10 SEP. 20

NAGANOWARE

SEGURIDAD INFORMÁTICA

CONSEJOS PARA TRABAJAR DE FORMA SEGURA.

CONSEJOS PARA TRABAJAR DE FORMA SEGURA

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente documento se ha creado con el objetivo de presentar de la forma más clara y completa posible las medidas de seguridad a nivel informático que toda empresa debería tomar si sus trabajadores y colaboradores están teletrabajando.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

CIBERSEGURIDAD O SEGURIDAD INFORMÁTICA

La **ciberseguridad** o **seguridad informática** es un concepto muy amplio y complejo que tiene en cuenta multitud de conceptos y disciplinas dentro de la informática y las telecomunicaciones.

Cuando una **persona** o un **equipo informático** están conectados a **Internet**, quedan expuestos a situaciones de riesgo de diversa índole.

No estamos hablando únicamente de los ordenadores, sino que los teléfonos móviles, los televisores inteligentes y cualquier **dispositivo electrónico** con capacidad de conectarse a Internet están también en riesgo.

Hay que tener en cuenta que según el informe *2019 Data Breach Investigations Report* creado por **Verizon** [1], en 2.019 el **71%** de todos los ataques detectados tenían una motivación económica.

Además **RiskIQ** [2] en su artículo *The Evil Internet Minute 2019* estima que cada minuto se perdieron **$2.900.000** debido a ciberataques.

[1] **Verizon Wireless** es un operador de telefonía móvil de Estados Unidos fundado en el año 2000. Es el mayor operador móvil del país con más de 80 millones de clientes. Detrás le sigue AT&T Mobility, con un total de 67,2 millones de clientes.

[2] **RiskIQ** es una empresa de seguridad informática con sede en San Francisco, California. Proporciona software como servicio (SaaS) basado en la nube para que las organizaciones detecten el phishing, el fraude, el malware y otras amenazas a la seguridad en línea.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

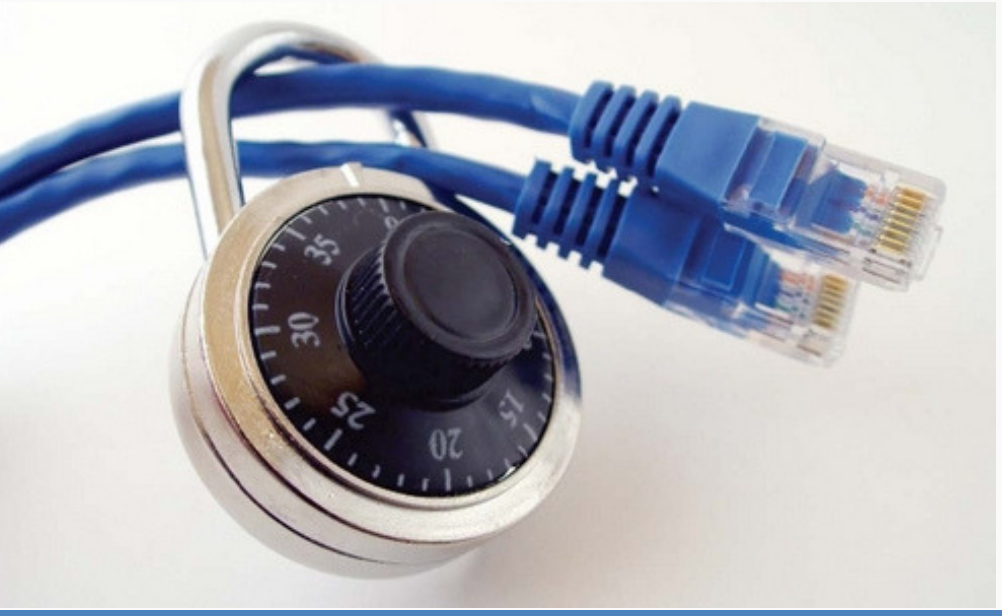
CONSECUENCIAS DEL TELETRABAJO

Antes de la pandemia causada por la **COVID-19**, trabajar desde casa era un lujo que pocos tenían. Esto permitía al equipo IT gestionar e implementar las medidas de seguridad y protocolos de un modo centralizado.

Ahora el trabajo remoto se ha convertido en una **realidad** y para muchas empresas va a convertirse en algo habitual.

En este nuevo escenario, la seguridad informática está siendo comprometida y muchas empresas se ven obligadas a actualizar sus **políticas de seguridad**.

Incluso en un escenario híbrido, en el cual parte del personal está en la oficina y parte teletrabajando, hay que reestructurar los **protocolos de seguridad** y reforzar los canales de acceso al correo electrónico, documentos y servicios internos.



NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

RIESGOS A TENER EN CUENTA EN CUALQUIER SITUACIÓN (I)

- Presentamos situaciones de riesgo en las que nos podemos encontrar en cualquier momento -

1. Malware y Phising

El correo electrónico es una de las principales fuentes de riesgo. Según el informe de **Verizon**, en 2019 el 94% del **malware** [3] llegó por correo electrónico.

Más del 80% de los ataques de ingeniería social llegan por correo electrónico en forma de ataques tipo **phishing** [4]. Muchos ataques basados en el uso del **correo electrónico** tienen ahora como **argumento principal** la **pandemia de la COVID-19**. Este tipo de ataques va creciendo día a día y son cada vez más sofisticados.

2. Redes WIFI públicas

Una de las técnicas que utilizan los **hackers** para tener acceso a nuestra información es la de **compartir** una **red WiFi** desde su propio equipo y **rastrear** todo el tráfico de datos que se genera entre nuestro equipo e Internet.

Pueden hacerlo, aunque nos ofrezcan una **red WiFi** protegida mediante contraseña ya que el equipo del hacker hace de **router** y la información que viaja por la **red WiFi** está encriptada entre el equipo cliente y el **router**, en el **router** se **desencripta** y se **envía a Internet.** Además, el resto de usuarios y dispositivos conectados a la misma red podrían obtener acceso a nuestro equipo.

3. Memorias USB desconocidas

Otra de las técnicas que utilizan los **hackers** es la de dejar diversas **memorias USB** con **archivos infectados** repartidas cerca del edificio de la entidad que quieren atacar.

La probabilidad de que un trabajador coja una de estas memorias USB y la conecte a un equipo de la empresa es muy alta.

[3] **Malware** hace referencia a un tipo de programas diseñado para realizar **acciones dañinas** a un sistema informático y sin el consentimiento y conocimiento del usuario. A finales del siglo XX se conocía a este tipo de software como **virus informático**. Actualmente un **virus informático** es un tipo de **malware**.

[4] **Phishing** es un término informático que denomina a un conjunto de **técnicas** que persiguen el engaño a una víctima ganándose su confianza **haciéndose pasar** por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para **manipularla** y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).**Malware formático**. Actualmente un **virus informático** es un tipo de **malware**.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

RIESGOS A TENER EN CUENTA EN CUALQUIER SITUACIÓN (II)

- Presentamos situaciones de riesgo en las que nos podemos encontrar en cualquier momento -

4. Trabajar en espacios abiertos

Hay que ir con mucho cuidado si trabajamos en un espacio donde alguien pueda observar en nuestra **pantalla** lo que estamos escribiendo o poder ver en nuestro **teclado** las teclas que estamos pulsando.

