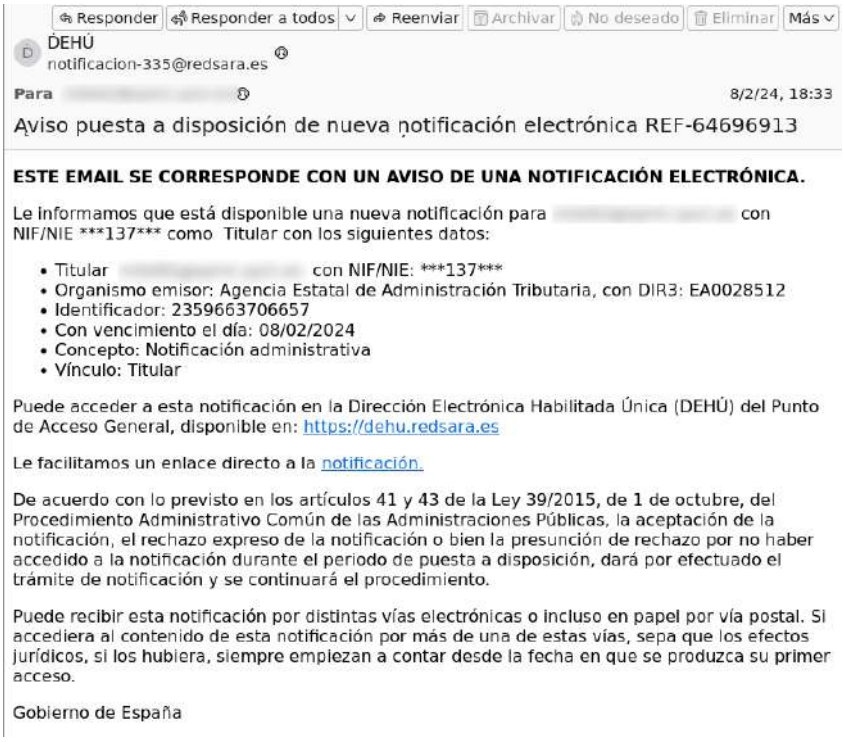


Ilustración 4. Phishing que suplanta la Dirección Electrónica Habilitada Única (DEHú) de la Agencia Tributaria

¿Has recibido algún correo de este tipo y dudas de si es legítimo o fraudulento?

A continuación, se resaltan los **aspectos más relevantes que deben ser considerados** a la hora de identificar la legitimidad de un correo electrónico.

- **Remitente.** Los correos de tipo ***phishing*** en ocasiones contienen remitentes que no coinciden con la organización a la que supuestamente representan. Este es el **primer indicador que ha de comprobarse**. Por ejemplo, un correo que supuestamente procede de una entidad bancaria tendría un remitente, cuyo dominio coincidiría con la entidad a la que representa. **Si dicho dominio no coincide, es un síntoma de fraude.**

- En otras ocasiones, los ciberdelincuentes utilizan la **técnica de *email spoofing,*** que consiste en **falsear el remitente**, haciendo que parezca proceder de la entidad legitima cuando en realidad no es así. Para comprobar si el remitente realmente es el que figura en el correo, **se deben analizar las cabeceras del mismo**. Para ello, puedes seguir las instrucciones facilitadas en el artículo **"¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos".**

- **Necesidad de llevar a cabo la petición de manera urgente.** La ingeniería social es el componente esencial en los **correos electrónicos de tipo *phishing***. Los ciberdelincuentes suelen alertar a las víctimas sobre situaciones negativas a las que tendrán que hacer frente a no ser que sigan las instrucciones que facilitan. Algunos de los ganchos más utilizados son la **cancelación del servicio o cuenta**, **multas, sanciones por no acceder en tiempo y forma, etc**. Son muchas las artimañas utilizadas, cuyo fin es forzar al usuario a realizar una determinada acción a través de una coacción.

Ilustración 5. Cómo identificar la legitimidad de un correo

- **Enlaces falseados.** Los **enlaces ofuscados** son una parte fundamental de este tipo de fraude. En la mayoría de las ocasiones es la vía esencial que utilizan los ciberdelincuentes para **robar la información confidencial**. Los enlaces suelen aparentar que corresponden a la web legítima o sencillamente contienen un texto haciendo referencia a que sea seleccionado o **"clicado"**. Para comprobar a dónde apunta realmente el enlace, **se puede situar el ratón encima y comprobar el cuadro de dialogo que figura en la parte inferior de la pantalla con la verdadera dirección**. También se pueden utilizar herramientas online, como:

  - Informe de transparencia de Google [12]
  - Free website Security Check & Malware Scanner [13]
  - VirusTotal [14]
  - URLhaus [15]

- En otras ocasiones **los enlaces pueden estar acortados**, no siendo posible visualizar su destino si no se utilizan herramientas específicas, como:
  - **Unshorten.It! [16]**

- Siempre se ha de tener **especial cuidado** al acceder a enlaces en correos electrónicos, siendo preferible acceder introduciendo la dirección web directamente en el navegador o utilizando la aplicación oficial de la entidad. Las entidades legítimas, como las financieras, nunca solicitarán a los clientes credenciales de acceso en comunicaciones por correo electrónico.

- **Comunicaciones impersonales.** En la mayoría de las ocasiones las comunicaciones fraudulentas recibidas por correo electrónico son impersonales, como, por ejemplo, «Estimado cliente, usuario, etc.». Las comunicaciones legítimas suelen ser personales, indicando el nombre de la persona o entidad a la que van dirigidas.

- **Errores ortográficos y gramaticales.** Una auténtica comunicación de cualquier entidad no contendrá errores ortográficos o gramaticales, ya que la comunicación con sus clientes es un aspecto muy cuidado.

- **Firmas y estética del correo.** La estética y la firma del correo electrónico es otro factor a considerar. Cuando se está familiarizado con los correos de una determinada organización y una comunicación no sigue ese patrón, es un síntoma de fraude.

Si después de estos consejos todavía tienes dudas, recuerda que puedes trasladar cualquier consulta a nuestra **Línea de Ayuda en Ciberseguridad, 017.**

Smishing

El ***smishing*** es una variante del *phishing* que se centra en el uso de los mensajes de texto (SMS) para la obtención de la información a través del engaño. El término proviene de la combinación de las palabras «SMS» y «*phishing*».

Los **mensajes enviados** por los ciberdelincuentes intentan parecer legítimos y suelen imitar a los mensajes de texto de bancos, aplicaciones u otros proveedores de servicios.

En los mensajes se suele incitar al destinatario a **hacer clic en un enlace** con la excusa de verificar su identidad, actualizar su contraseña, hacer el seguimiento de un paquete o activar alguna nueva versión de la aplicación a la que tratan de suplantar.

El siguiente ejemplo es un **caso real de *smishing*** en el que se intenta suplantar a una entidad bancaria. En ocasiones, los mensajes fraudulentos recibidos se hacen pasar por una entidad bancaria de la que el usuario ni siquiera es cliente. En este caso, sería fácil reconocer el engaño, pero, en caso de coincidir la entidad con la real del usuario, puede llevar a la víctima a **«morder el anzuelo»**.

Ilustración 6. Campaña de smishing suplantando a una entidad bancaria

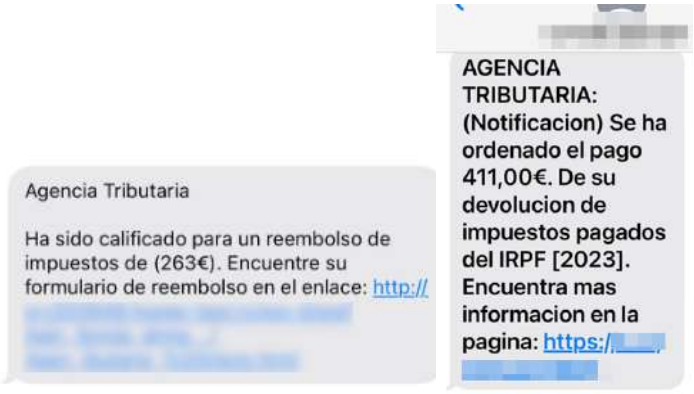


Ilustración 7. Campañas de smishing suplantando a la Agencia Tributaria

Ilustración 8. Campaña de smishing suplantando a la DGT

El **enlace**, como en el caso del ***phishing***, normalmente redirige a una página web falsa que parece legítima. También puede **descargar *software* malicioso en el dispositivo**.

Para hacer aún más creíble el engaño, los ciberdelincuentes pueden buscar información, por ejemplo, en redes sociales para personalizar los mensajes. Asimismo, utilizan **técnicas de *spoofing***, pudiendo suplantar la identidad del remitente para que parezca provenir de una fuente legítima. Incluso, consiguen enviar los mensajes fraudulentos en un hilo de mensajes reales (por ejemplo, de una entidad financiera), haciendo aún más difícil identificar la estafa.

Vishing

El término ***vishing*** nace de la combinación de «*voice*» (voz) y «*phishing*» y, como su propio nombre indica, es una técnica de ingeniería social que emplea las **llamadas telefónicas** para, como en los casos anteriores, **obtener información de la víctima mediante el engaño**.

En este caso, los ciberdelincuentes utilizan sus armas de engaño para convencer a la víctima de que la llamada proviene de una empresa legítima. Suelen hacerse pasar por representantes de compañías telefónicas, entidades bancarias, agencias gubernamentales, etc., con el fin de **convencer a la víctima de revelar información personal y/o financiera**.

Los ciberdelincuentes suplantan la identidad de las empresas e incluso a veces el número que aparece al recibir la llamada es igual que el original.

En el caso de las pymes, los ciberdelincuentes usan esta técnica haciéndose pasar por un proveedor, un cliente o incluso alguien interno de la empresa. En el caso de fingir ser un empleado interno, el ciberdelincuente suele optar por alguien del Departamento Tecnológico, en quien la víctima suele confiar para proporcionarle cualquier tipo de información, incluso credenciales. Puedes escuchar una llamada de ***vishing* real** a través del siguiente **enlace.**

3.1.2.2. Infección por malware

¿Alguna vez te has encontrado en tu correo un mensaje que parece ser de empresas o entidades de las que eres cliente o usuario, instándote a descargar y abrir un adjunto al correo o a través de un enlace, con el pretexto de ser una factura o una comunicación urgente? Presta atención, pues estos archivos que descargas pueden estar infectados con ***malware***.

El *malware* hace referencia a los programas diseñados para instalarse de forma no autorizada en los dispositivos de las víctimas. Una vez comprometido el dispositivo, permite al ciberdelincuente obtener un **rédito económico** por la extracción de información para su uso o venta, por el uso de los recursos del sistema infectado o extorsionando a la víctima. Para ello, se desarrollan variantes de *malware* que aprovechan, con esos propósitos, debilidades del *software* y *hardware* de teléfonos móviles, ordenadores de sobremesa y portátiles y todo tipo de sistemas.

Los desarrolladores de *malware* lo van adaptando al entorno y a las circunstancias, aplicando los **avances tecnológicos** para su elaboración y distribución. Así, por ejemplo, aprovechan el uso masivo de determinada tecnología con alguna vulnerabilidad o de errores de configuración. Su constante adaptabilidad y la existencia de un verdadero negocio rentable del *malware* hace que, en ocasiones, sea difícil de detectar y que se extienda y agrave sus efectos perjudiciales.

El *malware* se vale en gran medida de la **ingeniería social** para su distribución. Los ciberdelincuentes utilizan ingeniosas campañas de correo electrónico, SMS o mensajería instantánea; suplantan a entidades reconocidas, o apelan a las emociones de las víctimas para lograr su objetivo: que **haga clic e instale el *malware***.

Estas campañas de correos electrónicos fraudulentos principalmente distribuyen estos **tipos de *malware***:

Keyloggers

Software malicioso que registra las pulsaciones que se realizan en el teclado, realiza capturas de pantalla, etc.

Herramientas de acceso remoto o RAT (*Remote Access Tool*)

Utilizadas por los ciberdelincuentes para acceder a nuestros equipos.

Ransomware

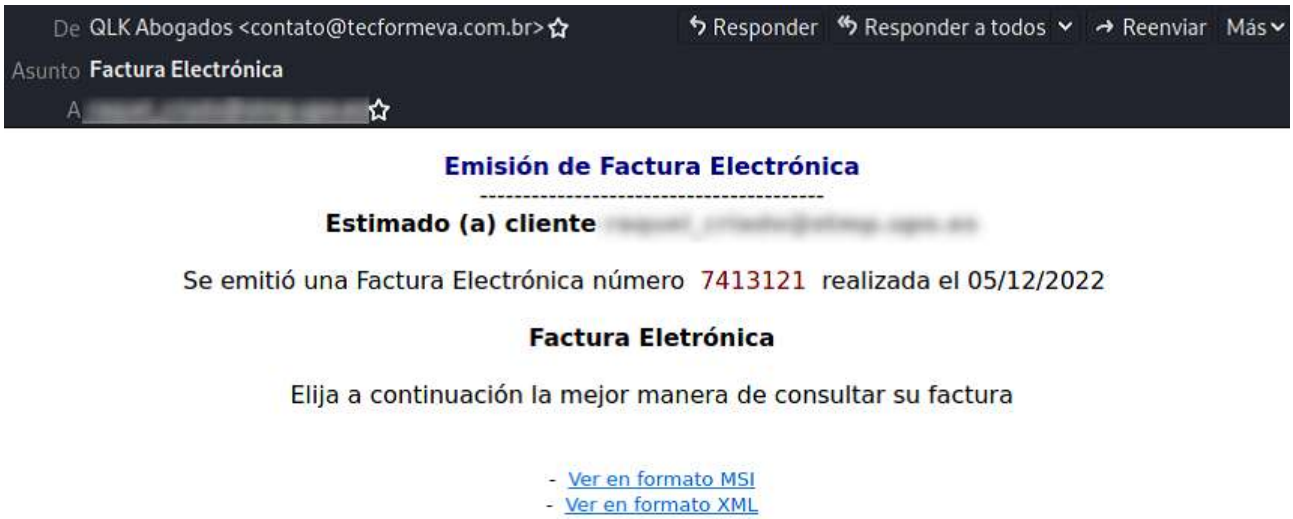


Ilustración 9. Factura falsa que distribuye malware

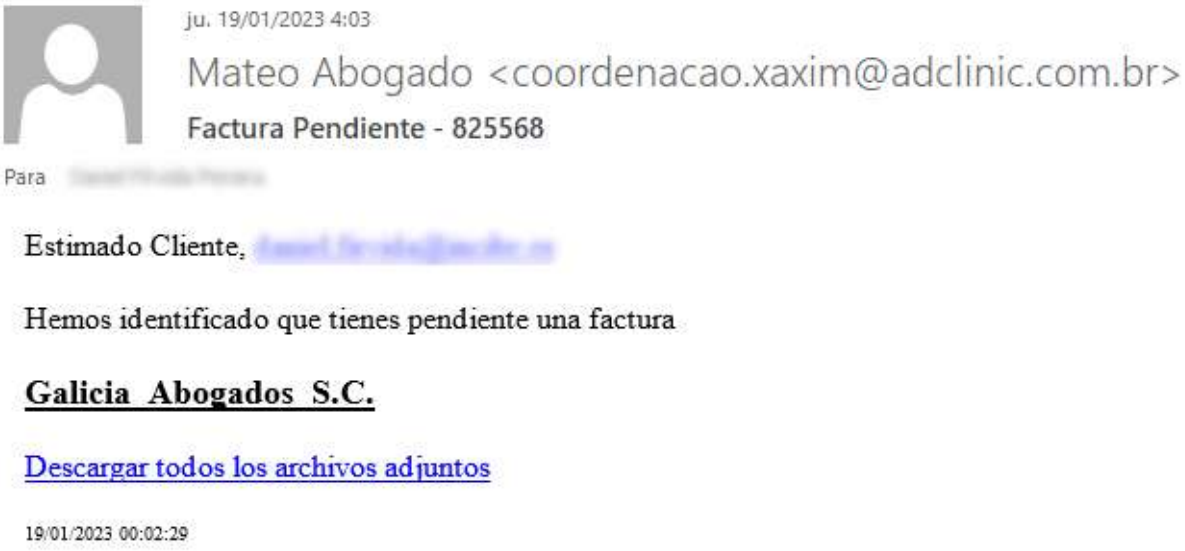


Ilustración 10. Factura falsa que distribuye malware

Responder | Responder a todos | Reenviar | Archivar | No deseado | Eliminar | Más

Agencia Tributaria
agenciatributaria796868596861034284890 4@hacienda.gob.es

Para [redacted] 8/3/24, 9:44

Ya puedes descargar El Impuesto 2024 Ref 364666376466338225 81

VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE HACIENDA
Agencia Tributaria

Emisión de Impuesto

Estimado(a) [redacted] ,

Se emitió el Impuesto respecto a su pedido Nº **778730819971022-032024**, en la fecha de **08/03/2024 as 02:49**

Elige a continuación la mejor forma de consultar tu archivo:

- Ver en formato PDF
- Ver en formato XML

Verifique todos los datos ingresados en su comprobante para conocer las medidas de

Ilustración 11. Suplantación a la Agencia Tributaria que distribuye malware

3.1.2.2.1. Ransomware, el malware que secuestra tu información

De los ataques que se están produciendo actualmente destacan por su frecuencia los producidos por ***ransomware***, un tipo de *malware* que tiene como objetivo **bloquear el uso de un equipo o parte de la información que contiene para después pedir un rescate a cambio de su liberación**. El secuestro generalmente se produce a través del **cifrado de la información del dispositivo infectado**. Esto causa un gran impacto en las víctimas, pudiendo afectar a cualquier usuario, negocio o actividad.

