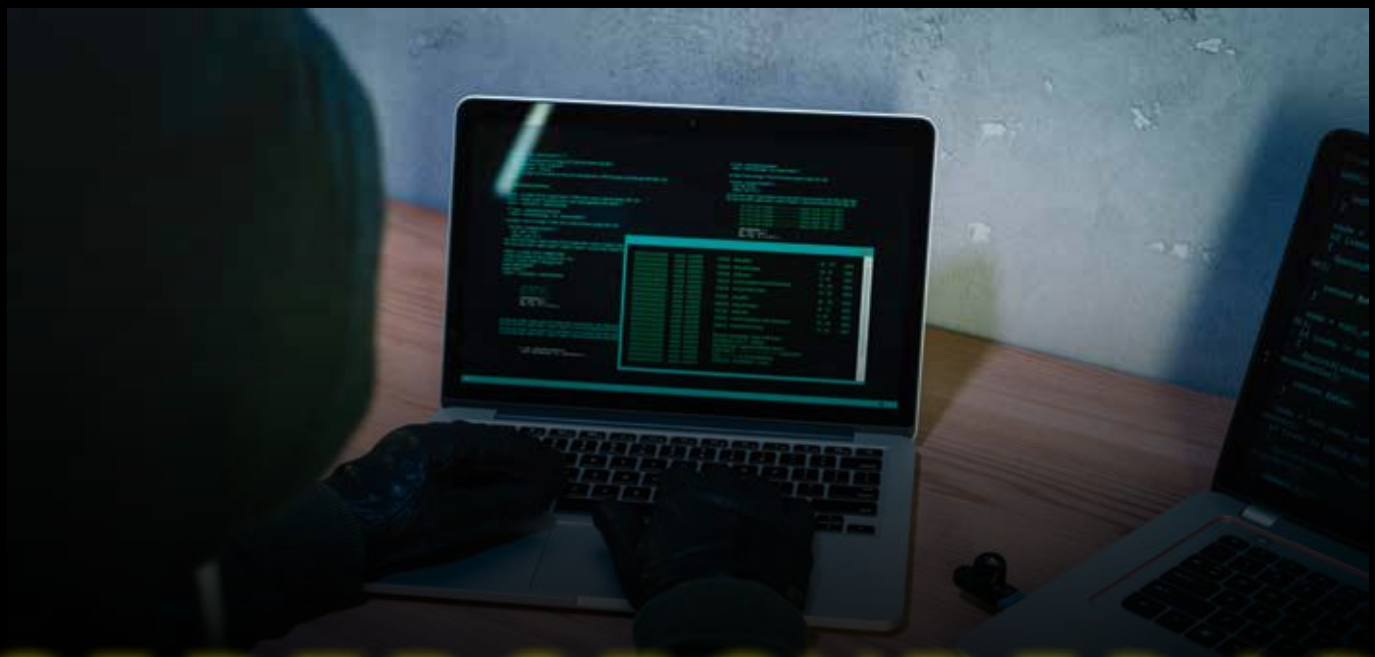


CIBERSEGURIDAD
en los despachos

Unión de Mutuas MCSS N.°267
Pilar Jiménez Ruiz
Responsable de Seguridad de la Información y del Servicio

INTRODUCCIÓN: LA MUTUA

Las mutuas colaboradoras con la Seguridad Social forman parte del Sector Público Institucional, y entre otras, tienen encomendadas las gestiones de:

- El control y seguimiento de las bajas por incapacidad temporal por contingencias comunes y las prestaciones económicas en caso de incapacidad temporal por contingencias comunes. Las prestaciones económicas por riesgo durante el embarazo o la lactancia natural.
- Las prestaciones económicas por cese de actividad de trabajadores autónomos.
- Las prestaciones económicas por cuidado de menores afectados por cáncer u otra enfermedad grave.
- El incentivo a empresas que hayan disminuido de manera considerable la siniestralidad laboral.
- Actividades preventivas conforme a lo dispuesto en la legislación vigente.

Unión de Mutuas dispone de 31 centros propios, entre los cuales se cuenta un hospital, y diversas unidades médicas especializadas: Unidad de Ondas de Choque, Unidad Cardiorrespiratoria, Unidad de Apnea del Sueño y Diagnóstico por la Imagen, entre otras.

IMPORTANCIA DE LA DISPONIBILIDAD DEL SERVICIO Y DE LA INFORMACIÓN

Para garantizar que todos los servicios de Unión de Mutuas se encuentren disponibles en tiempo y forma será necesario adoptar una serie de medidas de protección para evitar que cualquier incidente de cualquier tipología provoque una caída de los servicios esenciales o impida un acceso completo a la información de nuestros pacientes y usuarios.

Los despachos de abogados y graduados sociales también dependen de la información, del acceso a servicios web y de aplicaciones instaladas en sus equipos para atender y gestionar su negocio y a sus clientes. Hoy en día, no disponer de los datos de negocio, de las aplicaciones que los proporcionan o de acceso a Internet y al correo

electrónico, puede provocar grandes pérdidas de negocio o, dependiendo del tiempo de recuperación, el cierre definitivo de nuestra empresa.