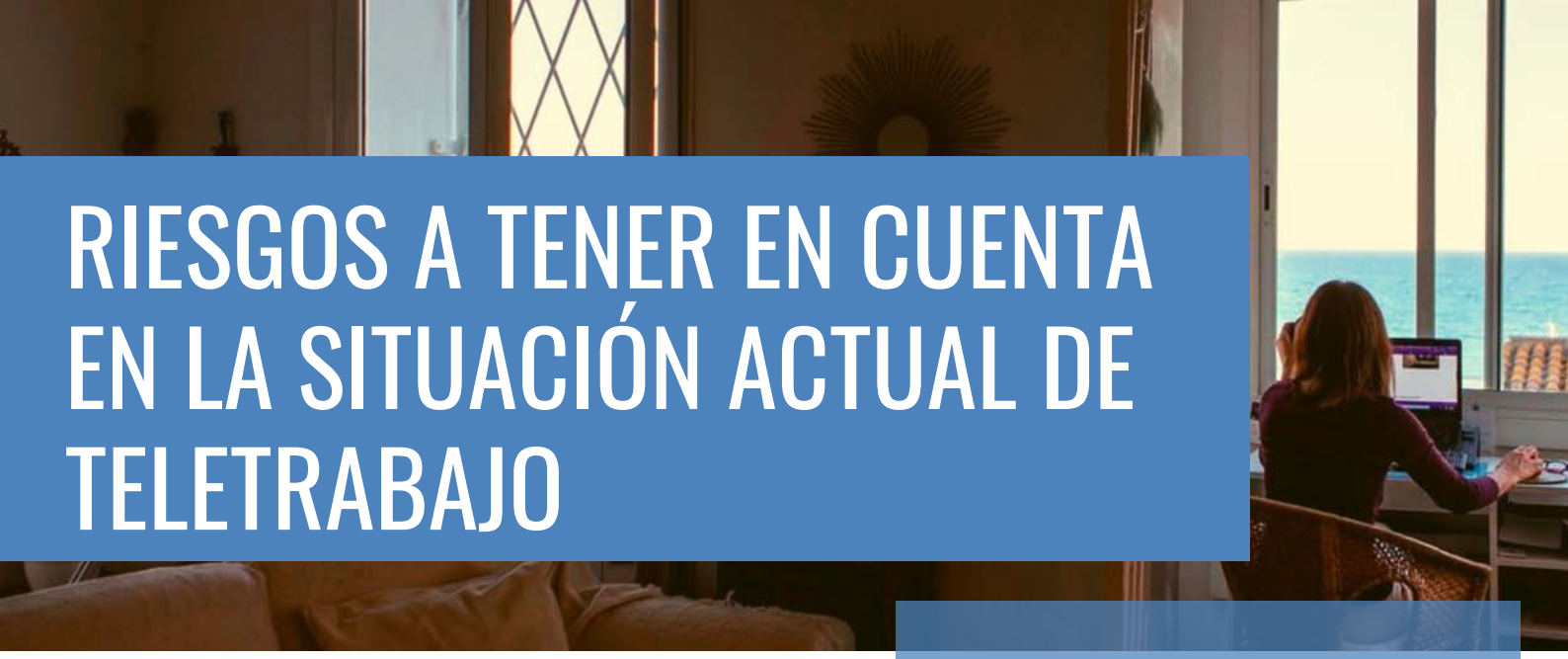
Además, hay que tener nuestros dispositivos todo el rato a nuestro alcance. En el tiempo que nos toma **ir al baño**, un **hacker** podría intentar **desbloquear** nuestra **sesión de usuario** con herramientas copiadas en una memoria USB que son capaces de probar secuencias de hasta 1.000 palabras por minuto.

5. No dejar nuestros dispositivos a ningún desconocido sin nuestra supervisión

Otra de las técnicas que utilizan los **hackers** para tener acceso a nuestra información es pedir a la víctima el **teléfono** para hacer **una llamada.**

En el tiempo que podría tomar a una persona teclear el número de teléfono al que quieren llamar, un hacker podría instalar una aplicación malware en nuestro teléfono que le permita tomar control total del dispositivo.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com



RIESGOS A TENER EN CUENTA EN LA SITUACIÓN ACTUAL DE TELETRABAJO

El teletrabajo tiene sus beneficios. Ofrece más flexibilidad y permite conciliar la vida personal y la profesional. Pero desde el punto de vista de seguridad, presenta una serie de problemas si los trabajadores bajan la guardia.

1. Todo está cambiando muy rápido

Desde el inicio del confinamiento hemos experimentado en cuestión de meses una transformación digital que en condiciones normales hubiera tomado años. Este cambio tan rápido genera una serie de **vulnerabilidades** en los **sistemas informáticos** y muchas **dudas** a los trabajadores. Los **atacantes** pueden aprovechar esta **confusión** y **conseguir sus objetivos** de forma mucho más **fácil.**

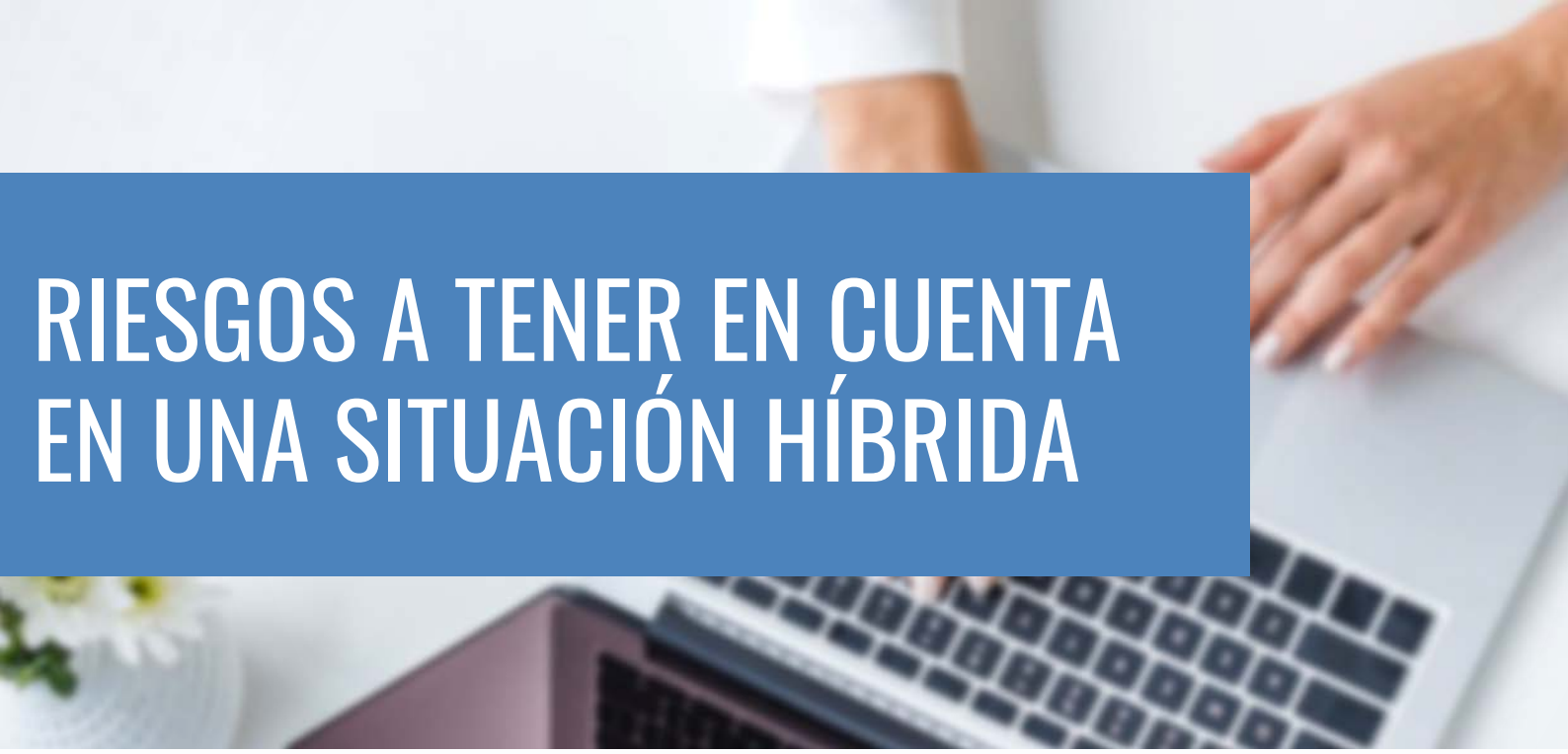
2. Relajación por parte de los trabajadores