La infección por este tipo de *malware* se suele producir utilizando **técnicas de ingeniería social**, es decir, **engañando a la víctima para que acceda un sitio web malicioso o descargue un adjunto que contiene el *ransomware***. Este tipo de engaños suelen utilizar correos electrónicos o mensajes de texto (**SMS**) con los archivos adjuntos o enlaces maliciosos. También pueden aprovechar equipos o dispositivos vulnerables, así como otro *malware*.

El *ransomware* se manifiesta cuando el daño ya está hecho, es decir, cuando la información ha sido bloqueada, mostrando un mensaje que advierte de este hecho y pidiendo un rescate para su liberación. Dicho mensaje puede incluir **amenazas de destrucción total de la información** si no se paga e insta a realizar el pago de manera urgente.

Si tu empresa se ha visto afectada por un *ransomware*, lo más importante es **no pagar nunca el rescate y reportar el incidente [17].**

Ilustración 12. Ejemplo ransomware

3.1.2.3. Fraude email comprometido

El fraude del **correo electrónico corporativo comprometido** o **fraude BEC** [18], del inglés *Business E-mail Compromise*, es un tipo de fraude contra empresas que realizan transferencias electrónicas de dinero.

Supongamos que nuestra empresa se llama **AdminFincs S.L.**

El **ciberdelincuente** suplanta a uno de nuestros proveedores (**Proveedor S.L.**) e intercepta los correos de facturación que nos envía, cambiando la cuenta del banco donde realizar los pagos, de manera que hagamos una **transferencia** a una cuenta controlada por ellos.

Imagínate que para el último pedido, una vez acordado el precio con el proveedor, hemos quedado en que nos van a enviar la factura por medio del **correo electrónico** para realizar la transferencia. Recibimos la factura y **realizamos el pago** al número de cuenta indicado en el correo recibido.

Ilustración 13. El ciberdelincuente intercepta las comunicaciones

Pasados unos días, como no recibimos el pedido nos ponemos en contacto con **Proveedor S.L.** para reclamarlo. Una empleada de **Proveedor S.L.** nos indica que aún no han recibido el pago, requisito indispensable para realizar el envío.

Desde **AdminFincs S.L.** enviamos el justificante de la transferencia. Al comprobar el justificante, una empleada de **Proveedor S.L.** nos advierte que ese no es su número de cuenta bancaria. **¿Qué ha sucedido?** Puede ser que nuestra cuenta de correo o la de nuestro proveedor estén comprometidas, es decir, **controladas por el ciberdelincuente**.

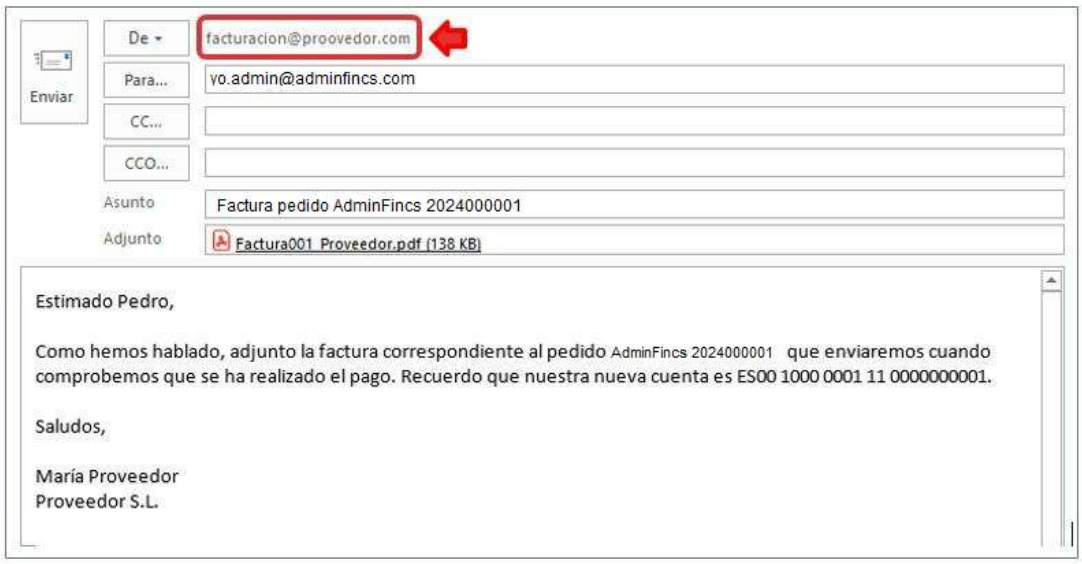


Ilustración 14. Correo fraudulento suplantando al proveedor legítimo

Caso 1: nuestra cuenta de correo está comprometida

El ciberdelincuente ha podido acceder a nuestra cuenta y ha creado una regla de entrada en nuestro buzón de correo. Esta regla funciona reenviando todo el correo procedente de ***facturacion@proveedor.com*** a una cuenta de correo desconocida, ***ciberdelincuente@email.ru***. Además, mueve el correo de la bandeja de entrada a una carpeta oculta para que no lo detectemos.

Si revisamos las cabeceras del correo **[19]** que hemos recibido con la cuenta bancaria modificada, se detecta que la dirección desde la que se envió la factura es ***facturacion@proveedor.com***. El atacante ha creado un dominio muy parecido al de **Proveedor S.A.** para suplantar su identidad y cometer el fraude.

Caso 2: cuenta de correo del proveedor comprometida

En este caso, **Proveedor S.A.** recibe llamadas de clientes que han recibido correos con facturas con el número de cuenta modificado, es decir, su correo está comprometido. Aparentemente, los correos se envían desde la dirección legítima.

Se detecta una regla de salida en el buzón de correo de **Proveedor S.A.** que ellos no habían configurado. Esta regla funciona interceptando todo el correo saliente con facturas hacia clientes y los reenvía a una cuenta de correo desconocida, ***ciberdelincuente@email.ru***.

Es posible que su cuenta siga comprometida, ya que los correos a clientes están siendo enviados desde el correo legítimo. Es probable que el ciberdelincuente esté interceptando toda la información que llega al buzón del proveedor para posteriormente acceder al **correo de facturación del proveedor** para cometer el fraude.

3.1.2.4. ¿Cómo acceden los ciberdelincuentes a nuestras cuentas de correo?

Si los ciberdelincuentes han conseguido las credenciales de nuestro correo electrónico, esto puede ser porque:

- Han entrado en nuestra cuenta de correo por **falta de concienciación**:
  - Tenemos **equipos sin acceso** por contraseña.
  - Nuestras **contraseñas están escritas** en papeles accesibles o a la vista.
  - Tenemos las **contraseñas almacenadas en texto plano en el propio equipo**, es decir, en cualquier fichero.
  - Utilizamos **contraseñas poco robustas**.
  - **No utilizamos doble factor de autenticación**.
- Si han obtenido las **credenciales de nuestra cuenta de correo**:
  - Utilizando **ingeniería social**.
  - Hemos introducido las credenciales (usuario y contraseña) al caer en alguna campaña de ***phishing*** suplantando a otra empresa, bancos, entidades de referencia, herramienta o servicio (*cloud*, Microsoft 365, etc.).
  - ***Shoulder surfing:*** visualizan las credenciales cuando las tecleamos o si hay una cámara espiando.
- Hemos sido infectados por *malware* que puede espiar y robar nuestras credenciales. En particular, un ***keylogger***, que es un *malware* que registra nuestras pulsaciones en el teclado. Este también puede ser de tipo *hardware*. Por ello, revisaremos que no hay ningún **dispositivo extraño** conectado a nuestros ordenadores y servidores.
- Lanzan **ataques automatizados** contra el servidor de correo con contraseñas comunes o contraseñas filtradas por brechas de seguridad:
  - ***Password spraying*** o ataque de fuerza bruta, probando de manera automatizada y lentamente para no ser detectados una a una contraseñas de uso común (12345678, 11111111, administrador...) de una lista contra las cuentas del servidor de correo, hasta que consiguen entrar.
  - **Relleno de credenciales reutilizadas** (*credential stuffing / credential reuse*): los ciberdelincuentes prueban de manera automatizada pares de nombres de usuario y contraseña extraídos de alguna filtración. Se aprovechan de una mala práctica extendida que consiste en la reutilización de credenciales de aplicaciones personales (por ejemplo, redes sociales o servicios de *streaming*) en aplicaciones del entorno corporativo como el correo. De ahí, la importancia de **utilizar contraseñas únicas en cada servicio**. También se recomienda por el mismo motivo no utilizar la cuenta corporativa para registrarse en plataformas ajenas a las de la propia empresa.
- **Podemos comprobar si alguna de nuestras cuentas está en una filtración** que haya tenido lugar debida a brechas de seguridad de algún servicio, red social o aplicación que utilicemos:
  - **Have i been pwned**
  - **Mozilla Monitor**

- Si **han entrado en nuestros sistemas:**
  - Aprovechando **vulnerabilidades [20]** no parcheadas en el servidor de correo o errores de configuración.
  - O porque tenemos *software*, sistemas operativos o navegadores **desactualizados y son vulnerables.**

- **Han tenido acceso al correo y lo han manipulado, pero no tienen las credenciales:**
  - **Dejamos las sesiones abiertas** cuando no estamos delante del ordenador en un entorno abierto.
  - Utilizamos el **correo en equipos de uso compartido o en lugares públicos.**
  - Los ciberdelincuentes utilizan ***malware tipo RAT*** *(Remote Access Trojan)* o vulnerabilidades de acceso remoto.
  - La **wifi [21]** está comprometida o no está bien configurada y enviamos los correos sin cifrar.

3.1.2.5. Otros tipos de fraudes que pueden afectar a los despachos de administración de fincas

Como adelantábamos, los correos de ***phishing***, de distribución de ***malware*** y del **email comprometido** son los que más afectan a los despachos de administración de fincas, pero también tenemos que tener en cuenta las siguientes **amenazas** que pueden poner en peligro nuestros negocios.

3.1.2.5.1. Fraude del CEO

El **fraude del CEO** se trata de un ataque dirigido contra una víctima en concreto, de la cual se ha recopilado información previamente por distintos medios, como la página web corporativa, redes sociales profesionales o cualquier otro medio, cuyo objetivo es **hacer que el ataque sea más creíble**. En este fraude se atacan dos objetivos de la misma organización: un **alto directivo** de la empresa y un **empleado** con capacidad para poder realizar transferencias bancarias.

Los **ciberdelincuentes** suplantan la identidad de un alto directivo y solicitan a un empleado, con capacidad de realizar transacciones financieras, una **transferencia de dinero**, que generalmente suele ser de un monto importante, alegando cerrar una operación reseñable en la que se está trabajando. Las comunicaciones suelen producirse por medio del **correo electrónico** y utilizando direcciones falseadas, ***email spoofing*** o ***typosquatting*** **[22]**, aunque a veces se usa la dirección legítima del directivo que previamente se ha comprometido.

Esta técnica suele ser llevada a cabo por los ciberdelincuentes, coincidiendo con la **ausencia del directivo suplantado de la sede**, debido a viajes de negocio o cualquier otra eventualidad, ya que así se dificulta verificar la comunicación. El **empleado**, al comprobar que la comunicación proviene de un alto directivo, **no suele dudar de la solicitud** y realiza la transferencia bancaria, produciéndose finalmente el fraude. En muchas ocasiones, la solicitud de transferencia va acompañada de una **petición de urgencia y confidencialidad**, buscando como objetivo que el empleado no se comunique con otros compañeros y que el fraude se realice con la mayor brevedad posible.

Este tipo de ataques dirigidos suelen estar orientados a **organizaciones de tamaño medio o grande**, donde el rédito económico es mayor.

Consulta los **casos reales de la Línea de Ayuda 017** si quieres conocer más detalles sobre este fraude.

3.1.2.5.2. Fraude de RR.HH

El **fraude de RR.HH.** utiliza técnicas similares al fraude del CEO, pero en esta ocasión las víctimas son el **personal de recursos humanos de la empresa** y un **empleado** al que suplantan su identidad.

En la comunicación **el ciberdelincuente se hace pasar por un empleado de la empresa** y solicita que el siguiente ingreso correspondiente a su nómina se realice a un nuevo número de cuenta controlado por el estafador. Para perpetrar el ataque, los ciberdelincuentes han realizado un estudio previo de la empresa víctima, identificando a los empleados del Departamento de Recursos Humanos, los empleados con los que cuenta la empresa, la entidad financiera con la que trabaja y las cuentas de correo electrónico utilizadas. Al igual que otros tipos de fraudes, para dotar de más veracidad a la comunicación fraudulenta, los ciberdelincuentes utilizan técnicas de ***email spoofing*** o ***cybersquatting*** **[23].**

¿Cómo identificar un ataque de fraude de RR.HH. y poder prevenirlo?

Las pautas para identificar este tipo de estafa son similares al fraude del CEO, siendo la principal diferencia la **solicitud de cambio de cuenta bancaria por un empleado de la organización**. Ante cualquier correo que parezca proceder de un empleado de la empresa, se debe **verificar dicha solicitud mediante otro medio de comunicación**, como una llamada telefónica o presencialmente. Así, se podrá verificar sin ninguna duda si el cambio de cuenta bancaria es legítimo o no.

Ilustración 15. Correo real fraude RR.HH.

3.1.2.5.3. Fraude del falso soporte técnico

Una llamada de un supuesto técnico de Microsoft avisando sobre múltiples **errores de seguridad** detectados en los dispositivos de la empresa es el comienzo de un **fraude** que podría saquear las cuentas e información estratégica y confidencial de cualquier organización.

En el fraude del falso soporte de Microsoft el estafador **suplanta la identidad de un técnico de esta compañía** con el pretexto de solucionar ciertos problemas técnicos en el equipo, siendo su objetivo real **comprometer la seguridad y privacidad del dispositivo afectado** y, por lo tanto, de la propia empresa. **Los ciberdelincuentes contactan con la víctima mediante dos vías diferentes:**

- **Llamada directa a un teléfono de la organización.** Los ciberdelincuentes contactan directamente con un empleado de la empresa haciéndose pasar por técnico de soporte de Microsoft. En la llamada informan que los dispositivos de la empresa están en peligro y deben llevarse a cabo acciones de inmediato para garantizar la seguridad.

- **Página de error fraudulenta.** Los ciberdelincuentes crean páginas falsas de error donde se indica al usuario que su equipo está en riesgo y debe ponerse en contacto con ellos para solucionar los problemas. En la página se muestra un número de teléfono al que llamar, donde supuestamente ayudarán a solucionar los fallos.

Una vez se establece la comunicación telefónica, los ciberdelincuentes suelen proporcionar una serie de **datos técnicos para dar más credibilidad al fraude**. El siguiente paso es indicar a la víctima que debe **instalar un *software* de acceso remoto para poder solucionar los problemas**. Esta herramienta permitirá al ciberdelincuente acceder al equipo y tomar el control del mismo, con el consiguiente riesgo para la privacidad y seguridad de la empresa. En una variante de este fraude los ciberdelincuentes solicitarán el **pago de una cantidad determinada de dinero a cambio de solucionar los supuestos problemas de seguridad**. Además, permitir el acceso remoto puede tener otras **consecuencias**, como:

- **Fugas de información.** Al permitir el acceso de los ciberdelincuentes al dispositivo corporativo, estos pueden acceder a información confidencial e incluso a datos privados de clientes.

- **Robo de credenciales de acceso e información bancaria.** Los dispositivos pueden almacenar nombres de usuario y contraseñas de acceso, particularmente en los navegadores web, a diferentes servicios de la empresa que pueden ser robados. También pueden robar información bancaria en caso de que se encuentre almacenada en el dispositivo.

- **Instalación de *malware*.** En algunos casos pueden instalar software malicioso que puede provocar diferentes situaciones de riesgo, como fugas de información, incluso utilizarlo para perpetrar otros tipos de fraude o impedir el acceso a la información que contiene por medio de un *ransomware*.