¿POR QUÉ APLICAR MEDIDAS DE SEGURIDAD?

Aplicar seguridad sin un motivo o fundamento no tendría sentido. Sin embargo, habitamos una sociedad digitalizada a la que hemos llegado gracias a un enorme desarrollo tecnológico que ha ido evolucionando en paralelo a un gran cambio social. Este desarrollo ha propiciado que actualmente nos conectemos desde cualquier lugar y podamos controlar nuestros negocios y vida disfrutando de una biblioteca de conocimientos en la palma de nuestra mano. Nos encontramos ante una revolución tecnológica global que hemos de conocer muy bien para conocer también los riesgos que trae consigo. Las tecnologías, por sí mismas, no son un problema pero un mal uso de las mismas sí puede generarlo. Disponer de una red de ordenadores y dispositivos móviles en nuestro despacho, conectados a Internet, con acceso al e-mail y servicios web, nos aporta grandes ventajas pero también comporta grandes riesgos. Con solo escuchar las noticias más recientes podemos hacernos una idea:

- España bate su récord en ciberataques: 120.000 incidentes en 2017 (INCIBE).
- El Ministerio de Defensa de España sufre un ataque en su red interna (marzo 2019).
- España fue el objetivo del 80% de los ciberataques a dispositivos del Internet de las Cosas (IoT).
- El Banco de España sufre un ciberataque que impide el acceso a su web desde servidores externos (agosto 2018).

Nos podemos hacer una idea sobre cuál es el nuevo universo social en el que nos encontramos. Estamos frente a un ataque continuado, en muchas ocasiones dirigido contra instituciones concretas pero en otras como ataques de gran difusión, y pueden afectar a cualquiera con acceso a Internet y al correo electrónico.

ATAQUES A LOS DESPACHOS ¿A QUÉ RIESGOS SE ENFRENTAN LAS FIRMAS?

Cuanto más sensible es la información que se gestiona más susceptible es esta de ser objeto del deseo de ciberdelincuentes, para su secuestro y chantaje posterior o reventa. Datos fiscales y laborales de clientes hacen que la información que gestiona un despacho pueda ser objeto tanto de un secuestro de información como de fuga interna. Grandes firmas de despachos ya han denunciado en los últimos años múltiples ataques relacionados con robo de datos e infección de sus equipos.

"Solo durante 2016, en España, se reportaron al menos 70 ataques de *ransomware* en despachos. Cifra que se refiere solo a las denuncias presentadas por los afectados, el número real puede ser muy superior." (Alberto Hernández Moreno. Director general del Instituto Nacional de Ciberseguridad. INCIBE).

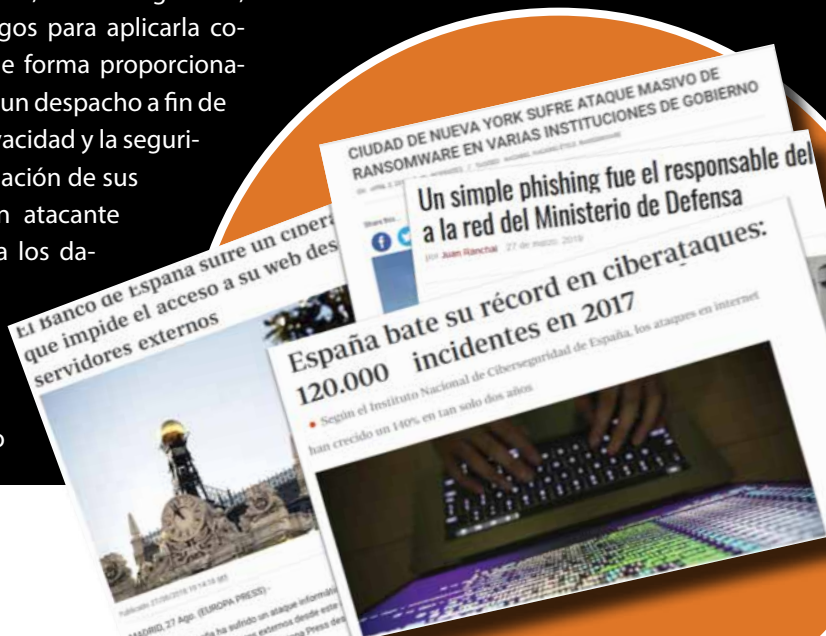
Por este motivo, la ciberseguridad, conocer los riesgos para aplicarla correctamente y de forma proporcionada, será clave en un despacho a fin de garantizar la privacidad y la seguridad de la información de sus clientes. Que un atacante pueda acceder a los datos de nuestros despachos y cifrarlos pidiendo un rescate posterior, o que intenten dañar nuestra reputación a través del secuestro de nuestra página web incorporando en ella contenido malicioso, son riesgos a los que se va a enfrentar un despacho todos los días. Mientras tengamos correo electrónico, acceso a Internet, servicios online o página web, estaremos conectados y seremos susceptibles de sufrir ataques por estos distintos canales.