Un trabajador bajará la guardia cuando está en casa. Algunos incluso dejarán el equipo de empresa a sus hijos para que jueguen, o aún peor, trabajará con su equipo personal, sin herramientas seguras para protegerlo.

3. La conexión VPN no soluciona todos los problemas

Es cierto que las **conexiones VPN** son una herramienta muy útil para proteger las comunicaciones entre los equipos remotos y la red de la oficina, pero **no bloqueará** a un posible **atacante** que tenga acceso al equipo remoto y que pueda utilizar el canal VPN para acceder y comprometer la seguridad de la red interna.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com



RIESGOS A TENER EN CUENTA EN UNA SITUACIÓN HÍBRIDA

*Una solución **híbrida** presenta todavía más problemas para aquellos que trabajan a**lgunos días en casa y otros en la oficina**.*

1. Red comprometida

La **red interna** de la oficina podría estar en riesgo si un trabajador utiliza un **equipo infectado** dentro de la oficina. Un equipo que ayer era seguro puede que hoy sea un riesgo para la empresa. En algunos casos el equipo infectado tendría acceso a la red **sin necesidad de credenciales** ya que la **sesión de usuario** sigue siendo válida.

2. Documentos infectados

Un **documento infectado** fuera de la oficina puede ser un problema.

Un **trabajador** podría **enviar** este documento por **correo electrónico** a un compañero de trabajo que está conectado a la **red interna** que, al abrirlo, quedará **infectado** si no se toman las **medidas adecuadas**.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (I)

1. Formar a los administradores IT y trabajadores de la empresa

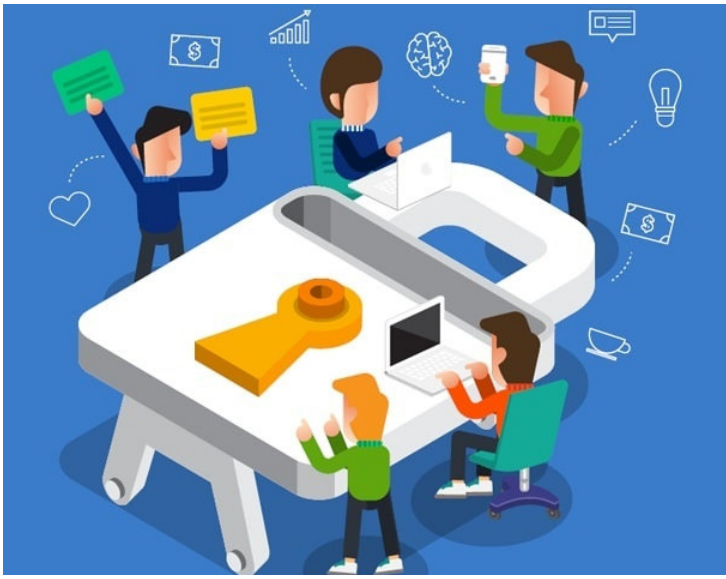
Dada la rapidez en la que se están sucediendo los cambios y la aparición de nuevas amenazas, lo primero y más importante es que expertos en la materia pongan al día a los administradores IT y les presenten **herramientas** y **soluciones** que sean **efectivas**.

Los **trabajadores** deben recibir **formación** para **identificar ataques** que les puedan llegar a través del **correo electrónico** y que intenten, por ejemplo, conseguir información por ingeniería social.

Los ataques basados en **ingeniería social no son exclusivos del correo electrónico**. Pueden darse mediante una **llamada telefónica** con un desconocido (o incluso con una persona con la que tenemos cierta confianza).

Hasta en una **conversación informal** en un restaurante, bar o incluso por la calle. Requieren ciertas **habilidades sociales** y el uso de una serie de técnicas con el objetivo de **extraer información** que permita al atacante acceder a **nuestras cuentas** o utilizar dicha información para tener acceso a **otra presa de mayor interés**.

Es la llamada "sensibilización a la ciberseguridad" (en inglés "cybersecurity awareness"). Hoy en día existen multitud de opciones de formación enfocadas a que las personas tomen consciencia de las situaciones de riesgo en las que pueden verse involucradas.



NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (II)

2. Copia de seguridad

La mejor herramienta contra cualquier situación de secuestro de información es disponer de **una copia de seguridad**.

Hay muchas situaciones en las que tener el sistema de copias de seguridad en perfecto funcionamiento nos puede ser muy útil: **Borrado** accidental o intencionado de **información**, **corrupción** de algún **archivo** o **sistema de archivos** del disco de algún equipo, **desastres naturales, robo** o **destrucción** de **equipos informáticos**, etc…

Desde un punto de vista de **ciberseguridad**, los ataques tipo "**Ransomware**" son el mejor ejemplo de situación que se soluciona simplemente con una **copia de seguridad al día**.

Los ataques tipo **"Ransomware" encriptan** todos los **archivos** de usuario del **equipo** y a **todos los archivos a los que tienen acceso vía red**. A continuación, dejan algún documento o mensaje en pantalla en el que indican que para poder disponer de la clave para **desencriptar** los **archivos** debemos **pagar un rescate**. Este tipo de ataques normalmente llegan a través del **correo electrónico** y son muy **peligrosos** debido al hecho de que no se detienen en el equipo sino que el ataque se **propaga a través de la red**.

La recomendación en estos casos es evitar pagar el rescate ya que al final estamos financiando una actividad muy peligrosa y dañina para los negocios.

Existen **empresas expertas** en este tipo de situaciones que disponen de **herramientas** que permiten **romper la encriptación** y conseguir la **contraseña**.

Es un servicio que tiene un coste inferior del que pide el secuestrador, pero no es 100% efectivo.

La mejor solución es disponer de una copia de seguridad. Una vez eliminado el malware que está encriptando los archivos, podremos eliminar los archivos encriptados y sustituirlos por los existentes en la copia de seguridad.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (III)

3. Activar la verificación en 2 pasos

Hay que activar la **verificación en 2 pasos** (en inglés "**2-step verification**") en el **correo electrónico** y en **cualquier servicio que lo permita**, incluso para los servicios internos de la empresa. Este tipo de autenticación necesita de un código generado una vez introducidos el nombre de usuario y contraseña correctos.

Dicho código se generará mediante una App de móvil o se nos enviará vía e-mail o SMS. También podemos usar llaves de seguridad para facilitar el proceso de verificación.