3.2. Amenazas al sitio web corporativo

Hoy en día las **webs corporativas son un activo muy importante para los despachos de administración de fincas**, ya que se trata del escaparate en Internet, permitiendo ofrecer sus servicios de manera global, llegando así a un mayor número de clientes. Por lo tanto, **un incidente de seguridad relacionado con el sitio web podría perjudicar seriamente a la continuidad de negocio**.

Las webs son objetivos de los ciberdelincuentes por diversos motivos. El principal suele ser el **beneficio económico**, pero también **hacerse con información confidencial** y utilizar dicha información para perpetrar otros ataques o simplemente para dañar la imagen del despacho, por lo que **disponer de un portal web funcional, seguro y que cumpla las necesidades de los trabajadores y clientes**, es imprescindible.

Los incidentes de seguridad, cuyo origen está en el sitio web corporativo, se producen principalmente por los siguientes **motivos:**

- **Vulnerabilidades no parcheadas:** entendiendo como vulnerabilidad un fallo o deficiencia en un *software*, que puede ser utilizado por un ciberdelincuente para llevar a cabo acciones maliciosas. Los sitios web pueden contar con vulnerabilidades que, si no son parcheadas, podrían llegar a ser explotadas, causando un incidente de seguridad.

- **Malas configuraciones:** a través de acciones como permitir contraseñas simples, no aplicar sistemas de verificación tipo captcha o mostrar más información que la estrictamente necesaria cuando se produce un error, pudiendo estas malas prácticas suponer el origen de un incidente de ciberseguridad.

- **Errores de diseño:** produciéndose cuando una web no está diseñada siguiendo unos estándares de seguridad, como el elaborado por la **Fundación OWASP** [24]. Esto origina que la web contenga errores de diseño, los cuales podrían ser la puerta de entrada a nuestro portal web.

Si finalmente estos errores de seguridad dan lugar a un incidente, podrían tener lugar varias situaciones que comprometan la seguridad y privacidad del despacho y, por ende, de sus clientes:

- **Fugas de información:** lo que puede dar lugar a la pérdida de confidencialidad de la misma, siendo accesible por personas no autorizadas. Estas fugas de información pueden dar lugar a sanciones económicas, debido a un incumplimiento de la LOPDGDD, o a extorsiones por parte de los ciberdelincuentes, entre otros incidentes. En cualquier caso, siempre van a tener un impacto negativo en la imagen y reputación de la organización.

- **Ataques de denegación de servicio o DoS [25]**, por sus siglas en inglés (*Denial of Service*), que tienen por objetivo dejar un servidor inoperativo. Como consecuencia, este tipo de ataques provocan que tanto clientes como trabajadores no puedan interactuar con el sitio web de forma normal, lo que puede afectar gravemente a la continuidad del negocio y a la imagen del despacho.

- **Defacement [26]**: ataque que consiste en cambiar la apariencia de la web corporativa por otra a elección del ciberdelincuente con diversos motivos, como:

  - **Dañar la imagen del despacho**, generando así desconfianza entre sus clientes.

  - **Alojar un sitio falso,** con el fin de ganar dinero, por ejemplo, una página de *phishing* de una entidad bancaria.

  - **Distribuir *malware* o contenido catalogado como *spam.***

  - **Llevar a cabo acciones de vandalismo,** como enviar mensajes de protesta.

También hay que tener en cuenta que **cuando un ciberdelincuente vulnera la seguridad del sitio web corporativo, puede llegar a comprometer otros sistemas de la organización**, como el correo electrónico, o dispositivos, como ordenadores o aparatos **IoT** *(Internet of Things)* **[27]**, etc.

3.3. Amenazas en redes sociales

Hoy en día las **redes sociales** son una herramienta de gran valor para muchos despachos, permitiendo dar a conocer sus servicios de una manera muy **visual e interactiva**, y a la vez estableciendo un trato más cercano con los actuales o potenciales clientes.

Los despachos se valen de estas aplicaciones para **llegar a un gran número de usuarios**, de una manera mucho más personal, en comparación con cómo se presenta un despacho en una página web.

Pero en este escenario tan ventajoso no podemos ignorar que muchas veces las redes sociales son un **blanco fácil para los ciberdelincuentes**, sobre todo si como administradores desconocemos los riesgos asociados a su uso. Debemos prestar especial atención a ciertas campañas maliciosas que se llevan a cabo a través de las redes sociales, como:

- Los fraudes por **suplantación de clientes o proveedores.**
- Las campañas de ***malware.***
- Las campañas de ***phishing.***

Ilustración 16. Objetivo del robo/suplantación en redes sociales

Consulta el artículo **"Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas"** si han suplantado el perfil de tu despacho y necesitas sabes cómo debes actuar.

3.4. Riesgos del *software on-premise*

En los despachos de administración de fincas es muy habitual la utilización de ***software on-premise***, es decir, aquel que se instala en los propios servidores y entorno informático del despacho.

En este caso, seremos los responsables de velar por la seguridad de nuestros sistemas para evitar posibles ataques que puedan comprometer nuestra información. Por tanto, debemos conocer **cuáles son las principales amenazas** del modelo *on-premise* tanto si ya lo estamos utilizando como si lo estamos valorando como opción:

- **Acceso no autorizado [28]:** la falta de controles de acceso adecuados puede permitir a los ciberatacantes obtener acceso a los servidores y, por ende, comprometer la seguridad de los datos que almacenan.
- **Ciberataques:** estos servidores están expuestos a diversos ataques, como, por ejemplo, a ataques de ***malware*** o de **denegación de servicio (DDoS)**, que pueden comprometer la seguridad de los sistemas, además de afectar seriamente a la continuidad de negocio.
- **Vulnerabilidades en el *software* instalado:** las vulnerabilidades no parcheadas podrían ser explotadas por los ciberdelincuentes para obtener acceso no autorizado al sistema y dar lugar a una brecha de datos. La falta de actualizaciones regulares puede poner en peligro los sistemas.

3.5. Riesgos del *software* en la nube

El ***software* en la nube o *cloud computing*** **[29]** es un c**onjunto de soluciones accesibles desde Internet ofrecidas por diferentes proveedores**, de manera que las empresas no precisan realizar grandes inversiones iniciales en infraestructura o ***software.***

Estos servicios ofrecen a los despachos la posibilidad de **escalar el negocio de manera más sencilla y con la flexibilidad de disponer de los recursos necesarios en menor tiempo**, así como pagar por solo aquello que se utiliza.

Como hemos comentado, **cada negocio deberá escoger lo que más se adapte a sus necesidades**, aunque lo más habitual en los despachos de administración de fincas es contar con aplicaciones ***SaaS*[1]*, como CRM, ERP*** y soluciones de gestión documental alojadas en lo que se conoce como nube pública[2].

¿Qué riesgos puede suponer el uso de software en la nube para los despachos de administración de fincas?

La tendencia es que cada vez más despachos apuestan por trabajar y ofrecer sus servicios desde la nube. Esto permite abaratar costes, acceder desde cualquier dispositivo y lugar o trabajar de forma colaborativa.

No obstante, los empleados que hagan uso de la nube deben conocer cómo realizar una buena gestión de los **recursos de almacenamiento**. Para ello, se contará con una política de clasificación de información **[30]** que indique qué tipo de información puede subirse a la nube. Además, contará con una normativa interna para el tratamiento y cifrado de la información confidencial. También se deben establecer procedimientos para aplicar otras medidas de seguridad, como *backups* o borrados seguros de información.

Los recursos en la nube están expuestos a **amenazas de ciberseguridad**: **filtraciones de datos**, ***ransomware***, **ataques DDoS** (denegación de servicio distribuida) o ***phishing***. Los **ciberatacantes** podrían explotar fallos de seguridad o malas configuraciones utilizando credenciales robadas o *malware* para perpetrar ataques, interrumpir servicios o robar datos confidenciales.

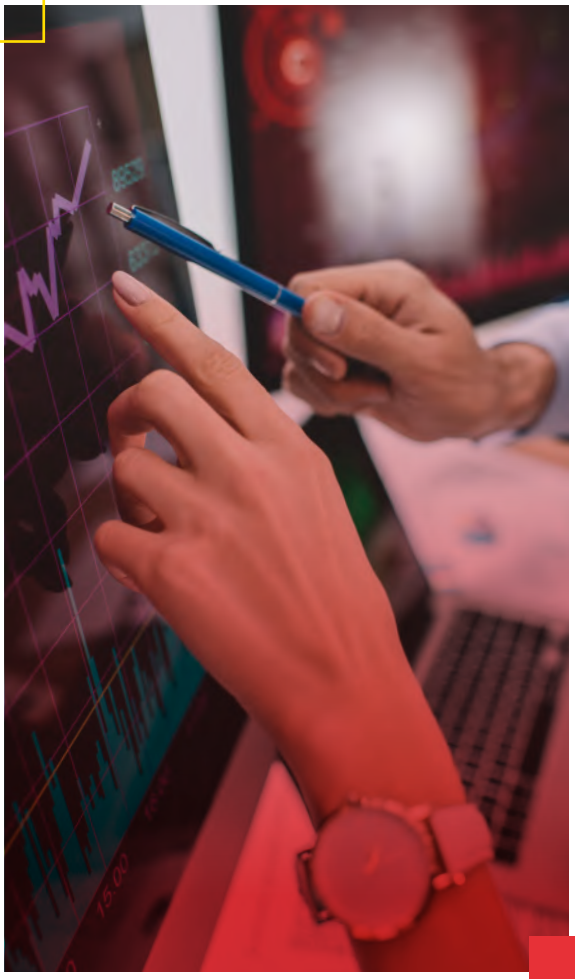
[1] Software como servicio (Saas): El proveedor ofrece aplicaciones de software a los clientes a través de Internet. Estos servicios son mayormente utilizados para almacenamiento e intercambio documental por parte de las empresas.
[2] Nube pública: el proveedor es el responsable del mantenimiento de la infraestructura, debido a que se encuentra en sus instalaciones.

4. Medidas de ciberseguridad para el sector de administraciones de fincas

Los **despachos de administración de fincas** se enfrentan a grandes amenazas en materia de ciberseguridad. Una brecha de seguridad puede ocasionar una pérdida de confianza por parte de los clientes, daño a la reputación de la empresa, pérdidas económicas y perjuicios legales. Pese a que estos ataques crecen exponencialmente, muchos de estos **riesgos** pueden ser evitados o al menos controlados, minimizando así su impacto, si aplicamos ciertas medidas de ciberseguridad y, sobre todo, el sentido común.

4.1. Protección de datos

En el **sector de la administración de fincas** se maneja una alta cantidad de datos e información de carácter personal, como pueden ser nombres de los propietarios, documentos nacionales de identidad, direcciones postales, acuerdos, contratos e incluso cuentas bancarias, entre muchos otros. Es de vital importancia conocer **cómo tratar estos datos** adecuadamente y prevenir que se produzca una fuga de información.



Para tratar datos de carácter personal de los copropietarios de una comunidad de propietarios en virtud de un encargo de servicios o gestiones de las comprendidas en la LPH [31], **se deberá contar con el consentimiento específico, informado e inequívoco de todos los afectados.**

Adicionalmente, **no solo se debe proteger la información de posibles fugas, también se debe garantizar la confidencialidad de los datos.** Por ello, es necesario conocer la normativa aplicable en protección de datos y asegurar que se aplican las medidas de seguridad adecuadas para su resguardo.

Responsabilidad de los administradores de fincas

Un aspecto a tener en cuenta es que los administradores de fincas que representan a las comunidades de propietarios suelen actuar como encargados del tratamiento en relación con los datos de los propietarios, siendo la **Comunidad de Propietarios** la responsable del tratamiento.

El administrador de fincas debe tener acceso a los datos personales recabados por la **Comunidad de Propietarios**, con la única finalidad de asesorar a la comunidad en aquellos usos que se realicen conforme a la **Ley de Propiedad Horizontal**.

En este sentido, como encargado de tratamiento, el administrador de fincas debe firmar un contrato con la **Comunidad de Propietarios** en el que se incluyan los tratamientos concretos y específicos a realizar, atendiendo al servicio prestado por el administrador.

Asimismo, los contratos o acuerdos tratados por los administradores de fincas incluirán cláusulas de confidencialidad en las que se garantizará por parte de la empresa la protección de la información.

La importancia de mantener la confidencialidad de la información

Asegurar la **confidencialidad** de la información es imprescindible para las empresas del sector de administración de fincas, ya que protege la privacidad de los datos, demuestra que se cumple con las regulaciones y normativas legales aplicables, previene la posibilidad de incumplimiento y litigios por fuga de información (sea esta intencionada o no), otorga seguridad en el ámbito bancario y aporta una mejor imagen y reputación de la empresa de cara a los clientes.

Protección de la privacidad de los propietarios e inquilinos

- **Los administradores de fincas están autorizados a manejar información personal de sus representados**, es decir de los propietarios e inquilinos. Esta información es de carácter personal, por lo que mantener a resguardo la información es esencial para proteger la privacidad de los clientes.
- **Los propietarios e inquilinos depositan la confianza en los administradores de fincas,** esperando que esta información otorgada sea tratada de la manera más segura posible y que se tomen las medidas oportunas para asegurar su confidencialidad e integridad.
- **Las empresas del sector gestionan información financiera de sus clientes**, en las que se incluyen transacciones bancarias, pagos y presupuestos. Es de vital importancia que se mantenga esta información segura de fugas y para evitar fraudes.

Regulaciones y cumplimiento normativo

- **Las compañías que traten datos de carácter personal deben cumplir con las leyes y regulaciones en materia de protección de datos, en concreto el Reglamento General de Protección de Datos (RGPD)** [32] y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) [33], así como respetar lo dispuesto en la Ley 49/1960, de 21 de julio, sobre Propiedad Horizontal y la Ley 8/1999 que la modifica.
- **El incumplimiento de estas leyes puede conllevar sanciones administrativas y económicas.**

Conflictos y litigios

- **La fuga o revelación de la información confidencial** tratada por los administradores de fincas puede generar conflictos entre las partes involucradas: inquilinos, propietarios y administradores, lo que puede derivar en pérdidas económicas derivadas de sanciones, pérdida de confianza de los clientes, daño en la imagen y reputación de la empresa, consecuencias legales, etc.
- **La responsabilidad legal de la filtración** de cualquier tipo de información **recae sobre los administradores de fincas**, y ante una fuga de información, puede derivar en demandas y litigios.

Impacto reputacional

- **Ofrecer una imagen profesional viene relacionado con saber mantener la confidencialidad de la información y manejar de manera segura todos los datos**. Proporciona una imagen más valorada por los clientes, ya que ofrecen una mayor confianza.
- **Estar implicado en una fuga de información por no mantener la confidencialidad de los datos puede repercutir negativamente en la imagen que la empresa proyecta a sus clientes.** Esto puede llevar a una pérdida de reputación y confianza que se vea reflejado en la disminución de la cartera de clientes.

Notificación de brechas de seguridad

Una de las obligaciones que establece la normativa de protección de datos es la notificación de brechas de seguridad que se produzcan en la empresa, tanto a los afectados como a la Agencia Española de Protección de Datos (AEPD). **En el caso de que se haya sufrido una brecha, a causa de un ciberataque o una infracción**, se debería contar con un plan de gestión de incidentes. Según la AEPD, existe un **plazo de 72 horas para notificar a las autoridades** de esta situación, así como facilitar la información.

4.1.1. Guía AEPD

La **Agencia Española de Protección de Datos** ha elaborado una guía para facilitar al sector de la administración de fincas todo lo relativo al conocimiento y cumplimiento de la normativa de protección de datos. **Consulta esta guía** para estar al tanto de todo lo necesario en materia de protección de datos que pueda afectarte como administrador de fincas.

4.1.2. ¿Qué es la fuga de información?

Sin duda, **uno de los peores incidentes a los que puede enfrentarse un despacho de administración de fincas es la fuga de información.** El término fuga de información se utiliza para denominar la pérdida de confidencialidad[3] ocasionada como consecuencia de un incidente de ciberseguridad interno o externo (**independientemente de que haya sido intencionado o no**), pudiendo afectar tanto a su integridad[4] como a su disponibilidad[5].

Las fugas de información pueden ser de dos tipos:

Internas, de forma consciente: venganza de empleados descontentos, espionaje industrial, etc. **Internas de forma inconsciente:** pérdida de documentos o dispositivos, falta de formación o desconocimiento, etc.