Así pues, será de vital importancia conocer los riesgos a los que se enfrenta nuestro negocio, en el marco del uso de Internet y de estas nuevas tecnologías, para saber exactamente qué medidas de seguridad será necesario implementar.

Aunque existen muchos riesgos que pueden materializarse en un despacho, podríamos hacer una agrupación sobre la base de diversos riesgos:

- Riesgo de fuga de información
- Riesgo de acceso no autorizado a la información
- Riesgo de entrada de software malicioso.

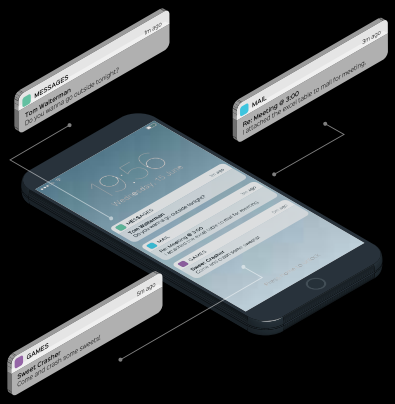
A partir de estas categorías, podemos empezar a trabajar con una serie de controles básicos que serán las instrucciones mínimas con las que deberemos funcionar y trasladar a nuestro personal como parte de sus obligaciones laborales.



MEDIDAS DE CIBERSEGURIDAD BÁSICAS EN EL DESPACHO

Controles para el riesgo de fuga de información

1. Usa dispositivos extraíbles que permitan el cifrado para proteger la información y, consulta previamente si estás autorizado.
2. Trabaja con dispositivos móviles corporativos (smartphones, tablets o portátiles) que se hayan cifrado previamente. Respeta en ellos la configuración original corporativa.



3. No abandones documentación en impresoras o escáneres, sobre todo si estos se encuentran en zonas de paso o son accesibles por terceros no autorizados.

Destruye la documentación en papel mediante mecanismos seguros: haz de la trituradora tu aliada.

4. Política de escritorio limpio: guarda la documentación del puesto de trabajo al finalizar la jornada.

Controles para el riesgo de acceso no autorizado a la información

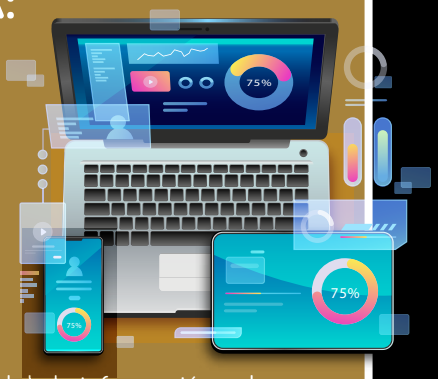
5. Usa contraseñas robustas y, por supuesto, ¡no las compartas ni dejes apuntadas en ningún sitio! Comprueba si son robustas en páginas dedicadas a ello.
6. Cuando te ausentes de tu puesto de trabajo, bloquea la sesión y/o apaga el monitor: puedes activarte el salvapantallas con contraseña.

7. Manda los correos electrónicos cifrados si estos llevan adjuntos con información sensible: evitarás el acceso de terceros no autorizados si lo mandas por error a otra dirección.

Controles para el riesgo de entrada de software malicioso

8. No uses dispositivos USB personales o que hayan podido estar en entornos inseguros. Para evitar la entrada a cualquier software infeccioso utiliza los que te haya proporcionado tu empresa para tus funciones y solo con esa finalidad
9. Sé prudente en la apertura de correos electrónicos. Aplica el sentido común: no pinches en enlaces de correos o remitentes desconocidos, o que demuestren un mal uso del lenguaje y desconfía de los chollos demasiado increíbles.
10. Usa un buen antivirus y mantenlo actualizado. Es el mejor sistema de defensa corporativo contra ataques malintencionados que evitará en gran medida el acceso a nuestro sistema.
11. Realiza copias de seguridad de tus activos más importantes, de forma periódica, y comprueba que funcionan habitualmente.
12. Mantente informado y formado: conocer los riesgos que nos pueden afectar nos ayudará a adoptar medidas que de otro modo no tendríamos en cuenta.

VALORA INVERTIR EN LA ÚLTIMA LÍNEA DE LA DEFENSA: EL CIBERSEGURO



Aplica diariamente estas buenas prácticas e inclúyelas en la política interna de seguridad para los empleados y crea un compromiso corporativo con la seguridad de la información y la protección de datos. Estamos siendo atacados de forma continuada. Los ciberdelincuentes no descansan, los riesgos para la seguridad de la información y de nuestros datos están ahí y ya los conocemos, por lo que la mejor táctica será una buena defensa. Parafraseando a Vegecio, famoso escritor romano sobre temas militares, “Si quieres la paz prepárate para la guerra”.