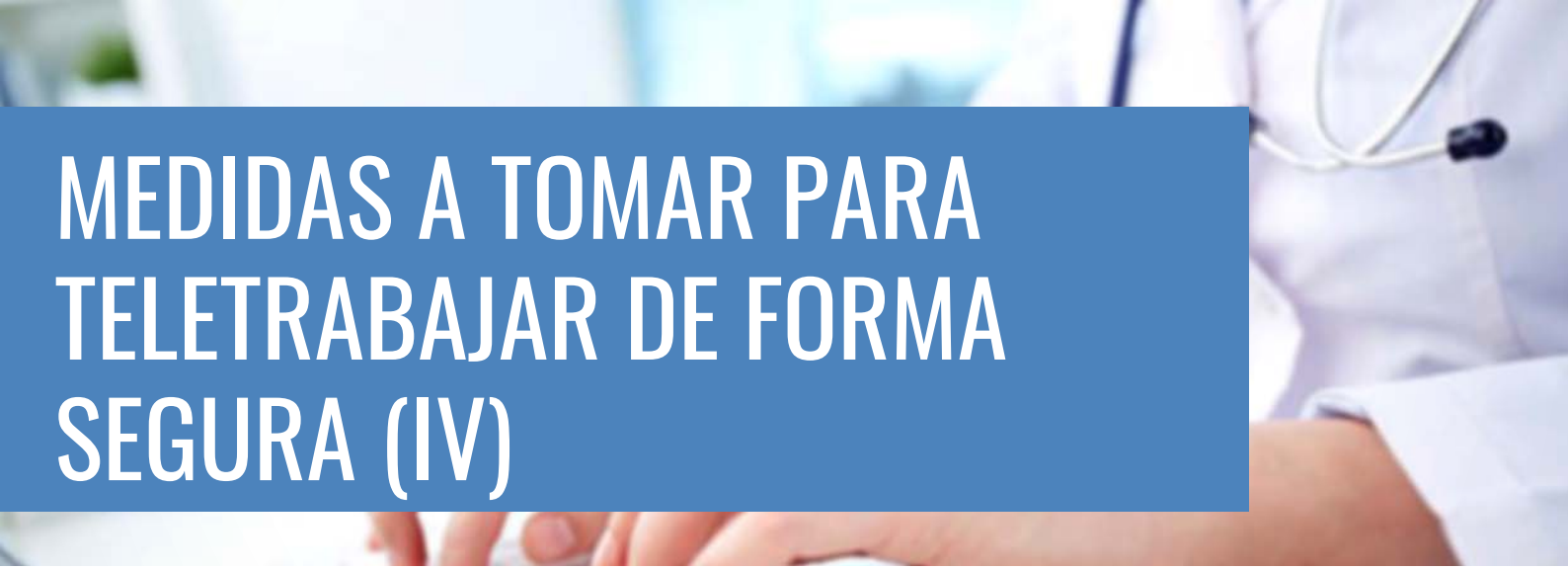
Recomendamos **evitar** el uso del sistema de envío de **SMS** ya que un **hacker** podría interceptar este **SMS** simplemente pidiendo un **duplicado** a nuestra **compañía telefónica** si conoce nuestro **NIF** y **número de teléfono**.

Si queremos usar la opción de la App de móvil podemos usar la aplicación **Microsoft Authenticator** (disponible para Android y Apple). Esta aplicación permite guardar la configuración de llave en una cuenta Microsoft, por lo que, si perdemos o se rompe nuestro dispositivo, podemos recuperar la configuración de llaves ahorrando mucho tiempo para resetear la configuración de seguridad de todas las cuentas.

Haciendo esto, cualquier **intento de acceso** a nuestra cuenta no podrá completarse si no se dispone del **código**.

Además, un **intento fallido** de acceso generará un **aviso** que nos dará a entender que alguien más dispone de nuestras credenciales y que **deberemos modificarlas lo antes posible**.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com



MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (IV)

4. Detener los ataques que lleguen a través del correo electrónico

Da igual la gran cantidad de vulnerabilidades que aparecen constantemente y los ingeniosos sistemas que se crean para romper la seguridad de una red.

Hay un canal de acceso que despunta por encima del resto: el **correo electrónico.**

Hay un tipo de ataque indetectable por muchos sistemas automáticos: los basados en **ingeniería social** y en concreto el **phishing**.

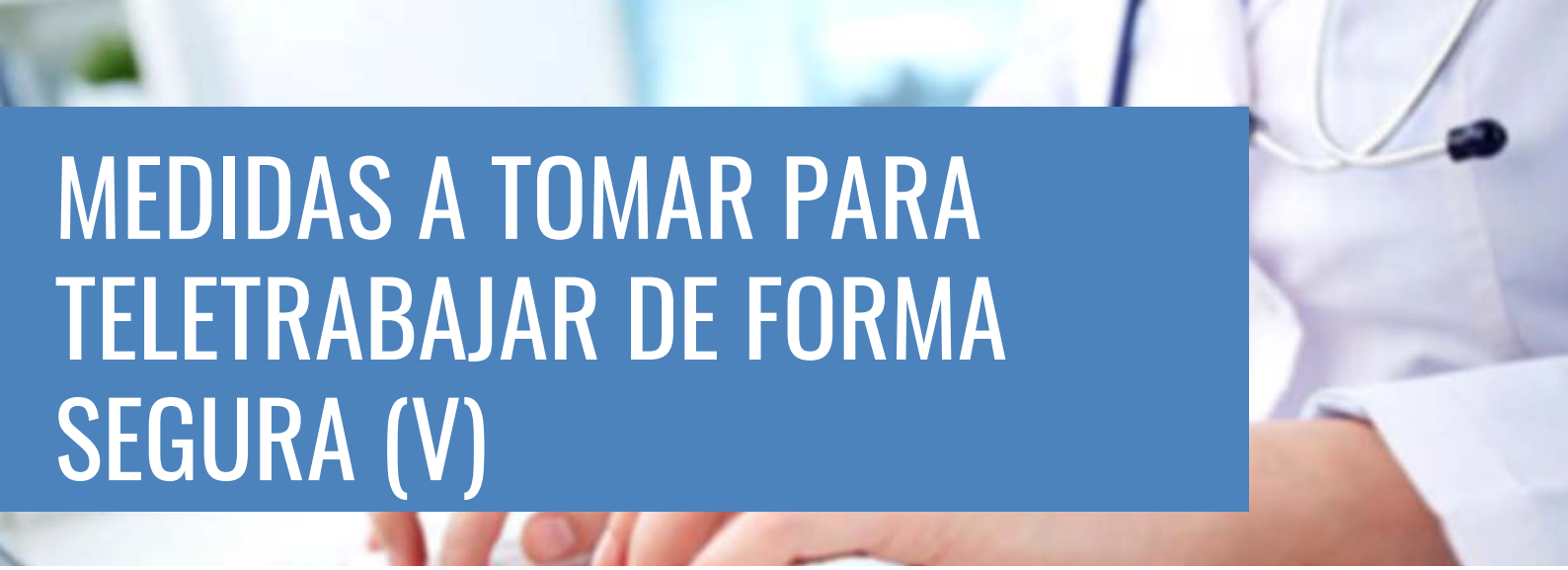
Los ataques tipo **phishing** nos presentan un **correo electrónico**, supuestamente de nuestro **banco** o de **algún proveedor de servicios**, que nos invita a acceder a dicho servicio para leer algún **mensaje privado, descargar una factura** o cualquier otro motivo que despierte nuestra **curiosidad** o **necesidad** de acceder.