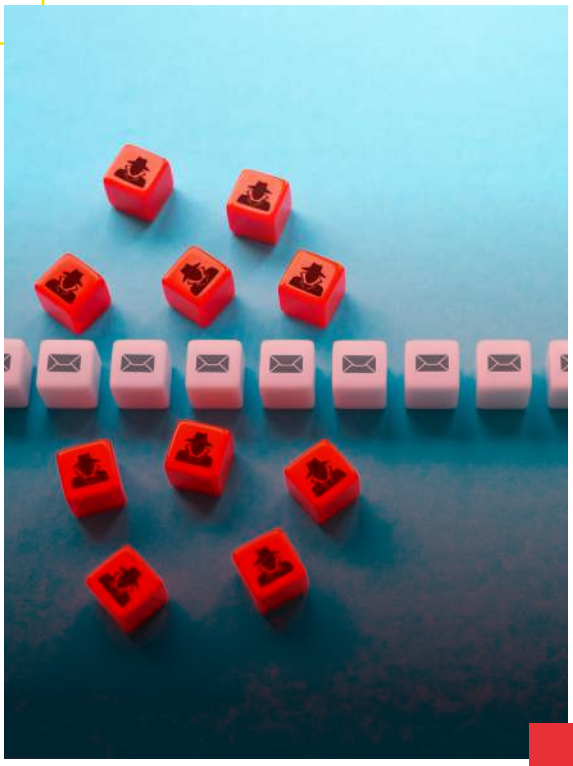
Externas, generalmente procedentes de terceros con fines ilícitos, que buscan acceder a la información confidencial sin autorización: ciberdelincuentes, clientes descontentos, antiguos empleados, etc.

4.1.3. Prevención de fuga de información

Aunque somos conscientes de que la seguridad al cien por cien no existe, disponemos de herramientas que nos ayudan en este proceso. Las siglas **DLP** provienen del inglés ***Data Loss Prevention***, que significa prevención de pérdida de datos. Consiste en un conjunto de herramientas y procesos diseñados para permitir la **identificación de la información sensible** de la organización y prevenir una posible fuga de información.

Mediante la implantación de una solución DLP, se pretende controlar el movimiento de los datos a través de todas las vías utilizadas, como el correo electrónico, la nube, los dispositivos móviles, etc.

Las **soluciones DLP** funcionan con la ayuda de reglas y directivas que se gestionan a través de un *software* y evitan que se filtre la información confidencial de la organización.



[3] La confidencialidad implica que la información es accesible únicamente por el personal autorizado.
[4] La integridad de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores.
[5] La disponibilidad de la información hace referencia a que la información esté accesible cuando la necesitemos.

¿Qué aspectos se deben tener en cuenta a la hora de elegir una solución DLP?

En el mercado existen multitud de soluciones DLP, cuya función es la de proteger los datos empresariales. Algunos **aspectos relevantes** a la hora de evaluar estas soluciones son los siguientes:

- **Identificar las necesidades de la empresa:** definir qué tipo de datos se necesita proteger y cuáles son las regulaciones y normativas aplicables.

- **Cobertura y alcance:** cerciorarse de que la solución cubra la totalidad de los canales a través de los cuales pueden moverse los datos (correo electrónico, almacenamiento en la nube, dispositivos extraíbles...) y verificar que sea compatible con otras aplicaciones del despacho.

- **Especificaciones técnicas:** cada solución puede ofrecer diferentes funcionalidades, entre ellas:
  - Monitoreo en tiempo real y control de bloqueo/desbloqueo.
  - Clasificación de los datos.
  - Integración con otros sistemas de seguridad.

- **Facilidad de uso y gestión:** las herramientas con interfaces intuitivas y fáciles de utilizar nos permitirán gestionar las alertas y políticas de forma más eficiente. Asimismo, sería de utilidad la posibilidad de generar informes detallados.

- **Actualizaciones y soporte:** se deberá verificar que la solución cuenta con actualizaciones regulares para una mayor seguridad y que el proveedor ofrece soporte técnico.

- **Escalabilidad:** se deberá asegurar la escalabilidad de la solución por si crecieran las necesidades del despacho.

- **Costes:** se deberá tener en cuenta la inversión necesaria para la implementación, así como el valor que proporcionará en cuanto a prevención de pérdida de datos.

Tipos de DLP

Según el enfoque y las funcionalidades que ofrecen, existen diferentes tipos de **soluciones DLP**. Cada una de ellas proporciona una estrategia de prevención de pérdida de datos diferente y puede ser más recomendable para cierto tipo de organizaciones. A continuación, se enumerarán las diferentes soluciones y cómo pueden ayudar en el sector administración de fincas.

- **EDLP (*Entreprise Data Loss Prevention*):** este tipo de soluciones ofrece una estrategia integral de prevención de pérdida de datos. Permiten establecer políticas que protegen la información confidencial y las gestiona de forma centralizada, así como generar informes. En el sector de la administración de fincas puede ayudar a prevenir que la información confidencial, como los datos personales de propietarios, inquilinos, contratos, etc., sean compartidos accidentalmente a través del correo electrónico o de otros medios no autorizados.

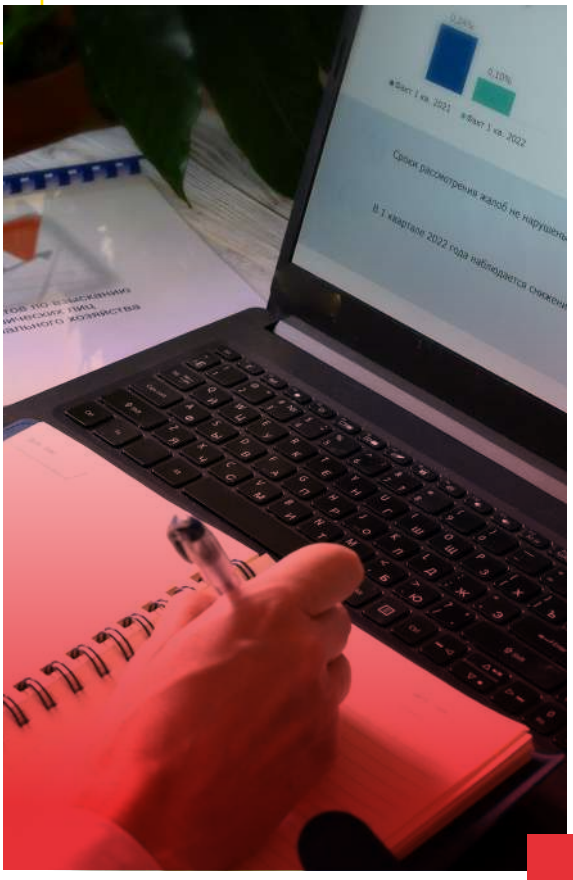
- **IDLP *(Integrate Data Loss Prevention):*** estas soluciones se integran directamente con las aplicaciones y sistemas de la organización, actuando como una capa extra de protección. En el sector de la administración de fincas podría integrarse con sistemas de gestión de propiedades, con el correo electrónico o con servicios de almacenamiento en la nube.

- **DLP centradas en la nube:** este tipo de soluciones están enfocadas en la seguridad de los datos en servicios y aplicaciones en la nube. En el sector de la administración de fincas, en el que muchas operaciones se gestionan a través de plataformas en la nube, este tipo de soluciones pueden ayudar a restringir los accesos no autorizados y evitar que la información confidencial sea manipulada por usuarios sin permisos.

¿Qué beneficios puede suponer la implantación de una solución DLP en un despacho de administración de fincas?

La implementación y uso de soluciones de prevención de pérdida de datos en la pueden ayudar a gestionar los accesos a la información, proteger los datos, facilitar el trabajo en remoto de manera más segura y aportar una mejor valoración por parte del cliente al ofrecer una mayor confianza. **Contar con una solución DLP puede aportar a nuestro despacho:**

- **Protección de la información confidencial**: las empresas de este sector manejan a diario una gran cantidad de información confidencial, como los datos personales de los propietarios e inquilinos, información financiera, contratos, etc. La implantación de una solución DLP asegura la protección de este tipo de información, evitando que sea filtrada, ya sea de forma accidental o por usuarios malintencionados.



- **Cumplimiento normativo:** las soluciones DLP ayudan a las empresas a cumplir con normativas y regulaciones, como el RGPD o la LOPDGDD, de obligado cumplimiento para el sector de administración de fincas. Esto puede evitar implicaciones legales, multas e, incluso, daños a la reputación de la empresa.

- **Gestión de accesos:** controla que solo el personal autorizado disponga de acceso a la información sensible mediante la implementación de políticas de acceso basadas en roles. Permite la monitorización del uso de los datos, registrando también cómo y cuándo se accede a la información para detectar patrones sospechosos.

- **Prevención de la fuga de información:** el bloqueo de ciertas acciones no autorizadas puede prevenir que los empleados compartan información confidencial a través del correo electrónico, las aplicaciones de mensajería instantánea, dispositivos de almacenamiento extraíble o los servicios de almacenamiento en la nube.

- **Seguridad en el trabajo remoto:** las soluciones DLP protegen la información confidencial, permitiendo la conexión desde diferentes ubicaciones y dispositivos, sin poner en riesgo la seguridad de la compañía cuando los empleados se encuentran trabajando fuera de la seguridad de la oficina.

- **Mejora de la confianza del cliente:** los clientes perciben que sus datos se encuentran más protegidos cuando las empresas implementan soluciones DLP. Esto puede ser contemplado como una demostración de compromiso hacia los clientes, que puede conllevar una mejora de la imagen y reputación y en una mayor fidelización.

4.1.4. Conservación de la información

Los **plazos de conservación de la información** previo a su destrucción varían, en el ámbito nacional, en función del tipo de documentación y de la normativa que se le aplica. Respecto a los **tipos de documentación que trata una empresa del sector de la administración de fincas** se pueden encontrar:

Documentación societaria

- Toda la documentación relacionada con las **escrituras de constitución y registro de la sociedad**, estatutos sociales, escrituras de elevación de acuerdos sociales, otorgamiento/renovación de poderes escritura de compraventa y otro tipo de documentación societaria.

  Plazo: se recomienda conservarla durante toda la vida de la sociedad, desde su constitución hasta como mínimo 6 años después de su disolución o liquidación.

Documentación fiscal y tributaria

- **Justificantes** de ingresos y gastos, contratos, facturas, recibos, albaranes, todo tipo de declaraciones fiscales.

  Plazo: obligación de conservar la documentación mínimo 4 años. Arts. 66, 67 y 68 de la Ley General Tributaria. Respecto a las declaraciones fiscales, el periodo de prescripción de 4 años empieza a contar a partir del día en el que finaliza el plazo de presentación voluntaria de impuestos. En caso de actuación posterior de la Administración o del sujeto pasivo que haya interrumpido la prescripción, comenzará un nuevo plazo de 4 años a partir de esa actuación.

- La **Orden EHA/962/2007** contempla la posibilidad de destruir las facturas recibidas en papel si previamente se ha realizado un proceso de digitalización certificada que obtiene copias digitales firmadas electrónicamente.

Documentación contable

- Libro diario, libro de inventarios y cuentas anuales, informes de auditoría, informes del administrador, correspondencia, documentación y justificantes concernientes al negocio, etc.

  Plazo: obligación de conservar la documentación un mínimo de 6 años a partir del último asiento realizado en los libros. Art. 30 del Código de Comercio.

Documentación contable

- **Contratos y otra documentación laboral**.

  Plazo: mínimo 4 años desde su firma. Ley de Infracciones y Sanciones del Orden Social.

- **Infracciones laborales.**

  Plazo: regla general de prescripción de las infracciones laborales a los 3 años (art. 4.1. del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.)

- **Infracciones seguridad social.**

  Plazo: 5 años - Ley de Infracciones y Sanciones en el Orden Social.

- **Registro de la jornada laboral.**

  Plazo: 4 años desde que se obtienen los datos (art. 34.9 del Real Decreto Legislativo 2/2015, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).

- Documentación relativa a la **selección de personal**. *Currículum*, anotaciones de entrevistas e información del proceso de selección.

  Plazo: recomendación de 1 año desde la última actualización. Aunque no existe un plazo determinado por ley, muchos expertos afirman que 24 meses es el periodo adecuado para guardar un currículum y tras ese tiempo se debería de eliminar.

- Documentación relacionada con el **cumplimiento de obligaciones** de alta de seguridad social y pago de cuotas (afiliación, altas, bajas, recibos de pago de salarios, etc.).

  Plazo: 4 años (art. 21 del Real Decreto Legislativo 5/2000, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social). *Dicho periodo de 4 años será ampliado por un año más por la responsabilidad civil contractual que se pudiera derivar, es decir, 5 años.

- **Cursos de formación** realizados por empleados.

  Plazo: 4 años desde la finalización de la relación contractual (art. 5.2 de la Orden TAS/2307/2007).

- Documentación en materia de **prevención de riesgos laborales o asociada a la contratación**. Certificados de aptitud (apto/no apto) e informes de accidentes laborales. Documentación necesaria para gestionar los seguros de salud, siniestros y fallecimiento.

  Plazo: 15 años (relaciones jurídicas iniciadas con anterioridad al 7 de octubre de 2005) y 5 años (relaciones jurídicas iniciadas entre el 7 de octubre de 2005 y el 7 de octubre de 2015, así como las iniciadas a partir del 7 de octubre de 2015). Ley 42/2015, de 5 de octubre.

Documentación relacionada con la protección de datos

- Los **datos personales** o de carácter sensible.

  Plazo: deben ser almacenados durante el tiempo necesario para los fines para los que fueron recabados. Una vez finalizado el trámite, los datos deben ser eliminados o bloqueados según el RGPD y la LOPDGDD.

- **Videovigilancia.** Imágenes y, en su caso, sonidos, que sean captados por sistemas de videovigilancia, únicamente en los supuestos en los que no se detecte un ilícito (en cuyo supuesto, podrán ser conservados hasta la prescripción de la acción que se deriva de dicho ilícito).

  Plazo: 30 días desde que se hizo la grabación.

Documentación de pólizas, seguridad y mantenimiento

- Las **pólizas de seguros** deben conservarse durante la vigencia de la póliza, y una vez expirada, por un periodo adicional de al menos 5 años.

- Los **informes de inspección de seguridad** de los inmuebles y certificados de mantenimiento deben conservarse durante al menos 5 años. Es posible que algunos certificados requieran periodo de tiempo superiores, ya que depende de la normativa específica aplicable.

  Plazo: el Código Civil español establece plazos para la prescripción de acciones que pueden relacionarse con los seguros, que normalmente es de 5 años para reclamaciones derivadas de contratos.

Documentación relativa a la propiedad horizontal

Plazo: el secretario custodiará los libros de actas de la Junta de Propietarios. La documentación sobre convocatorias, comunicaciones, apoderamientos y toda la documentación adjunta a las actas es recomendable conservarlas durante 5 años (art. 19 LPH).

- El plazo de 5 años se relaciona con el periodo de **prescripción** para las acciones administrativas, como la impugnación de acuerdos o la reclamación de cuotas impagadas. Por lo tanto, es importante que las comunidades de propietarios conserven estas actas durante ese tiempo para poder hacer frente a posibles reclamaciones o consultas por parte de los propietarios.

Además, es recomendable que las comunidades de propietarios mantengan un archivo más prolongado de las actas, aunque no sea obligatorio, con fines de referencia y transparencia.

- La **Ley de Propiedad Horizontal** no especifica cuántos años han de guardarse las actas de la comunidad, pero al no ser documentos independientes como las cuentas, sino que forman parte del libro de actas, tienen validez permanente y, por ello, han de conservarse indefinidamente, junto con la división horizontal y otros documentos legales, como el CIF de la comunidad.

Documentación relativa al blanqueo de capitales.

Plazo: 10 años - Ley 10/2010, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

- Tras la **reforma del Código Penal** en materia de transparencia y lucha contra el fraude discal y en la seguridad social, se amplía en 10 años el periodo de prescripción y plazo en el que se puede exigir documentación de carácter fiscal, laboral o contable, aumentando así el tiempo mínimo necesario de conversación de dicha documentación. Ley Orgánica 7/2012 por la que se modifica la LO 10/1995, del Código Penal.

Legislación aplicable

- **Código de Comercio:** regula la conservación de documentación contable y mercantil.
- **Ley General Tributaria:** indica los plazos de prescripción de las obligaciones tributarias.
- **Ley sobre Infracciones y Sanciones en el Orden Social:** regulariza los plazos de conservación de la documentación laboral.
- **Código Civil:** indica los plazos generales de prescripción de acciones contractuales. Se debe tener presenta que este código puede variar en función de las comunidades autónomas.
- **Ley de Propiedad Horizontal:** regula las relaciones entre los propietarios y la gestión de la documentación de la comunidad de vecinos.
- **Reglamento General de Protección de Datos (RGPD):** establece las normas sobre la protección de la información de carácter personal y su conservación.
- **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD):** complementa a nivel nacional el RGPD y detalla de manera específica la protección de datos.
- **Ley 10/2010, de 28 de abril,** de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.
- **Real Decreto Legislativo 5/2000, de 4 de agosto,** por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.
- **Orden EHA/962/2007, de 10 de abril,** por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas, contenidas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el reglamento por el que se regulan las obligaciones de facturación.

A continuación, se muestra una **tabla resumen de los plazos recomendados por diferentes normativas aplicables en materia de conservación de documentación utilizada por los administradores de fincas.**

Tipo de documentación	Plazo de conservación
Documentación societaria y de constitución	Indefinidamente y mínimo 6 años desde disolución
Documentación fiscal y tributaria	4 años
Documentación contable	6 años
Contratos laborales	4 años
Infracciones laborales y de SS	3 y 5 años
Registro de jornada laboral	4 años
Selección de personal	1 año aprox.
Obligaciones de seguridad social	4 años + 1 de responsabilidad civil contractual = 5 años
Cursos de formación	4 años
Prevención de riesgos laborales	15 años / 5 años
Protección de datos y videovigilancia	Tiempo estrictamente necesario (principio de limitación del tiempo de conservación), 30 días respectivamente.
Actas de juntas de vecinos	Al menos 5 años
Convocatorias y documentación	Al menos 5 años
Escrituras y documentos de propiedad	5 años
Pólizas de seguro, informes de inspección y certificados de mantenimiento	Vigencia de la poliza 5 años
Blanqueo de capitales	10 años

Tabla 2. Plazos de conservación recomendados

4.1.5. Destrucción segura de la información

La **conservación, tratamiento y uso de la información sensible** para los administradores de fincas cobra la misma importancia que su destrucción y borrado. Por ello, se deben utilizar procedimientos que garanticen su destrucción de forma segura.

La **destrucción segura de la información** permite eliminar los datos de manera definitiva para que estos no puedan ser recuperados o reutilizados de forma indebida. Estos procesos protegen la confidencialidad de los datos y permiten cumplir con las normativas y regulaciones aplicables en materia de protección de datos.

Importancia de la destrucción segura de la información

Existen dos maneras de almacenar la información. Por un lado, se dispone del **almacenamiento físico**[6], y por otro, del **almacenamiento lógico**[7].

Los administradores de fincas tratan con un gran volumen de datos de carácter personal. Su **tratamiento, almacenamiento y destrucción** deben realizarse de manera segura para proteger su confidencialidad, prevenir fugas de información o accesos no autorizados.

A continuación, se indican los **puntos por los que es importante aplicar estos procedimientos** en los despachos de administración de fincas:

Protección de datos

- Contribuye el **cumplimiento de las regulaciones y leyes de protección de datos (RGPD y la LOPDGDD).**
- Asegura que la información **no pueda ser accesible por personas no autorizadas.**

Prevención de fraudes

- Aplicar un proceso de destrucción seguro **evita que la información pueda ser utilizada para cometer fraudes, delitos o robos de identidad.**

Proteger la confidencialidad

- **Evita que se produzcan accesos a información del despacho o de clientes** donde pueda verse afectada la confidencialidad de los datos.

Reducción de riesgos de fuga de información

- Al eliminar de manera segura los datos, **disminuye el riesgo de posibles filtraciones de información y accesos no autorizados [34]**.

Además, se tendrá en cuenta que **se deben aplicar los mecanismos seguros de destrucción de la información tanto para la documentación en formato físico como lógico.**

[6] Los datos son guardados en medios de almacenamiento tangibles. Dentro de este conjunto se encuentran: papel, USB, discos duros extraíbles, tarjetas de memoria, entre otros.
[7] Hace referencia a la organización y estructura de los datos de manera abstracta, independiente de cómo sean almacenados de manera física. Trata la forma en la que los datos se gestionan, son accedidos y se presentan a los usuarios. Algunos ejemplos son: Bases de Datos, almacenamiento en la nube, redes de almacenamiento (SAN), etc.

4.1.6. Procesos de destrucción de la información

El **borrado seguro de la información** [35] es el proceso mediante el cual los datos son eliminados, de cualquier soporte en el que se encuentren almacenados, de forma que **no puedan ser recuperados**, ni siquiera con técnicas avanzadas de recuperación de datos.

Existen diferentes métodos de eliminación de que pueden variar en función del **formato o soporte** en el que se encuentran almacenados. Algunos pueden suponer la **destrucción total** del soporte de almacenamiento, mientras que otros pueden permitir la reutilización de los dispositivos físicos.

En el sector de administración de fincas, a la hora de eliminar la información de carácter personal de propietarios, inquilinos, etc., se deben seguir procesos rigurosos que se adapten a las regulaciones y normativas de protección de datos personales.

Borrado seguro según normativa ISO 27001

El **RGPD** y la **LOPDGDD** establecen los requisitos sobre el tratamiento y eliminación de los datos personales, pero, además, existen estándares como la **ISO27001** que, a pesar de no ser obligatoria, proporciona un marco robusto para la gestión de la seguridad de la información.

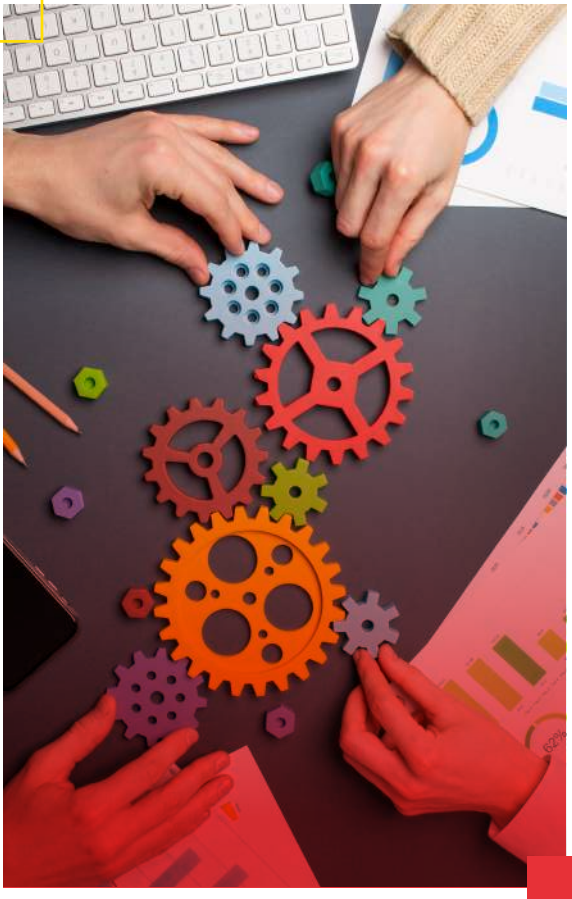
La **implementación del borrado seguro conforme a la ISO 27001**, permite a los despachos de administración de fincas garantizar que la información sensible se elimine de manera segura y conforme a la normativa aplicable.

En concreto, son de especial interés para el borrado seguro los **puntos**:

A.8.3.2. Eliminación de soportes:
Este control proporciona las pautas para eliminar de forma segura los soportes cuando ya no sean necesarios.

A.11.2.7. Reutilización o eliminación segura de equipos:

Trata sobre la confirmación de que los datos sensibles, en todos los soportes de almacenamiento, sean eliminados de forma segura antes de deshacerse de ellos o reutilizarlos.



Borrado seguro de la información

Algunos **procesos o métodos de borrado** no destruyen la información de manera segura, como por ejemplo comando suprimir de los teclados. Por lo tanto, cualquier acción que no destruya la información para que ésta sea irrecuperable no puede considerarse un método seguro. **A continuación, se muestran algunos procesos que permiten una destrucción segura de la información:**

- **Triturado:** destrucción de la información mediante el uso de máquinas trituradoras que cortan los documentos en papel en pequeñas tiras. También es útil para el caso de dispositivo de almacenamiento como los CD. Las máquinas más sofisticadas reducen el papel en trozo muy pequeños (desintegración), por lo que imposibilita su reconstrucción. Adicionalmente, en algunas oficinas dividen los residuos de las máquinas trituradoras en diferentes bolsas para no ser depositadas en el mismo contenedor.

- **Incineración:** los documentos y dispositivos son quemados en instalaciones preparadas para ello, y cumpliendo con las normativas ambientales aplicables.

- **Pulpeo:** Se mezcla la documentación con agua y productos químicos para convertir el documento de papel en una pasta. Esta opción admite la posibilidad de reciclaje, aunque es exclusiva para la documentación en papel.

- **Desmagnetización o *degaussing*:** se utilizan fuertes campos magnéticos para borrar los datos almacenados en dispositivos como discos duros, cintas magnéticas, etc.

- **Sobreescritura:** se trata de un proceso de borrado seguro en el que se escriben patrones aleatorios de datos sobre la información almacenada en dispositivos como discos duros, memorias flash, etc.

- **Borrado criptográfico:** se cifra la información y después se elimina la clave de cifrado haciendo inviable su recuperación.

- **Eliminación como servicio (EaaS):** consiste en la contratación de un servicio proporcionado por empresas especializadas que garantizan la eliminación segura de los datos. Este método ofrece tranquilidad y comodidad, ya que la empresa se encarga de todo el proceso asegurando el cumplimiento de las normativas de protección de datos y proporcionando la documentación y certificación de la eliminación segura.

Borrado seguro de la información en la nube

Para asegurar la **eliminación de la información almacenada en la nube,** las empresas pueden utilizar diferentes recursos:

- **Borrado criptográfico:** los datos almacenados en la nube se cifran con claves antes de ser almacenados. Este tipo de borrado seguro consiste en la destrucción de esas claves de cifrado, haciendo irrecuperables los datos sin la necesidad de sobrescribir físicamente.

- **Sobreescritura:** si el proveedor de servicios en la nube lo permite, los datos almacenados pueden sobrescribirse con patrones aleatorios, garantizando que no se puedan recuperar.

- **Eliminación gestionada por el proveedor:** a la hora de contratar un proveedor en la nube, se debe tener en cuenta que cuente con políticas que aseguren la eliminación de los datos después de un determinado tiempo. Algunos proveedores, además, ofrecen servicios especializados de eliminación segura de los datos que garantizan el cumplimiento normativo.

Destrucción certificada

El **proceso de destrucción certificada** de la información es una forma de **garantizar**, de forma documentada, **que los datos se han eliminado de forma segura y cumpliendo la normativa vigente**. El proceso de eliminación va acompañado de un documento que certifica que se ha realizado de forma segura, emitido por la entidad que lo realiza, y que evidencia el cumplimiento de la normativa aplicable. **Este proceso consta de cinco fases:**

- **Recolección:** toda la información o dispositivos que se quieren destruir son recolectados de forma segura, manteniendo la cadena de custodia y evitando accesos no autorizados.
- **Transporte:** todo lo recogido se transporta, de forma segura, a las instalaciones donde se destruirá.
- **Destrucción:** se aplican los procesos de destrucción pertinentes que aseguren la eliminación completa de los datos.
- **Certificación:** la entidad encargada de la destrucción emite un certificado que documenta el proceso utilizado y la fecha de destrucción, entre otros detalles.
- **Auditoría:** se realizan auditorias para verificar que el proceso se ha llevado a cabo de forma segura, cumpliendo con la normativa aplicable.

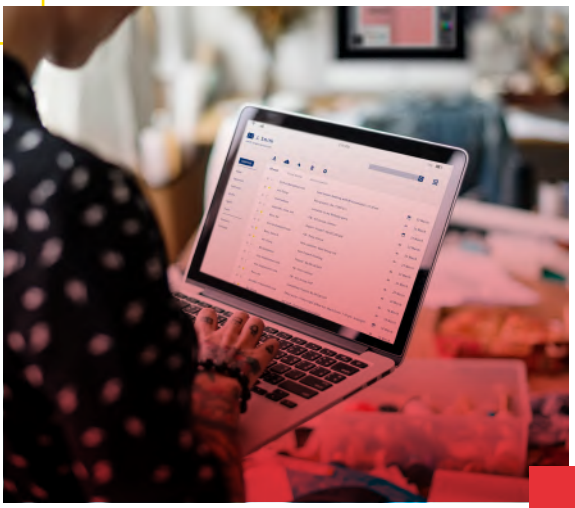
4.2. Protección de dispositivos móviles corporativos y BYOD

Hoy en día trabajar fuera de las instalaciones corporativas es posible con el uso de dispositivos móviles (portátiles, *tablets* y teléfonos móviles) **propiedad de la empresa [36] o del empleado [37].**

Las tecnologías de movilidad, como los ordenadores portátiles, **permiten al empleado desempeñar su trabajo como si estuviera en las instalaciones de la empresa**: acceso al correo, aplicaciones corporativas, información confidencial, etc.

Estos dispositivos son más susceptibles de pérdida o robo, por lo que existe un **riesgo añadido al acceso de la información corporativa**. Por eso, es imprescindible tomar algunas medidas de seguridad, como establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el equipo siempre actualizado y con el antivirus activo, etc.

Consulta la siguiente ***checklist*** para conocer las medidas de seguridad aplicables a estos dispositivos:



PERSONAL TÉCNICO

USO DE DISPOSITIVOS MÓVILES CORPORATIVOS

BÁSICO

- ☐ ***Asignación de dispositivos.*** Elaboras un procedimiento de solicitud y asignación de los dispositivos móviles corporativos.
- ☐ ***Protección de la BIOS.*** Configuras el acceso a la BIOS mediante contraseña.
- ☐ ***Registro de equipos.*** Mantienes un registro de los portátiles asignados (qué portátil y a quién se le asigna). Registras el uso que se da al portátil, así como el software y hardware que son requeridos por el empleado.
- ☐ ***Mantenimiento de dispositivos.*** Elaboras un formulario de solicitud de cambios en el dispositivo (modificación de hardware, instalación de software, cambios en la confguración).
- ☐ ***Software de localización.*** Comunicas al usuario del dispositivo si este dispone de software de localización o si fuera necesaria su instalación.
- ☐ ***Almacenamiento de la información.*** No almacenes información corporativa que no sea estrictamente necesaria para el desarrollo del trabajo.
- ☐ ***Tratamiento de información confidencial.*** Cifras la información confidencial y la eliminas de forma segura (o solicitas la eliminación al técnico responsable).
- ☐ ***Conexión a redes.*** Conectas el portátil a redes conocidas y privadas. Optas por una conexión 3G/4G cuando el resto de las redes disponibles no sean confiables.
- ☐ ***Notificación en caso de infección.*** Notificas al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.
- ☐ ***Responsabilidades.*** Conoces las responsabilidades que conlleva el uso de dispositivos corporativos y aplicas las normas de seguridad correspondientes.

Si el despacho permite utilizar los **dispositivos personales para trabajar** (BYOD o ***Bring Your Own Device***) se deben aplicar las siguientes medidas de seguridad:

EMPLEADOS

USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS

BÁSICO

- ***Normas y procedimientos BYOD.***
  Elaboras normas y procedimientos específicos si permites BYOD en tu empresa (usos permitidos, antivirus, actualización, configuraciones,...)
- ***Prohibición de uso de dispositivos manipulados.***
  Prohíbes el uso de dispositivos rooteados o a los que se ha realizado jailbreak.
- ***Concienciación de los empleados.***
  Involucras a los usuarios en la protección de sus propios dispositivos y de los datos que contienen o a los que pueden acceder.
- ***Formación de los empleados.***
  Proporcionas a tus empleados charlas o formación sobre cómo proteger sus dispositivos (contraseñas, actualizaciones, permisos, etc.).
- ***Limitar el acceso a redes externas.***
  Prohíbes el uso de redes inalámbricas externas no corporativas salvo 3G/4G.
- ***Lista de aplicaciones no permitidas.***
  Mantienes una lista de aplicaciones no permitidas y la difundes entre tus empleados.
- ***Controlar el amacenamiento en la nube de datos corporativos.***
  Supervisas el uso de aplicaciones de almacenamiento en la nube.
- ***Proceso de borrado de la información.***
  Aplicas una normativa de entrega/eliminación de la información de sus dispositivos cuando el empleado abandona la empresa.
- ***Control de usuario y dispositivos.***
  Mantienes un registro actualizado con usuarios, dispositivos y privilegios de acceso.
- ***Bloqueo programado.***
  Configuras el bloqueo automático del dispositivo tras un periodo de inactividad.


EMPLEADOS
USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS
BÁSICO
Desconexión wifi y Bluethooth.
Desactivas en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no son necesarios.
Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos.
Instalas y configuras medidas para el almacenamiento seguro a la información (clasificación de información, cifrado de datos, etc.).
Cumplimiento de la normativa.
Conoces y aceptas la normativa corporativa vigente para el uso de tus dispositivos en actividades de la empresa.
AVANZADO
Control de acceso a la red.
Implementas un control de acceso (autenticación con contraseños, doble factor, VPN...) a la red corporativa desde estos dispositivos.
Extravío de dispositivos.
Configuras medidas de seguridad para proteger la información corporativa en los dispositivos (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas) en caso de extravío.

4.3. Protección de dispositivos de almacenamiento extraíbles

Los **dispositivos de almacenamiento extraíble** (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) permiten una transferencia rápida y directa de información. Hoy en día son imprescindibles y muy utilizados. Debemos aplicar las **medidas de seguridad** que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus [38].