Al pulsar el enlace accedemos a una página web que no es realmente la de nuestro proveedor, sino que es una **página trampa** que ha preparado el **hacker**.

Si introducimos nuestro nombre de usuario y contraseña estaremos **dando nuestras credenciales al hacker**.

Es importante **contratar** un **servicio de filtraje de correo** que sea efectivo y capaz de detectar éste y muchos otros tipos de ataques para **evitar que lleguen a la bandeja de entrada de los empleados.**

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com



MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (V)

5. Reforzar la seguridad en los equipos de trabajo

Gran cantidad de los ataques que ocurren actualmente van dirigidos a las **personas** como medio a través del cual acceder a **información que sea de valor**.

Eso significa que en una situación de teletrabajo el foco de atención se ha desplazado a la red doméstica, mucho menos segura que una red empresarial.

Es importante que los trabajadores utilicen **dispositivos proporcionados por la empresa** y que estos equipos se entreguen con **medidas de seguridad** como son la instalación de un **firewall, sistemas de detección de amenazas (EDR o Endpoint Detection and Response) y antivirus.**

Un trabajador con derechos de administración podría deshabilitar estas herramientas de seguridad argumentando que reducen el rendimiento del equipo o podría instalar programas que podrían contener malware.

Por ese motivo los trabajadores deberían trabajar con **usuarios sin privilegios de administración.**

6. Disponer de un sistema centralizado de monitorización, detección de riesgos y ataques

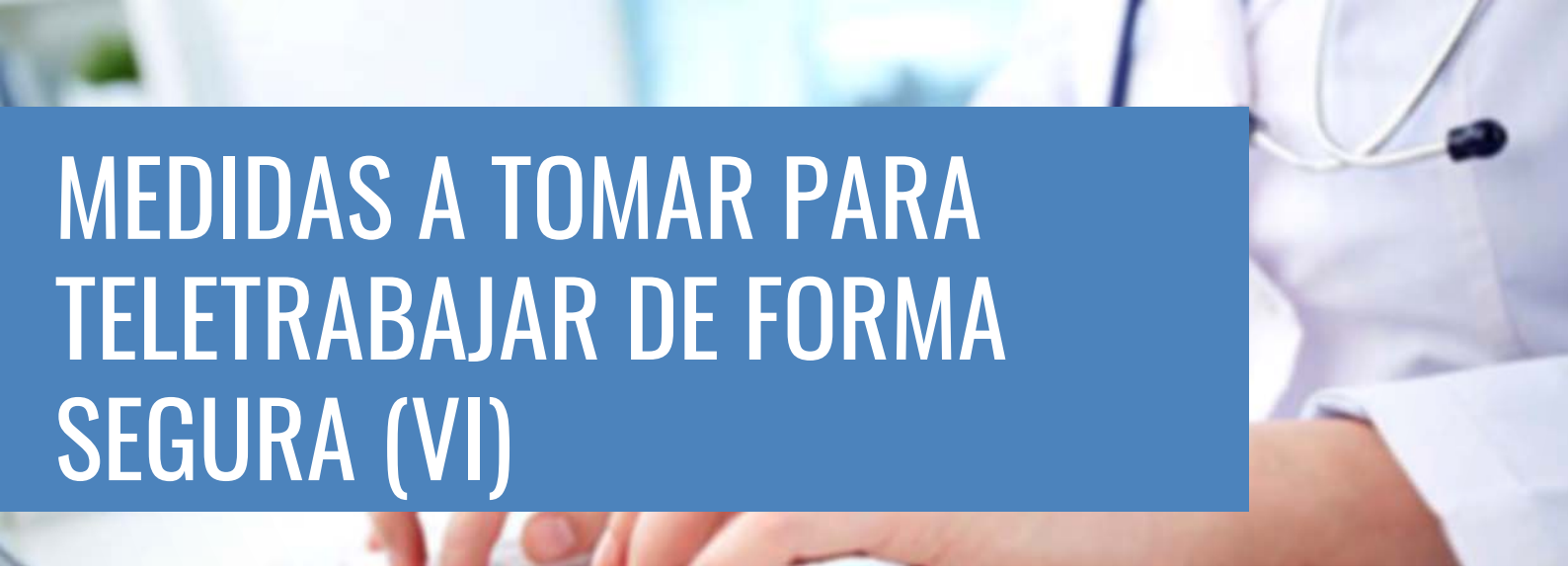
Todas las medidas de seguridad que tomemos para proteger los equipos no sirven de nada si no son capaces de **reportar en tiempo real** a los **responsables IT** cuando aparecen problemas, incluso cuando este equipo no está conectado a la red de la oficina.

Las soluciones tipo **SaaS** [5] que nos ofrecen los propios fabricantes de los **EDR** y **antivirus** son muy útiles para poner en marcha un **sistema de monitorización** de **alarmas** con muy poco esfuerzo.

Sea cual sea la solución seleccionada, **ésta debe disponer** de elementos de seguridad capaces de **enviar notificaciones en tiempo real** a los **responsables IT**.

[5] **SaaS** (del inglés "Software as a Service") es un modelo de distribución de soluciones software donde el soporte lógico y los datos que maneja se alojan en servidores de terceros a los que se accede vía Internet desde cualquier computador en forma de página web, programa de escritorio o Aplicación móvil.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com



MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (VI)

7. Responder a las incidencias detectadas

Aunque parezca una trivialidad, nuestro equipo técnico debe ser capaz de procesar las alarmas generadas por las herramientas de monitorización.

Es importante definir los protocolos de actuación y los tiempos de resolución de las incidencias.

En ciertos casos, quizás nos interese externalizar este servicio de respuesta a incidencias y contratar una empresa que, por ejemplo, pueda actuar las 24 horas del día y los 7 días de la semana.

8. Conexión VPN a la red de la oficina

Las **Redes Privadas Virtuales** o **VPN** crean una **conexión de red segura** a través de Internet entre 2 redes o equipos informáticos.

En un entorno empresarial, se utiliza para **conectar** entre sí la **red** de 2 o más **sedes** de una empresa y permite a un **equipo informático** que está fuera de la oficina **conectar** de **forma segura** con la **red de la oficina**.

Esto posibilita que podamos usar todos los **servicios internos** de la empresa sin estar físicamente en nuestro lugar de trabajo, intercambiar información entre sedes de **forma segura**, proteger el acceso al **correo** electrónico **corporativo** forzando que se pueda acceder únicamente desde la **red interna** de la oficina.

Las **conexiones VPN** permiten la integración con **sistemas de verificación** en **2 pasos**, aumentando considerablemente la seguridad que ya ofrece una VPN y reduciendo el riesgo en caso de **pérdida** de un equipo portátil o el robo de credenciales.

Otra ventaja de la **conexión VPN** es que la navegación por **Internet** queda **protegida** del mismo modo que lo está cuando se navega desde un equipo de la oficina.

Este hecho tiene como consecuencia principal que la **ubicación física** del trabajador queda **oculta** detrás del **Firewall** de la empresa, por lo que damos un extra de protección al trabajador.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (VII)

9. Exigir un nivel mínimo de seguridad para permitir acceso a la red interna

Es importante que cuando un equipo se conecte a la red de la oficina tengamos garantías de que lo hace de forma segura y que no supone ningún **riesgo** para el resto de usuarios.

Para poder asegurar y automatizar esta restricción, disponemos de herramientas que, por ejemplo, no permiten abrir la **conexión VPN** si el antivirus reporta algún aviso de seguridad.