El despacho debe decidir si se permite el uso de dispositivos de almacenamiento externo, y de ser así, aplicar **medidas de seguridad como las siguientes:**

4.4. Medidas para el correo electrónico

Considerando los fraudes a través del correo electrónico que más afectan a los despachos de administración de fincas, es importante tener en cuenta las principales **medidas de ciberseguridad que pueden implementarse para evitar o minimizar los efectos de este tipo de ataques**:

- Hay que asegurarse de que los c**orreos proceden de un origen confiable**, aunque los ciberdelincuentes pueden utilizar la técnica conocida como ***email spoofing*** para suplantar direcciones legítimas. Por ello, también se debe revisar con detalle el cuerpo del mensaje, verificando que esté bien redactado y que el texto sea coherente. Aun con estas comprobaciones, se puede seguir teniendo dudas sobre la legitimidad de un correo. En estos casos, puede ayudar llevar a cabo el análisis de sus cabeceras.

- En relación con el punto anterior, en los fraudes en los que se solicita realizar algún tipo de pago, el cambio de cuenta para el ingreso de nómina o cualquier solicitud que implique movimientos de dinero, se debe **verificar la acción con la fuente que la solicita**. Esta comprobación se debe hacer por **otro medio distinto al correo electrónico**, bien sea una llamada telefónica, una videollamada o cualquier método en el que se pueda verificar la legitimidad de la acción solicitada.

- En ocasiones, los despachos pueden verse afectados por algún *ransomware* que haya sigo distribuido por correo electrónico. **En ningún caso se debe pagar el rescate.** Para minimizar el impacto de este tipo de ataques se deben realizar copias de seguridad de forma periódica de los datos del negocio. Estas copias de seguridad deben alojarse en un servidor diferente al que está contenida la información. También resulta conveniente desconectar el equipo infectado lo antes posible de la red para evitar que el ataque pueda propagarse al resto de equipos de la organización.

4.4.1. Recomendaciones a trasladar a nuestros clientes

Tus clientes también **pueden ayudarte a mantener la seguridad del despacho**, así como la suya propia siguiendo unos sencillos consejos como los siguientes:

1. Cuando realices una transacción importante con tu administrador, utiliza una **doble verificación**, es decir, si la primera comunicación se ha realizado por correo electrónico puedes además realizar una llamada para verificar que todo está en orden.

2. **Desconfía** si recibes una comunicación inusual de tu administrador. No hagas clic en los enlaces que contengan los mensajes ni descargues ningún adjunto. Es importante **aprender a identificar los correos sospechosos** y avisar a tu despacho ante cualquier intento de fraude o suplantación.

3. Realiza cada cierto tiempo un **análisis con un antivirus de tus equipos** y, de forma análoga, de todos los archivos que descargues.

4. Mantén **actualizados los sistemas operativos** y el *software* de los dispositivos que utilices, siempre que sea posible. Descarga el *software* sólo desde las páginas y mercados oficiales.

5. Infórmate sobre las **últimas amenazas y fraudes** que circulan por Internet, te ayudarán a estar más protegido [39].

6. **No reutilices la misma contraseña** en todos los servicios online que uses, no es una práctica segura.

7. Para una mayor seguridad en tus procesos de acceso, establece un doble factor de autenticación. También, puedes apoyarte en un **gestor de contraseñas** para proteger de forma segura y sencilla las claves que utilices en los diferentes servicios de Internet.

8. Si tienes perfiles en **redes sociales**, comprueba las opciones de privacidad de las mismas, es decir, lo que otras personas pueden ver cuando acceden a tu perfil.

9. Realiza **copias de seguridad** de la información que almacenas en tus dispositivos. De esta manera, en caso de intrusión (hackeo), pérdida o robo del dispositivo siempre podrás recuperar tus datos.

10. Y si necesitas ayuda para verificar si un correo electrónico es legítimo, si la página web que has visitado es confiable o te surge cualquier otra duda, puedes contactar con **'Tu Ayuda en Ciberseguridad'.**

4.5. Medidas para el sitio web corporativo

En ocasiones, las empresas tienen una política de actualización de sus sitios web corporativos deficiente, lo que puede conllevar diferentes **vulnerabilidades**, que los ciberdelincuentes pueden aprovechar para conseguir sus objetivos. Por ello, la primera medida de ciberseguridad consiste en mantener el **sitio web actualizado** y que cuente con, al menos, un conjunto mínimo de medidas de protección.

Para proteger el **portal web corporativo** [40], y así reducir su nivel de vulnerabilidad y evitar el compromiso de la privacidad y seguridad del despacho, se debe contar con una **política de seguridad** [41] que al menos contemple los siguientes puntos:

- **Tener instalado un certificado SSL** [42], también conocido como certificado web. Este certificado sirve para proteger las comunicaciones que se establecen entre la web corporativa y el dispositivo del cliente, evitando que los ciberdelincuentes puedan robar la información en tránsito, como, por ejemplo, nombres de usuario y contraseñas. **Esta medida siempre es recomendable**, ya que muchos navegadores marcan como inseguros los sitios web sin certificado SSL, con un cifrado anticuado, firmados por una entidad no reconocida o que cuentan con un certificado caducado. Además, sirven para **identificar la web de forma inequívoca**, generando así confianza entre los clientes.

- **Tener al día las actualizaciones de seguridad** del gestor de contenidos o CMS, por sus siglas en inglés ***Content Management System,*** y sus complementos. La actualización de este software debe ser considerada una tarea prioritaria a realizar, tanto si la gestión del sitio web se desarrolla en el despacho como si se realiza por parte de un tercero. Estas aplicaciones publican regularmente actualizaciones de seguridad que corrigen las últimas vulnerabilidades descubiertas. Siempre se debe contar con la última versión disponible tanto del CMS como de los ***plugins*** y temas utilizados.

- **Utilizar contraseñas robustas [43].** Las contraseñas de acceso al *backend* del sitio web corporativo deben ser lo más robustas posibles. Para evitar utilizar credenciales de acceso débiles es recomendable **establecer mecanismos** que no permitan utilizar contraseñas sin unos mínimos de seguridad. Para dotar de un extra de seguridad se puede establecer un mecanismo por el que, ante determinados intentos erróneos de acceso, se inhabilite al usuario asociado durante un determinado tiempo, que se incrementará exponen-cialmente si continúan los intentos fallidos. Además, se puede habilitar un factor de autenticación adicional **[44]**, que solamente deberá conocer el usuario legítimo, como puede ser una clave **OTP** (***One Time Password***).

- **Realizar copias de seguridad [45].** Las copias de seguridad son indispensables en cualquier entorno corporativo y el sitio web de la empresa no es una excepción. Se deben realizar copias de seguridad periódicas y almacenarlas en un entorno seguro, además de comprobar que pueden restaurarse.

- **Utilizar sistemas de respaldo.** Los sistemas de respaldo permiten que la web corporativa siga operativa en caso de incidente de seguridad o fallo del sistema. El sistema de respaldo debe estar ubicado en un servidor independiente, que pueda ser activado cuando el servidor principal no pueda ofrecer el servicio.

- **Utilizar sistemas *captcha* [46].** Los sistemas de respaldo permiten que la web corporativa siga operativa en caso de incidente de seguridad o fallo del sistema. El sistema de respaldo debe estar ubicado en un servidor independiente, que pueda ser activado cuando el servidor principal no pueda ofrecer el servicio.

- **Realizar una gestión de registros [47] (*logging*).** Un sistema de gestión de registros o *logs* guarda los eventos más importantes que tienen lugar en el sitio web corporativo. Así, en caso de incidente de seguridad, se podrá investigar lo sucedido para mitigar el incidente y tomar las medidas oportunas para evitar que suceda de nuevo.

- **Tener instalados entornos de producción y prueba.** Cuando se aplica una actualización de seguridad o cualquier otro cambio significativo en el sitio web corporativo es recomendable realizarlo previamente en un entorno controlado, de modo que, ante cualquier fallo imprevisto, el entorno de producción no se vea afectado. Por ello, es importante disponer de dos entornos bien diferenciados: uno de pruebas o preproducción y el sitio web funcional y público o producción.

- **Asegurar pagos online seguros.** Si el portal web permite a los clientes comprar de forma online, se deben **implementar métodos seguros [48],** como los TPV virtuales, cuyas comunicaciones viajen cifradas, o contar con pasarelas de pago, como PayPal o Redsys, entre otras.

- **Asegurar el cumplimiento legal y normativo.** No cumplir con la ley vigente puede derivar en distintas sanciones por incumplimiento normativo, además de generar desconfianza entre los clientes. Para cumplir con la normativa se deben tratar los datos personales de acuerdo a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), la Ley de Servicios de la Sociedad de la Información (LSSI) y la Ley de Propiedad Intelectual (LPI). Además, se debe cumplir cualquier otro tipo de normativa vigente **[49]** que afecte a la actividad de la empresa.

4.6. Medidas para las redes sociales

Debido al uso cada vez mayor de las redes sociales, **es importante asegurarse de no ser víctimas de un incidente de seguridad relacionado con la utilización de las mismas.** Para ello, se pueden adoptar una serie de medidas de carácter preventivo:

- **Utilizar contraseñas de acceso robustas.** El binomio usuario y contraseña permite acceder a la administración de las redes sociales, de ahí la importancia de utilizar una contraseña fuerte que no sea fácilmente descifrable y habilitar siempre que sea posible el doble factor de autenticación. Un acceso no autorizado por parte de un ciberdelincuente podría permitirle conseguir la información del perfil, comunicarse con clientes o publicar en nombre del despacho, lo que podría ocasionar fugas de información y graves consecuencias en la reputación, entre otros incidentes.

- **Realizar una correcta configuración de la privacidad.** Todas las redes sociales cuentan con parámetros de privacidad que disponen de distintos niveles de restricción. Esto permite encontrar un punto intermedio entre funcionalidad y seguridad para utilizar las redes sociales de manera efectiva e interactuar con los clientes, sin descuidar la seguridad y privacidad del perfil.

- **Elegir un responsable de publicación.** Si bien es una buena opción que los empleados aporten ideas para llevar a cabo acciones que aumenten la popularidad del despacho, no es una buena práctica permitir el acceso y publicación de forma indiscriminada. Con esta práctica, a la larga, la imagen del despacho puede verse dañada, además de aumentar el riesgo de sufrir un incidente de seguridad.

- **Llevar a cabo restricciones de acceso.** Existen aplicaciones que por diferentes motivos (gestión, estadísticos, publicitarios, etc.) solicitan acceso a los diferentes perfiles de las redes sociales. Ante esta situación, es recomendable analizar detenidamente dichos accesos antes de habilitarlos. De lo contrario, esta práctica puede suponer un riesgo para la privacidad, al permitir el acceso a determinados datos que pueden ser privados, como información de seguidores o clientes, o la publicación de contenido no supervisado.

- **Tener precaución a la hora de seguir enlaces y descargar adjuntos.** Es muy habitual la difusión de *malware* a través de redes sociales mediante documentos adjuntos, mensajes dentro de la propia red o sitios web de terceros. En caso de que un enlace dirija a cualquier web que solicite cualquier tipo de dato personal o bancario, es recomendable verificar que dicha web es legítima y comprobar su certificado de seguridad, asegurándose de que corresponde con el sitio al que se está accediendo.

- **Estar al día de las ciberamenazas.** La suscripción al **boletín de avisos de Protege tu empresa [50]**, de **INCIBE**, permite estar al día de las amenazas que pueden afectar a las empresas, facilitando la prevención y protección ante incidentes de seguridad.

- **Fomentar la formación y concienciación de los empleados.** La falta de formación en materia de ciberseguridad puede conllevar una mala gestión de las redes sociales por parte de su administrador. Un error frecuente y, por tanto, una práctica de riesgo, es la publicación de información privada, ya que los ciberdelincuentes utilizan estas aplicaciones como fuente de información para planificar y llevar a cabo sus ataques.

Además, hay que tener en cuenta una **serie de acciones a evitar a la hora de publicar en redes sociales:**

- **Dar** información confidencial o sujeta a propiedad intelectual.
- **Lanzar** comentarios inoportunos, negativos o inapropiados, como, por ejemplo, quejas laborales.
- **Emitir** juicios de valor.
- **Enfrascarse** en discusiones sin sentido, insultar, amenazar o acosar.
- **Propagar** noticias falsas.

4.7. Medidas para el *software on-premise*

El ***software on-premise*** ofrece a las empresas un gran control sobre la protección de la información almacenada y de los sistemas, siempre y cuando se cuente con las medidas de seguridad adecuada.

Los administradores de fincas suelen utilizar estas aplicaciones para facilitar la gestión y administración de documentación de sus clientes, por lo que se precisa implementar **medidas de seguridad** para salvaguardar la confidencialidad, integridad y disponibilidad de los datos como las siguientes.

- **Contraseñas y autenticación:**
  - **Contraseñas robustas:** se aconseja el uso de contraseñas de acceso robustas (longitud de entre 8-10 caracteres, que contenga números, mayúsculas, minúsculas, símbolos y caracteres especiales). No debemos usar estas contraseñas en otras aplicaciones o servicios.
  - **Almacenamiento seguro de contraseñas:** el uso de gestores de contraseñas es muy útil para el almacenamiento de las credenciales, evitando malas prácticas como su reutilización.
  - **Doble factor de autenticación:** aplicar doble factor de autenticación para el acceso a las aplicaciones supone una capa adicional de seguridad, ya que dificulta el acceso a la información en caso de robo de credenciales.
- **Gestión de acceso y usuarios:**
  - **Gestión de usuarios:** se deben administrar los usuarios en función de sus roles en la empresa y la necesidad de acceso a la información para el correcto desarrollo de su trabajo.
  - **Principio de mínimos privilegios:** se recomienda dar de alta a los usuarios otorgando los privilegios estrictamente necesarios para el desempeño de sus labores dentro del despacho. Además, para prevenir riesgos hay que evitar hacer uso de usuarios genéricos con permisos de administrador.
  - **Acceso restringido:** limitar el acceso a los datos, equipos críticos y servidores sólo a personal autorizado, tanto a nivel físico como lógico.
- **Protección de datos:**
  - **Clasificación de los datos:** cada organización deberá crear el esquema que mejor se adapte a sus necesidades de manera que cada activo de información contará con los controles más óptimos en función de su clasificación.
  - **Cifrado de datos [51]:** asegurar que los datos sensibles estén cifrados, tanto en tránsito como en reposo.

- **Preservación y eliminación segura de la información:** en función del tipo de documentación, se deben establecer los tiempos de conservación de la información y los procesos de borrado seguro de los datos cuando ya no sean necesarios.

- **Uso de soluciones DLP:** integrar las aplicaciones en las soluciones DLP para que puedan ser monitorizadas.

Seguridad de la red:

- **Protección *antimalware*:** implementar soluciones antivirus y *antimalware* y actualizadas para proteger las aplicaciones frente a posibles infecciones.

- **Uso de *firewall* [52]:** configurar las reglas del *firewall* para controlar el tráfico entrante y saliente.

- **Segmentación de la red [53]:** dividir la red en segmentos separados para limitar el acceso y contener posibles brechas de seguridad.

- **Uso de VPN [54]:** utilizar redes privadas virtuales para el acceso remoto, ya que permite el acceso a la red local de manera segura.

Mantenimiento y actualizaciones:

- **Actualizaciones y parches de seguridad [55]:** mantener los sistemas operativos y las aplicaciones actualizadas con los últimos parches de seguridad implementados, esto permite corregir vulnerabilidades que pueden poner en riesgo la seguridad de la empresa.

Respaldo y recuperación:

- **Copias de seguridad:** realizar copias de seguridad de manera periódica y almacenarlas cifradas en ubicaciones seguras, así como comprobar los procedimientos de recuperación de la información para evitar su pérdida.

- **Uso de soporte técnico:** utilizar las ayudas aportadas por soporte técnico de cada una de las aplicaciones para los casos que sea necesario. El personal de soporte cualificado podrá guiar a los empleados de la compañía a mantener una configuración óptima de las herramientas.

Políticas y procedimientos:

- **Políticas de seguridad:** desarrollar y divulgar entre los empleados la existencia de políticas de seguridad como: uso de contraseñas, copias de seguridad, uso de dispositivos corporativos, etc.

Monitorización y respuesta:

- **Monitoreo y registro de actividades:** utiliza sistemas IDS, IPS o SIEM [56]. Protegen las comunicaciones que y monitorizan el tráfico que entra o sale de nuestra red.

- **Respuesta ante incidentes:** se debe establecer un plan de respuesta ante incidentes [57].

Capacitación y soporte:

- **Formación y concienciación:** capacitar a los empleados para que sepan aplicar las medidas de seguridad necesarias.

- **Uso de soporte técnico:** utilizar las ayudas aportadas por el soporte técnico de cada una de las aplicaciones para los casos que sea necesario. El personal de soporte cualificado podrá guiar a los despachos a mantener una configuración óptima de las herramientas.

Auditorías y evaluaciones:

- **Auditorías:** realizar auditorías de seguridad de manera regular para detectar posibles brechas de seguridad, así como evaluar nuevas amenazas que puedan poner en riesgo la información y asegurar el cumplimiento de las normativas y regulaciones aplicables.

4.8. Medidas para el *software* en la nube

La seguridad del ***software*** ubicado en la nube es crucial para **proteger los datos y garantizar la integridad y disponibilidad de los servicios y la información.** La seguridad en la nube permite proteger los datos sensibles, cumplir con las regulaciones y normativas aplicables, prevenir brechas de seguridad y garantizar la continuidad del negocio. Se trata de una inversión que protege a la compañía de posibles amenazas y asegura un uso eficiente de los recursos en la nube.

Consejos generales para contratar servicios en la nube

A la hora de contratar la prestación de servicios en la nube, **se debe tener en consideración algunas pautas para proteger el negocio y su mayor activo, la información.**

- **Ubicación de los datos:** se debe tener en cuenta la ubicación física de los servidores donde será almacenada la información. Se tiene que asegurar que el proveedor cumpla con las normativas aplicables en materia de protección de datos.
- **Comparativa de proveedores de servicios:** comprobar la reputación de la empresa proveedora de los servicios previo a su contratación. No basar la decisión exclusivamente en el coste asociado de los servicios, tener en cuenta la imagen y reputación del proveedor, así como que el paquete de servicios se ajuste a las necesidades del negocio, tanto a nivel normativo como tecnológico. Se recomienda realizar una prospección de mercado para comparar los diferentes proveedores.
- **Acuerdos de nivel de servicios:** cuando se proceda a la contratación de los servicios es imprescindible tener en consideración los SLA **[58]**. Un acuerdo que se ajuste a las necesidades de la compañía podría evitar impactos en la continuidad del negocio.
- **Copias de seguridad:** solicitar al proveedor la asiduidad de realización de copias de seguridad y su garantía de almacenamiento y recuperación.
- **Cumplimiento legal:** asegurar que el proveedor escogido garantiza el cumplimiento de las normativas y regulaciones aplicables a la empresa.
- **Borrado seguro:** asegurar que el proveedor de servicio ofrece un servicio de borrado seguro manteniendo los tiempos de conservación de la información y eliminación cuando sea requerido por el personal de la empresa.

Si te estas planteando la contratación de servicios cloud o necesitas revisar en profundidad la seguridad de tu proveedor, consulta esta publicación: **"Simplifica y gana, servicios en la nube".**

4.8.1. Herramientas colaborativas

En las empresas del sector de administración de fincas, **las herramientas colaborativas facilitan el trabajo en equipo**, ya que estas aplicaciones permiten la compartición de archivos, las videoconferencias [59] o crear grupos de trabajo en un chat, entre otros. Si bien estas herramientas mejoran la eficiencia de las organizaciones, **su uso debe ser correctamente gestionado para asegurar la protección de los datos de los clientes.**

Si tenemos instaladas estas herramientas en nuestros despachos **debemos:**

- **Asegurar que todos los archivos, tanto en tránsito como en reposo, se encuentran cifrados.** Utilizar protocolos de comunicación seguros para la transmisión.
- **Implementar controles de accesos basados en roles,** limitando el acceso a la información confidencial solo al personal autorizado.
- **Utilizar un doble factor de autenticación** para acceder a las plataformas de gestión documental.
- **Monitorización continua y registro las actividades** para detectar comportamientos anómalos y tener constancia de qué usuarios acceden, modifican y descargan los documentos.
- **Establecer políticas claras** sobre la conservación y el borrado de los datos almacenados.
- **Garantizar que se cumple con el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)** y que los datos personales son almacenados y procesados dentro de los países de la UE.
- **Proporcionar formación a todos los empleados** sobre las buenas prácticas de seguridad en cuanto a protección de datos y privacidad.

Herramientas colaborativas gratuitas: la importancia de leer los términos y condiciones de privacidad para la seguridad de nuestros datos empresariales

En ocasiones, **se puede optar por utilizar herramientas colaborativas gratuitas para ahorrar costes o por la facilidad en los tiempos de adquisición**. Esta opción puede cumplir con las necesidades básicas y necesarias para el desarrollo del trabajo, pero también pueden poner en riesgo la seguridad de la empresa y comprometer los datos si no se hace un correcto uso de las mismas.

Cuando se crea una cuenta en este tipo de aplicaciones, **se suele aceptar una serie de términos y condiciones que, en la mayoría de las ocasiones, no se revisan.** Suelen aparecer al final del proceso, en letra pequeña y con una casilla que se debe marcar para continuar.

Al aceptar estos términos y condiciones se está firmando un contrato de vinculación legal que establece las reglas entre el proveedor de la herramienta y la empresa. Como se haría con cualquier contrato, **se debe leer detenidamente para saber qué se está aceptando**, pero, en ocasiones, se pasa por alto este paso.

¿Qué se debe revisar antes de aceptar?

- **Política de privacidad**, que incluye cómo la herramienta maneja y protege los datos.
- **Condiciones de uso**, que establece las obligaciones y derechos al usar la herramienta.
- **Permisos de acceso**, que deben ser razonables, es decir, la herramienta solo debería solicitar los necesarios para cumplir con su función.
- **Retención y eliminación de datos**, que indica el tiempo de conservación de los datos y el proceso de eliminación.

En definitiva, antes de aceptar los términos y condiciones de cualquier servicio **conviene recordar la importancia de los datos empresariales y seguir una serie de buenas prácticas:**

- **Leer con atención los términos y condiciones.**
- **Ante la duda, consultar con un asesor legal o un experto en protección de datos.**
- **Considerar el uso de herramientas de pago con mejores garantías.**
- **Asegurarse de que la configuración de la herramienta se ajusta a las políticas de privacidad de la empresa.**

4.8.2. CRM

Un CRM, en inglés ***Customer Relationship Management***, es una **herramienta que ayuda a la empresa a gestionar las relaciones con los clientes.** La seguridad en las herramientas CRM es de vital importancia para los despachos de administración de fincas por tres motivos principales:

- **La protección de los datos personales de los clientes que se almacenan en ellas.**
- **El cumplimiento normativo, como el RGPD y LOPDGDD, para evitar sanciones y consecuencias legales.**
- **La confianza del cliente para reforzar las relaciones comerciales y mantener la imagen y reputación.**

Medidas de seguridad para el CRM

- **Contraseñas:**
  - **Implementar una política de contraseñas robustas con requisitos tales como:** uso de mayúsculas, minúsculas, números y símbolos, y longitud de, al menos entre 8 y 10 caracteres.
  - **Utilizar un doble factor de autenticación** para acceder al CRM.
- **Monitorización de la actividad:**
  - **Registrar todas las actividades** realizadas en el CRM, como accesos, modificaciones de los datos o descargas.
  - Configurar **alertas para actividades sospechosas**, como intentos fallidos de inicio de sesión o accesos desde ubicaciones poco usuales.
- **Proveedor de confianza:**
  - Evaluar los posibles **proveedores** para seleccionar uno confiable, cuya reputación en el mercado asegure que cumpla con las normativas aplicables al negocio.
  - Es **recomendable** que el proveedor cuente con certificaciones reconocidas en materia de seguridad, como por ejemplo la ISO27001.
- **Cifrado de datos:**
  - **Cifrar los datos** en reposo almacenados en el CRM para proteger su confidencialidad.
  - Utilizar **protocolos seguros** para cifrar los datos transmitidos entre los usuarios y el CRM.
- **Control de acceso:**
  - Definir **roles y asignar permisos** en base a las necesidades exclusivas de cada usuario, asegurando que tengan solamente acceso a la información estrictamente necesaria para **desempeñar sus funciones**. Revisar periódicamente estos permisos y ajustar en base a los cambios de responsabilidades.
- **Copias de seguridad:**
  - Asegurar que se realizan **copias de seguridad** de los datos almacenados en el CRM periódicamente y que están disponibles para una restauración rápida en caso de incidente.
- **Actualizaciones y parches de seguridad:**
  - **Mantener el CRM** siempre actualizado con las últimas versiones y parches de seguridad.
- **Acceso remoto:**
  - Ten en cuenta las opciones seguras a la hora de acceder al **CRM en remoto** (VPN, VDI, etc.) **[60]**
- **Concienciación:**
  - **Formar y concienciar** al personal de forma continua sobre el uso seguro del CRM y la importancia de proteger la información.

4.8.2.1. Gestión turística

Algunos despachos del sector de administración de fincas pueden realizar **tareas de gestión de alquileres de temporada y turísticos.** Estos, además de utilizar el **CRM para la gestión de las reservas, pueden utilizar pasarelas de pago y bases de datos con información contractual de los clientes.** En estos casos, se deberá comprobar que el CRM cuenta con las medidas de seguridad necesarias para proteger los datos y las transacciones financieras:

- **Plataforma de reservas seguras que ofrezca certificado SSL/TLS [61]** y que cumpla con los estándares reconocidos de seguridad.
- **Utilizar pasarelas de pago que cumplan con el estándar PCI-DSS [62]**, que garantiza la protección de los datos de las tarjetas de crédito.
- **Implementar requisitos de seguridad según la normativa PSD2 [63]**, que regula los servicios de pago en la Unión Europea.
- **La plataforma de acceso del CRM** en la nube debe permitir la activación de autenticación multifactor y acceso Single Sign-On (SSO)[8].
- **Asegurar que se cifran los datos cuando son almacenados** en los servidores cumpliendo con controles de seguridad en los centros de datos del proveedor.
- **Garantizar la comprobación del cumplimiento de seguridad** mediante la elaboración de auditorías y certificaciones.
- **Asegurar la integridad de los datos tanto de la empresa como de los clientes.** Aunque no sean obligatorias, las certificaciones ISO, como la ISO 27001, son estándares reconocidos que aseguran que el proveedor de servicios CRM cuenta con las garantías de protección de la información.
- **Garantizar** que tanto el acceso a las bases de datos con información sensible como al calendario de reservas se realiza de forma segura y solo por el personal autorizado.
- **Protección de la información en todas sus fases:** almacenamiento, transmisión y eliminación.
- **Comprobar los procesos de borrado de información** y si son conformes a la legislación aplicable.
- **Definición de roles para el control de acceso a la información.**
- **Generar con asiduidad copias de seguridad.**
- **Accesos mediante interfaces y API seguras**, implantación siguiendo estándares de seguridad de desarrollo de aplicaciones.
- **Configurar un tiempo máximo de sesión y de inactividad**, tras el cual, la sesión de usuario será finalizada de manera automática.
- **Implementación de medidas de seguridad** frente a ataques que interrumpan la continuidad del negocio, tales como DoS o DDoS.

[8] Se trata de un sistema de autenticación que permite a los usuarios autenticados acceder a múltiples aplicaciones y servicios vinculados sin necesidad de volver a autenticarse.

4.9. Uso de mensajería instantánea para los administradores de fincas

Tanto en el ámbito laboral como en el personal, las **aplicaciones de mensajería instantánea** se han convertido en una parte esencial en el día a día. La facilidad de uso y la posibilidad de establecer comunicaciones de manera inmediata ha conseguido que estas herramientas se incorporen también en los despachos de administración de fincas.

Un uso responsable puede beneficiar a las empresas en diferentes aspectos, proporcionando una comunicación rápida y eficiente, tanto interna como externa. Este tipo de aplicaciones no solo permiten la coordinación entre empleados y la resolución de problemas de forma conjunta, sino que mejoran las comunicaciones con los clientes y proveedores, permitiendo proporcionar una atención más personalizada y ágil.

Sin embargo, para **garantizar la seguridad y la privacidad** en las comunicaciones y preservar la información compartida, es importante seguir ciertas pautas a la hora de utilizarlas.

El despacho que desee comunicarse con sus clientes por medio de aplicaciones de men-sajería instantánea **revisará si este tratamiento es lícito, y lo será si cumple con alguna de las condiciones descritas en el artículo 6**, licitud del tratamiento, del RGPD. La licitud del tratamiento se podrá establecer en el consentimiento explícito de los interesados (siempre en el caso de los clientes), en el interés legítimo de la empresa (en el caso de los empleados) o si es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

También se **debe cumplir con lo indicado en el artículo 13 del RGPD**. En este se indica que el responsable del tratamiento informará al interesado sobre su identidad, la finalidad del tratamiento y su base de legitimación, los destinatarios de los datos y qué derechos amparan a los interesados, entre otros aspectos.

Las **entidades** (empresas o autónomo/as) que quieran utilizar una aplicación de mensajería instantánea deberán utilizar las versiones profesionales. Por ejemplo, en la versión Business de WhatsApp, este sería el encargado del tratamiento de la entidad que la utiliza, siendo el despacho responsable de esos datos y no WhatsApp, como ocurriría con su versión ***Messenger***, diseñada para comunicaciones personales.

En este sentido, existen aplicaciones de mensajería, que en esa versión *Business* cuentan con una **API** (*Application Programming Interface*) que permite implementar diferentes funciones de la aplicación en otros productos *software* utilizados en los despachos, como es el caso del CRM, para la gestión de la comunicación con los clientes.

Dentro de esta API se puede ofrecer a los usuarios la información antes mencionada, en el primer mensaje que abra la conversación, lo que se conoce como la primera capa informativa, además de **obtener su consentimiento** [64] antes de comenzar a interactuar con ellos.

Es **recomendable que solamente se usen estas aplicaciones como canal de comunicación a nivel informativo** o como envío de publicidad, no como medio para compartir datos personales o información confidencial. Esto se debe a que los datos se escapan del control del despacho al depender de la política de privacidad de las aplicaciones que, en algunos casos, supone transferencias internacionales de datos, con el riesgo que ello supone.

Por otro lado, es responsabilidad del despacho implantar las **medidas de seguridad** necesarias que garanticen la protección de datos al usar estas aplicaciones, en concreto, las medidas referentes a la custodia de teléfonos móviles usados para estas comunicaciones y en los que se almacenen los datos personales de los clientes y/o empleados.

Además, en caso de violación de la seguridad o del ejercicio de los derechos de los interesados, el responsable será el despacho, tal como se indica el artículo 5 del RGPD.

Por último, cuando se pretendan realizar comunicaciones comerciales por medio de la aplicación, se deberán seguir las pautas que indica el artículo 21 de la **Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico** o **LSSI.**

4.10. Certificado digital y firma electrónica

En el sector de la administración de fincas, la eficiencia en la gestión de la documentación y los procesos administrativos es esencial; como también lo es su seguridad. **Con el avance de la digitalización, este tipo de gestiones han pasado de realizarse de manera presencial, en los despachos, a poder ser tramitadas de forma telemática.**

Uno de los mayores avances para garantizar la autenticidad, integridad y no repudio de la documentación digital es la **firma electrónica que utiliza certificados digitales**[9]. La firma electrónica[10] permite garantizar la identidad de la entidad firmante, así como la integridad del documento firmado, es decir, **certifica que dicho documento no ha sido modificado.**

Una de las características más útiles que puede ir asociada a la firma electrónica es lo que se conoce como ***«sellado en el tiempo»***. Se trata de un método para probar que un conjunto de datos (en este caso, la firma que se ha realizado) existió en un momento determinado (fecha y hora). El sellado de tiempo es aportado por un tercero de confianza conocido como **Autoridad de Sellado de Tiempo.**

Al trabajar con documentos de firma electrónica, es muy importante comprobar que los datos firmados se corresponden con los originales y que el certificado, con el que se firma, es válido. Para comprobar la validez de los certificados y firmas, así como validarlas y visualizarlas, deberás utilizar los **servicios suministrados por VALIDe**.

[9] El certificado digital es un documento electrónico que vincula la identidad de una persona física o jurídica con una clave. Es emitido por una autoridad de certificación y se utiliza para autenticar la identidad de los usuarios y poder firmar documentos electrónicamente con validez legal.
[10] La firma electrónica es un conjunto de datos asociados a un documento que permiten identificar al usuario que firma para asegurar la integridad del documento. Suelen utilizarse para firmar contratos o autorizar transacciones y pueden ser más o menos avanzadas, llegando a estar basadas en certificados digitales.

¿Cómo implementar el certificado digital y la firma electrónica en la empresa?

1. **Obtener el certificado digital:**
   - Solicitar el certificado digital en una entidad certificadora reconocida.
   - Instalar el certificado digital en los dispositivos de trabajo.
   - Verificar la validez y la vigencia del certificado digital.
2. **Cómo firmar:**
   - Online, a través de un servicio de verificación y generación de firmas electrónicas como es **VALIDe**;
   - A través de **aplicaciones de firma electrónica** o de **ofimática** que, tras ser descargadas y ejecutadas en un ordenador, permitirán realizar firmas de documentación sin la necesidad de estar conectado a Internet.
3. **Integrar en procesos de trabajo:**
   - Formar a los empleados en el correcto uso de la firma electrónica.
   - Incorporar el uso de certificado digital y firma electrónica en los procesos administrativos.
   - Actualizar y adaptar las políticas internas de seguridad al uso de estas herramientas.
   - Monitorizar y evaluar la eficiencia y seguridad de las herramientas implementadas de forma regular.