En una red de equipos informáticos basada en **Microsoft Windows**, disponemos de herramientas nativas que obligan a los equipos a cumplir una serie de requisitos antes de poder abrir una nueva sesión de usuario en el equipo cliente.

A parte de los sistemas automáticos, es importante que, por ejemplo, realicemos una revisión de los equipos que han estado trabajando fuera de la oficina antes de **conectarlos a la red interna** y revisar periódicamente que los controles de seguridad están activos.

10. Redes separadas

Una de las medidas que podemos tomar para aumentar la seguridad en un entorno de teletrabajo es la de separar la **red de los trabajadores** que acceden desde casa.

Deben seguir usando una **conexión VPN** pero se les pueden aplicar políticas de seguridad diferentes y restringir todavía más el acceso que tienen a servicios e información de la empresa.

Es importante también **limitar el acceso** que tienen los trabajadores a la información y servicios de la empresa y permitirles únicamente acceso a aquello que necesitan para realizar su trabajo.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (VIII)

11. Encriptar la información sensible

Es muy importante que encriptemos el disco de los equipos que salgan de la oficina. De esta manera en caso de robo o pérdida la **información sensible** que pueda contener el equipo será mucho más difícil de extraer.

Si vamos a enviar un documento o **información sensible** a través de Internet, es recomendable que la encriptemos antes usando aplicaciones como, por ejemplo, **Encrypt Files**.

El receptor deberá tener instalada la misma aplicación y conocer la **contraseña** para poder ver su contenido.

Una manera muy creativa de enviar mensajes de forma segura es incrustando mensajes **encriptados** a través de imágenes.

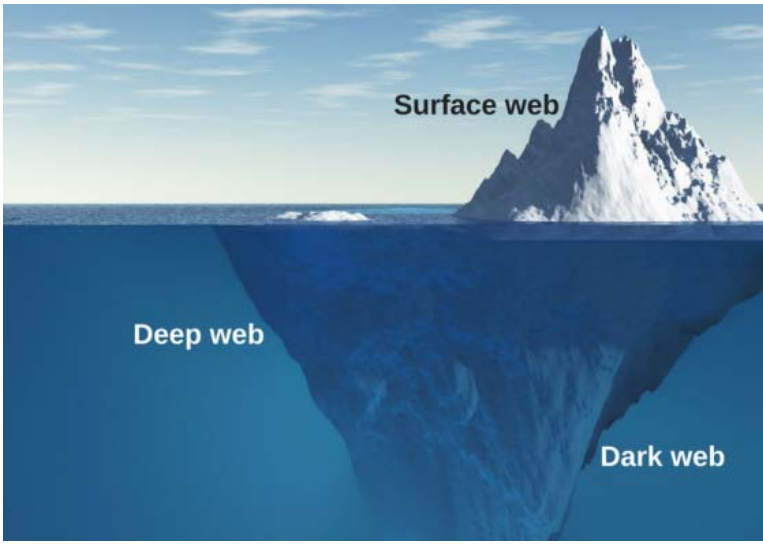
La aplicación ***4t HIT Mail Privacy Lite*** permite hacer esto sobre cualquier imagen de nuestra elección.

12. Gestión de contraseñas

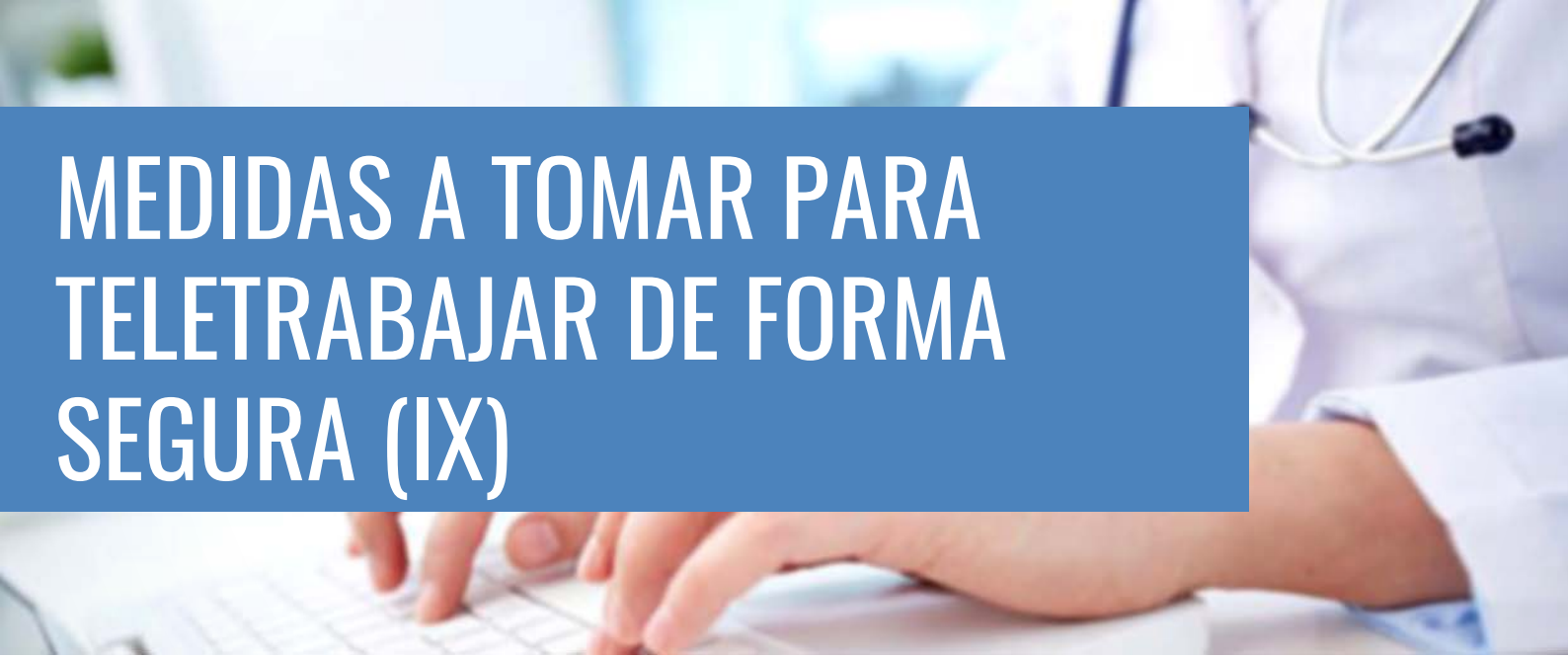
Hay que proteger nuestras cuentas con **buenas contraseñas**.

Para ello debemos conocer cómo evitar que los hackers rompan nuestra contraseña y qué herramientas tenemos para gestionarlas.

Hay varias técnicas que se utilizan para romper una contraseña como la **fuerza bruta**, el uso de **diccionarios**, **phishing** o la compra de contraseñas en la "***dark web*".**



NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com



MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (IX)

Una buena contraseña debe tener las siguientes características:

Mínimamente larga para que no se pueda romper por fuerza bruta. Una contraseña de **6-8 caracteres es demasiado corta** para ser usada en la actualidad. Debe contener **como mínimo 16 caracteres** para considerarse segura.

Evitar **contraseñas obvias** como números secuenciales o palabras simples como “123456789”, “password”, “111111”, “abc123”, “qwerty”, “q1w2e3r4t5” o similar. Evitar nombres de ciudades, personas o lugares sin ningún carácter más añadido. Hay que evitar que un ataque basado en diccionario sea capaz de encontrar nuestra contraseña.

Debe contener una **mezcla de caracteres**: Mayúsculas, minúsculas, números y símbolos.

Evitar **sustituciones comunes** como ciertas letras por números. Si en lugar de usar “Password” utilizamos “P4ssw0rd”, cualquier sistema de fuerza bruta lo va a romper con igual facilidad. En su lugar es mejor romper las palabras y realizar manipulaciones más **complejas**. Por ejemplo, podemos pensar en una frase larga y coger simplemente los 2 primeros caracteres de cada palabra.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (X)

Hay que modificar las contraseñas **periódicamente** ya que mantener una contraseña durante demasiado tiempo aumenta las probabilidades de que alguien las consiga sin que nos demos cuenta.

Una manera de **verificar** si nuestra cuenta de correo ha sido comprometida es usar algún servicio como **https://haveibeenpwned.com**, que nos indicará si nuestra cuenta de correo se ha dado de alta en algún servicio que ha sido recientemente comprometido.

No hay que usar la misma contraseña en todos nuestros accesos. Cada conjunto de credenciales debe contener contraseñas **diferentes** sin ningún **patrón en común**.

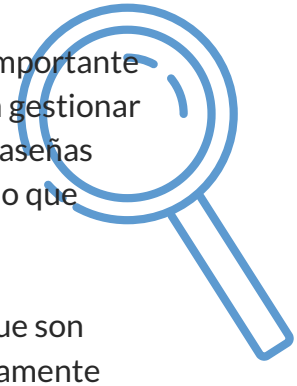
No **anotar** contraseñas en notas de papel que dejemos en la mesa de trabajo o que podamos perder. Tampoco anotar las contraseñas en documentos de texto sin ningún tipo de **protección**.

Es muy importante no **compartir** contraseñas de nuestra cuenta de correo electrónico, banco ni ningún otro servicio sensible o privado. Y no compartir contraseñas de servicios comunes en la empresa con nadie que no necesite tener acceso.

Por último, cuando un trabajador deja la empresa, sea por el motivo que sea, hay que **bloquear** o dar de baja todas sus cuentas y modificar las contraseñas de las cuentas comunes a las que tenía acceso.

El uso de gestores de contraseñas es una buena solución para cumplir con todos estos **requisitos**, aunque debemos elegir uno que cumpla unos mínimos de **seguridad** como, por ejemplo, que guarden las credenciales encriptadas y que permitan la **verificación en 2 pasos.**

En un entorno empresarial es importante que los responsables IT puedan gestionar de forma centralizada las contraseñas comunes de la empresa de modo que controlen **quién tiene acceso.**



Hay gestores de contraseñas que son capaces de **resetear** automáticamente contraseñas cada cierto tiempo, incluso son capaces de actualizar la contraseña en ciertos servicios online de forma automática. Cualquier situación que se produzca en la que sea posible que alguien pueda disponer de nuestras credenciales, deberíamos **modificar** la contraseña y cerrar todas las sesiones abiertas lo antes posible.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (XI)

13. Uso de llaves de seguridad

Las **llaves de seguridad** son la opción más segura de mantener protegida tus cuentas de usuario y acceso a diferentes servicios compatibles con este tipo de tecnología.

Son dispositivos hardware que hacen uso de **U2F, un estándar de verificación** en dos pasos. La diferencia respecto a la verificación en dos pasos tradicional y que ya muchos usamos es que, en lugar de recibir un código, aquí necesitamos tener acceso físico a un dispositivo hardware que hará la función de llave. Sin él no podremos acceder a nuestra cuenta de usuario.

Se presentan como dispositivos conectables a un puerto **USB** (**tipo A**, el formato de siempre, o **tipo C**, el nuevo formato más pequeño) aunque hay modelos inalámbricos, pensados para teléfonos móviles, que se conectan mediante **NFC** (se utiliza para hacer pagos con teléfono móvil) o **Bluetooth**.

La configuración es muy sencilla ya que los servicios compatibles lo presentan como opción al activar la verificación en 2 pasos.

Las llaves de seguridad más conocidas son las de **Yubico** (que se pueden comprar en Amazon) y las **Titan** de **Google** (que están disponibles en España a través de su tienda online).

Es posible **iniciar sesión** en un equipo con **Sistema Operativo Microsoft Windows sin escribir credenciales** utilizando **llaves de seguridad**. Para ello es necesario que ésta implemente el estándar **FIDO2**.

De momento es compatible únicamente con cuentas tipo **Azure AD**, y no funciona de forma nativa (sin añadir software que modifique el sistema de inicio de sesión propio de Windows) con un **Dominio** creado con un servidor con **Sistema Operativo Microsoft Windows.**

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (XII)

14. Aplicar actualizaciones de software / firmware

Tener el **Sistema Operativo** de los equipos (tanto servidores como clientes) y de **las aplicaciones** actualizado nos ayuda a tener nuestros equipos y nuestra red segura.

Las actualizaciones solucionan problemas y fallos detectados por el fabricante o por terceros.

Las **actualizaciones de seguridad** son todavía más importantes ya que solucionan **agujeros de seguridad** que se han hecho públicos y que hacen que nuestro sistema sea **vulnerable**.

Todos los dispositivos de red como **switches, firewall, antenas o controladores WiFi** y cualquier otro dispositivo conectado a la red debe ser actualizado de forma periódica.

Normalmente los fabricantes de este tipo de dispositivos ofrecen un servicio de actualizaciones más o menos automáticas.

Una buena seguridad perimetral requiere que todos los dispositivos estén al día.

Los responsables de IT deberían estar suscritos a algún canal de notificaciones de seguridad para acelerar la aplicación de los parches de seguridad si hay alguna actualización crítica.

Una parte importante de los ataques que aprovechan estos agujeros de seguridad se producen días después de su publicación.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (XIII)

15. Proteger los chats y sistemas de videoconferencia

Uno de los grandes cambios que hemos sufrido es el uso constante de los sistemas de chat y videoconferencia.

En relación a las herramientas de chat, deberíamos separar completamente la vida privada de la personal.