4.11. Conexiones remotas

El cada vez más extendido trabajo remoto ha traído consigo nuevos desafíos. **Cada vez son más las empresas que optan por el teletrabajo como opción para sus empleados,** y en el sector de la administración de fincas también es una práctica muy común.

La posibilidad de trabajar en remoto ofrece una mayor flexibilidad, requisito imprescindible para los administradores de fincas que, en ocasiones, **necesitan cambiar de ubicación para realizar sus tareas.**

Cuando se realiza una conexión desde un punto diferente a las instalaciones empresariales, ya sea desde casa o durante un viaje de empresa, **es imprescindible seguir una serie de recomendaciones y buenas prácticas que garanticen la seguridad de la información y la protección de los datos y permita evitar brechas de seguridad.**

Tanto si ya tienes implantada esta modalidad de trabajo en el despacho como si estás pensando en implementarla, te recomendamos que sigas las pautas indicadas en la **política de teletrabajo seguro.**

4.12. Proveedores de servicios TIC

Normalmente, **las empresas contratan ciertos servicios a terceros,** como pueden ser el diseño y mantenimiento de la web, almacenamiento en la nube o cualquier otro servicio, pero el hecho de tener estos servicios contratados no exime de exigir al proveedor de los mismos el **cumplimiento de medidas ciberseguridad, teniendo en cuenta que es importante:**

- **Que los proveedores de servicios tomen las debidas medidas de ciberseguridad** para alinearse y respaldar la política de ciberseguridad de la empresa,
- **Conocer cómo van a actuar los proveedores de los servicios,** en caso de ser víctimas de un incidente de seguridad relacionado con sus servicios.

4.13. Ciberseguros

La implementación de las medidas de seguridad expuestas hasta ahora, **junto con la concienciación y formación de los empleados mejorarán el nivel de seguridad de las empresas del sector de la administración de fincas.**

Aun así, la ciberseguridad al 100% no es posible, y es que los ciberdelincuentes están constantemente creando nuevas técnicas para atacar a las empresas. Ante esta incertidumbre y preocupación por la ciberseguridad de las empresas, **nacen los seguros cibernéticos o ciberseguros**.

Estos seguros están diseñados para proteger a las empresas de los costes asociados a los incidentes de ciberseguridad y gestionar el riesgo asociado. Las pólizas pueden cubrir una gran variedad de costes, y estos pueden ajustarse a las necesidades de la empresa:

- **Respuesta ante incidentes**, es decir, los gastos asociados a la investigación y recuperación tras un incidente de seguridad.
- **Daños y perjuicios**, compensación por las pérdidas económicas durante la interrupción del negocio.
- **Daños a terceros**, compensación a clientes y proveedores afectados por un incidente de seguridad.
- **Responsabilidad legal**, como pueden ser costes asociados con una fuga de datos personales.
- **Reparación de la reputación**, para mitigar los daños producidos a la reputación de la empresa.

Es importante destacar que **no estarán cubiertos los incidentes que sean atribuibles a nuestra empresa por comportamientos ilícitos o intencionados.**

Además, en ningún caso **los ciberseguros pueden sustituir las medidas de ciberseguridad,** sino que se trata de un complemento que puede ayudar a mitigar el impacto económico en caso de incidente.

4.14. Medidas básicas para un despacho seguro

Son muchas las medidas y cuestiones de ciberseguridad que se han tratado en esta guía. Por tanto, para finalizar, haremos un **resumen de las cuestiones que consideramos básicas a tener en cuenta para que nuestro negocio pueda contar con el valor añadido que le da la ciberseguridad y que presentamos en los siguientes puntos.**

4.14.1. Decálogo de ciberseguridad para empresas

Te recomendamos que tengas siempre a mano el **"Decálogo de ciberseguridad para empresas"** de **INCIBE**, que contiene diez pasos imprescindibles a tener en cuenta para ser un despacho ciberseguro, promover la confianza entre tus clientes y ser un negocio competitivo.

4.14.2. Protección del puesto de trabajo

Cualquier puesto de trabajo es susceptible de tener un incidente de ciberseguridad, pero evitarlo o minimizar su impacto es posible si se tienen en cuenta una serie de recomendaciones:

PROTECCIÓN DEL PUESTO DE TRABAJO

PUNTO 1
Destruye la información mediante mecanismos seguros

PUNTO 2
Mantén la confidencialidad de la información de tu empresa

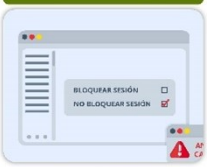
PUNTO 3
No publiques ni compartas contraseñas

PUNTO 4
No conserves contraseñas en lugares visibles

PUNTO 5
Usa contraseñas robustas

PUNTO 6
Mantén actualizado el sistema operativo y el antivirus

PUNTO 7
Bloquea la sesión al ausentarte del puesto de trabajo



PUNTO 8
Realiza un uso adecuado de los dispositivos extraíbles

PUNTO 9
No alteres la configuración de tu equipo corporativo

PUNTO 10
Controla el uso de dispositivos de almacenamiento personal

RECUERDA

- Notificar cualquier incidente de seguridad.
- No uses servicios de almacenamiento online no autorizados por la empresa.
- Guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral.
- No abandonar documentación en las impresoras o escáneres.
- Normativa de utilización de internet y el correo electrónico corporativo.

4.14.3 Empleados seguros: formación y concienciacion

Como ya hemos mencionado, un sistema es tan seguro como lo es su **eslabón más débil**, y normalmente en una organización en la que trabajan multitud de personas suele ser el usuario. Resulta **infructuoso** invertir dinero en tecnologías, herramientas y equipos que protejan la información o los sistemas que la gestionan, si los miembros que hacen uso de ella no tienen en cuenta buenas prácticas, como, por ejemplo, contar con contraseñas robustas.

Para evitar este tipo de situaciones, será de gran importancia **formar y concienciar a todos los miembros del despacho**, ya que en mayor o menor medida son los que gestionan sus recursos críticos. La **formación y concienciación** será la única herramienta con la que inculcar y mejorar sus habilidades en ciberseguridad, lo que, sin duda, repercutirá positivamente en el despacho y en la imagen que proyecta a sus clientes.

A un despacho que cuente con personal formado y concienciado en ciberseguridad, le será mucho más difícil sufrir un incidente de seguridad y, en su caso, lo gestionará de manera mucho más eficiente. Este factor es de **gran importancia**, ya que un incidente de seguridad podría repercutir muy negativamente en su funcionamiento, provocando pérdidas económicas y de reputación e imagen.

Desde **INCIBE** ponemos a vuestra disposición múltiples recursos y materiales con los que elevar la formación de empleados y empresarios. No dejes pasar la oportunidad de contribuir en la seguridad de tu despacho y entra en nuestra **sección de formación.**

4.15. Reporte y resolución de incidentes

Como sabemos la ciberseguridad al cien por cien no existe y cualquier empresa es susceptible de sufrir un incidente de seguridad. En este contexto cobra especial importancia el reporte de este tipo de problemas para interceptar a tiempo casos de fraude, nuevas tipologías de *malware*, fugas de información, etc.

En **INCIBE** contamos con un equipo especializado en el análisis y gestión de incidencias de seguridad y fraude electrónico: **INCIBE-CERT**. Este equipo opera de forma continuada **24 horas al día, 7 días a la semana.**

Si has tenido un incidente o has sido víctima de un caso de fraude electrónico, puedes reportarlo a **INCIBE-CERT** a través de la dirección **incidencias@incibe-cert.es** o mediante el **formulario de contacto**, detallando en el mismo la información de contacto y una descripción lo más completa posible del incidente.

Una vez reportado el incidente a través del correo indicado, los técnicos de INCIBE-CERT se encargarán de evaluarlo y ofrecerte soporte para su mitigación y resolución tanto en sus aspectos técnicos como en la denuncia ante otras entidades.

Puedes consultar el detalle de cómo reportar cada tipo de incidente en la sección **"Te ayudamos: reporta tu incidente"**.

Referencias

[1] **Glosario de términos de ciberseguridad: una guía de aproximación para el empresario** - https://www.incibe.es/empresas/guias/glosario-de-terminos-de-ciberseguridad-una-guia-de-aproximacion-para-el

[2] **TemáTICas Ransomware** - https://www.incibe.es/empresas/tematicas/ransomware

[3] **Cómo gestionar una fuga de información. Una guía de aproximación al empresario** - https://www.incibe.es/empresas/guias/guia-fuga-informacion

[4] **Herramienta de autodiagnóstico** - https://adl.incibe.es/

[5] **TemáTICas Ingeniería social** - https://www.incibe.es/empresas/tematicas/ingenieria-social

[6] **TemáTICas Phishing** - https://www.incibe.es/empresas/tematicas/phishing

[7] **TemáTICas Malware** - https://www.incibe.es/empresas/tematicas/malware

[8] **Principales formas de estafa a través del email: phishing más comunes** - https://www.incibe.es/empresas/blog/principales-formas-de-estafa-traves-del-email-phishing-mas-comunes

[9] **Conoce uno de los ataques más replicados en la Red. El phishing y sus variantes: smishing y vishing** - https://www.incibe.es/empresas/blog/conoce-uno-de-los-ataques-mas-replicados-en-la-red-el-phishing-y-sus-variantes

[10] **Fraude email comprometido** - https://www.incibe.es/empresas/te-ayudamos/fraude-email-comprometido

[11] **Spoofing: todo lo que necesitas saber para proteger tu empresa** - https://www.incibe.es/empresas/blog/spoofing-todo-lo-que-necesitas-saber-para-proteger-tu-empresa

[12] **Informe de transparencia de Google** - https://transparencyreport.google.com/safe-browsing/search

[13] **Free website security check & malware scanner** - https://sitecheck.sucuri.net/

[14] **Virustotal** - https://www.virustotal.com/gui/home/url

[15] **URL haus** - https://urlhaus.abuse.ch/

[16] **Unshorten.It! -** https://unshorten.it/

[17] **Reporta tu incidente -** https://www.incibe.es/empresas/te-ayudamos/reporta-tu-incidente

[18] **Fraude email comprometido -** https://www.incibe.es/empresas/te-ayudamos/fraude-email-comprometido

[19] **¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos -** https://www.incibe.es/empresas/blog/dudas-legitimidad-correo-aprende-identificarlos

[20] **Cuando revisas la seguridad de tu empresa, ¿te fijas en las vulnerabilidades? -** https://www.incibe.es/empresas/blog/cuando-revisas-seguridad-tu-empresa-te-fijas-las-vulnerabilidades

[21] **Seguridad en redes wifi: una guía de aproximación para el empresario -** https://www.incibe.es/empresas/guias/seguridad-redes-wifi-guia-aproximacion-el-empresario

[22] **Aprende Ciberseguridad – Typosquatting -** https://www.incibe.es/aprendeciberseguridad/typosquatting

[23] **Aprende Ciberseguridad – Cybersquatting -** https://www.incibe.es/aprendeciberseguridad/cybersquatting

[24] **Open Web Application Security Project® (OWASP) -** https://owasp.org/

[25] **Medidas de prevención contra ataques de denegación de servicio -** https://www.incibe.es/empresas/blog/medidas-prevencion-ataques-denegacion-servicio

[26] **Protégete frente al defacement y que no le cambien la cara a tu web -** https://www.incibe.es/empresas/blog/protegete-frente-al-defacement-y-no-le-cambien-cara-tu-web

[27] **Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario -** https://www.incibe.es/empresas/guias/seguridad-instalacion-y-uso-dispositivos-iot-guia-aproximacion-el

[28] **Menos es más, controla el acceso a la información -** https://www.incibe.es/empresas/blog/menos-mas-controla-el-acceso-informacion

[29] **TemáTICas Cloud -** https://www.incibe.es/empresas/tematicas/cloud

[30] **Política Clasificación de la información -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Clasificaci%C3%B3n%20de%20informaci%C3%B3n_Pol%C3%ADtica%20de%20Seguridad_2024.pdf

[31] **Ley de Propiedad Horizontal, LPH -** https://www.boe.es/buscar/act.php?id=BOE-A-1960-10906&tn=1&p=20231228

[32] **Reglamento General de Protección de Datos, RGPD -** https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

[33] **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, LOPDGDD -** https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[34] **Trashing o dumpster diving -** https://www.incibe.es/ciudadania/formacion/infografias/trashing-o-dumpster-diving

[35] **Política Borrado seguro y gestión de soportes -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Borrado_seguro_Pol%C3%ADtica%20de%20seguridad_2024.pdf

[36] **Política Uso de dispositivos móviles corporativos -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-corporativos.pdf

[37] **Política Uso de dispositivos móviles no corporativos -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-no-corporativos.pdf

[38] **Política Almacenamiento en dispositivos extraíbles -**https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Alm._dispositivos_extraibles_Pol%C3%ADtica_de_seguridad_2024.pdf

[39] **Boletines de CIUDADANÍA -** https://www.incibe.es/ciudadania/simplenews/subscriptions/landing

[40] **Protege tu web -** https://www.incibe.es/empresas/que-te-interesa/protege-tu-web

[41] **Política Protección de la página web -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-pagina-web.pdf

[42] **Si tu web cuenta con certificado de seguridad, comprueba que utilizas una versión segura del protocolo TLS -** https://www.incibe.es/empresas/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del

[43] **Política Contraseñas -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Contrase%C3%B1as_Pol%C3%ADtica%20de%20seguridad_2024.pdf

[44] **Asegura tus cuentas de usuario con la autenticación de doble factor -**https://www.incibe.es/empresas/blog/asegura-tus-cuentas-usuario-autenticacion-doble-factor

[45] **Copias de seguridad: una guía de aproximación para el empresario -** https://www.incibe.es/empresas/guias/copias-seguridad-guia-aproximacion-el-empresario

[46] **¿Humano o bot? Protege tu web con sistemas captcha -** https://www.incibe.es/empresas/blog/humano-o-bot-protege-tu-web-sistemas-captcha

[47] **Política Gestión de logs -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf

[48] **¿Conoces las pasarelas de pago? ¿Sabes cuál es la más adecuada para tu tienda online? -** https://www.incibe.es/empresas/blog/conoces-las-pasarelas-pago-sabes-cual-mas-adecuada-tu-tienda-online

[49] **Cumplir la ley, ya seas pyme o autónomo, nunca fue tan fácil -** https://www.incibe.es/empresas/blog/cumplir-ley-seas-pyme-o-autonomo-nunca-fue-tan-facil

[50] **Suscripción a boletines de Empresas -** https://www.incibe.es/empresas/simplenews/subscriptions/landing

[51] **Cifrado de la información: protege el principal activo de tu empresa -** https://www.incibe.es/empresas/blog/cifrado-de-la-informacion-protege-el-principal-activo-de-tu-empresa

[52] **Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades -** https://www.incibe.es/empresas/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

[53] **La microsegmentación como defensa contra el ransomware -** https://www.incibe.es/empresas/blog/la-microsegmentacion-como-defensa-contra-el-ransomware

[54] **Recomendaciones de seguridad en el empleo de redes VPN -** https://www.incibe.es/empresas/blog/recomendaciones-seguridad-el-empleo-redes-vpn

[55] **Política Actualizaciones de software -** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-software.pdf

[56] **¿Qué son y para qué sirven los SIEM, IDS e IPS? -** https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

[57] **Plan de Contingencia y Continuidad de Negocio -** https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio

[58] **Acuerdo pactado, contrato firmado. ¡Protege tu empresa! -** https://www.incibe.es/empresas/blog/acuerdo-pactado-contrato-firmado-protege-tu-empresa

[59] **Aplica estos consejos y protege tus videollamadas -** https://www.incibe.es/empresas/blog/aplica-estos-consejos-y-protege-tus-videollamadas

[60] **Ciberseguridad en el teletrabajo: una guía de aproximación para el empresario** https://www.incibe.es/empresas/guias/ciberseguridad-en-el-teletrabajo-una-guia-de-aproximacion-para-el-empresario

[61] **Si tu web cuenta con certificado de seguridad, comprueba que utilizas una versión segura del protocolo TLS -** https://www.incibe.es/empresas/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del

[62] **Pagos en línea más seguros: PCI DSS versión 4.0 -** https://www.incibe.es/empresas/blog/pagos-en-linea-mas-seguros-pci-dss-version-40

[63] **Directiva PSD2. Reforzando la seguridad de los pagos digitales en el comercio online -** https://www.incibe.es/empresas/blog/directiva-psd2-reforzando-seguridad-los-pagos-digitales-el-comercio-online

[64] **Obtener el consentimiento para WhatsApp -** https://developers.facebook.com/docs/whatsapp/overview/getting-opt-in

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

Consejo de Colegios Administradores de Fincas Castilla y León

Administrador Fincas Colegiado