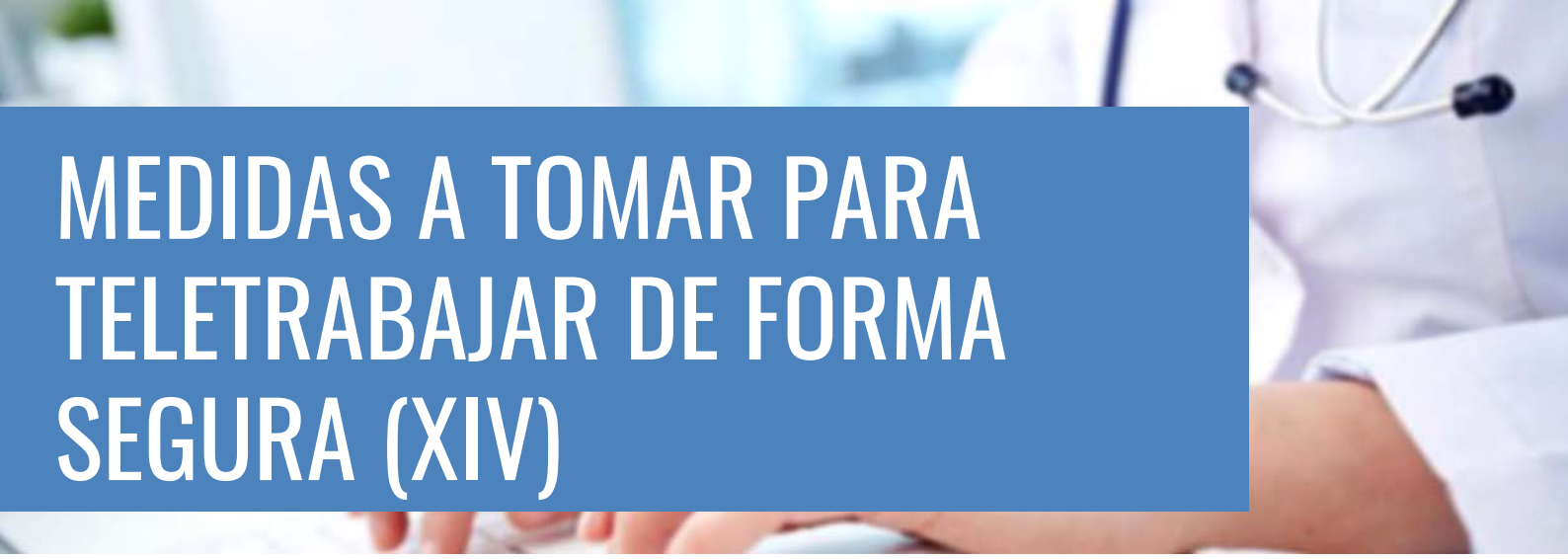
En concreto **WhatsApp** es una herramienta de chat genial que se puede usar en un entorno empresarial, pero es mucho más interesante usar una herramienta ya integrada con nuestra plataforma de correo electrónico, en las herramientas de oficina o el existente en el propio sistema de vídeo-conferencia.

Google Meets y Microsoft Teams son 2 ejemplos de herramientas enfocadas al entorno empresarial con capacidad para chatear y que nos pueden ser más útiles que **WhatsApp** ya que se integran con nuestro sistema de contactos empresarial y que se pueden parametrizar de forma centralizada para adaptarlas a las políticas de seguridad de la empresa.

En cuanto a la plataforma de vídeo-conferencia, antes de plantearse el uso de una plataforma de vídeo-conferencia deberíamos plantearnos las siguientes preguntas:

- *¿Quién puede acceder o entrar en la reunión?*
- *¿Puede ser grabada? En caso afirmativo, ¿lo saben todos los participantes?*
- *¿El contenido de los chats se guarda y es compartido?*
- *Si se pueden compartir archivos, ¿dónde se almacenan?*

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel*: 93 624 36 15*
Mòb*: 608978929*
info@naganoware.com



MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (XIV)

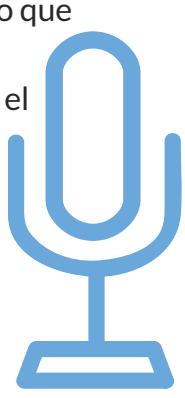
A parte de **Google Meets y Microsoft Teams**, existen plataformas como **Cisco WebEx, Zoom, Jitsi y Verizon BlueJeans** que se han usado muchísimo durante este confinamiento en entorno empresarial. Cada una con sus virtudes y defectos.

Cisco WebEx es la plataforma que lleva más años en el mercado es muy sólida y conocida en entorno universitario y empresarial.

Zoom es una herramienta muy potente que tuvo un crecimiento muy grande durante los meses previos al confinamiento y una muy mala crítica durante el inicio de la epidemia del COVID-19 por diversos problemas de seguridad que la empresa rápidamente solucionó.

Jitsi se presenta como una opción segura y fácil de usar ya que no requiere ningún tipo de instalación. Verizon BlueJeans es una solución empresarial muy segura y con una gran calidad de imagen.

Una de las características que presentan este tipo de herramientas de videconferencia es que permiten difuminar o incluso modificar el fondo de la grabación. Esto es importante en lo que respecta a la privacidad de los trabajadores ya que ayuda a separar el entorno personal del profesional.



NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (XV)

16. Gestión de dispositivos móviles

Al igual que con los equipos portátiles, en un entorno empresarial los trabajadores deberían utilizar teléfonos móviles proporcionados por la empresa y estos estar protegidos, monitorizados y gestionados de forma centralizada.

Para ello, existen las plataformas de **gestión de dispositivos móviles** (en Inglés Mobile Device Management, abreviado MDM) que permiten tener control sobre ellos independientemente del operador de telefonía móvil del que disponga la empresa.

Este tipo de soluciones posibilitan en todo momento aplicar políticas de seguridad que obliguen, por ejemplo, a configurar una contraseña de bloqueo de cierta longitud, permiten también localizar los teléfonos móviles, sincronizar archivos, bloquear funciones no deseadas, instalar software, controlar el consumo y realizar un borrado remoto del dispositivo.

Para que todo esto sea posible es necesario instalar una App en el móvil que hace de Agente de comunicaciones con el servidor central y que está conectado constantemente a Internet para permitir el control remoto del terminal móvil.

17. Auditoría de ciberseguridad

Es importante que de forma periódica se ponga a prueba la seguridad de nuestra empresa, en especial, de la red interna.

Para ello es necesario que expertos en seguridad externos a la empresa elaboren un exhaustivo plan de test, lo ejecuten, redacten un informe detallado de los resultados y, por último, trabajen conjuntamente con los **responsables IT** de la empresa para programar la resolución de los problemas encontrados.

Paralelamente a este análisis detallado, es importante definir una revisión constante de todos aquellos puntos de seguridad cuya monitorización se pueda automatizar y generar alarmas cada vez que alguno de ellos falle para permitir su resolución.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com

MEDIDAS A TOMAR PARA TELETRABAJAR DE FORMA SEGURA (XVI)

18. Disponer de un buen plan de contingencia

Un **Plan de Contingencia** es un conjunto de acciones que permiten reaccionar con eficacia ante crisis, eventualidades o accidentes en una empresa, con el objetivo de lograr que funcione con normalidad en un tiempo definido (llamado MTD o "Maximum Tolerance Downtime").

Desde un punto de vista informático o de **ciberseguridad**, el plan de contingencia va a establecer qué hacer en caso de pérdida de documentos, robo o filtraje de información confidencial, infección de equipos críticos en la red, fallos de servicios críticos y en definitiva cualquier situación que comprometa la seguridad o fiabilidad de los servicios informáticos que ofrece la red de la empresa y que afecten a los principales procesos del negocio.

La situación de **confinamiento** ha sido un ejemplo de contingencia contra la que muchas empresas no estaban preparadas.

En un **plan de contingencia informático**, las **copias de seguridad** tienen un papel muy importante ya que de ellas depende que se pueda, por ejemplo, restablecer el servicio en una nueva estructura de servidores después de un incendio y el tiempo que lleve recuperar los datos de la copia.

Es fundamental que en todo momento mantengamos las **copias de seguridad** lejos de los servidores y una copia siempre fuera de la oficina. Va a ser clave para resolver la mayoría de contingencias vinculadas con **desastres naturales.**

Una vez definido el plan de contingencia informático, éste debe probarse **periódicamente** y debe ser revisado cada cierto tiempo para intentar adaptarlo a los cambios que sufran los equipos informáticos, la red y los servicios de la empresa.

Además, el personal de la empresa debe recibir **formación** al respecto para estar preparados en caso de posibles situaciones de crisis.

NIF: *46761213M*
C/ Hospital 51, 08002 Barcelona
Tel: *93 624 36 15*
Mòb: *608978929*
info@naganoware.com