GUÍA

OBLIGACIONES Y BUENAS PRÁCTICAS

PARA EL TRATAMIENTO DE DATOS PERSONALES

Cruz Roja Española

Índice

1 INTRODUCCIÓN:

Desde el 25 de mayo de 2018 se aplica el **Reglamento Europeo De Protección De Datos** y es importante el conocer cuáles son sus implicaciones.

Esta guía te ayudará a conocer la base jurídica para tratar los datos personales, los derechos de las personas y tus obligaciones y buenas prácticas a seguir por los usuarios que tratan datos de carácter personal a través de medios informatizados y/o en papel.

Se entiende la protección como el derecho de las personas en lo concerniente al tratamiento de sus datos personales: protección contra la posible utilización por terceros de forma no autorizada por el titular de los datos, así como impedir elaborar información que afecte a su entorno personal, social o profesional.

Es imperativo el conocimiento de esta buenas prácticas dirigidas al buen funcionamiento, utilización y explotación de los medios que tratan y soportan los datos de carácter personal, con el objetivo de disminuir los riesgos en cuanto a su explotación, transferencia a través de aplicaciones informáticas y redes de comunicación, así como de los medios que se emplean hoy en día para su almacenamiento y custodia.

El conocimiento de las obligaciones reflejadas en el presente documento y de las buenas prácticas a seguir está dirigido a garantizar la confidencialidad e integridad de los datos personales suministrados por los afectados y que son objeto de tratamiento por aquellos empleados, personas y proveedores que, en cumplimiento de sus deberes y compromisos, hagan uso de los mismos.

Asimismo, se trata de proporcionar pautas para la utilización de medios ajenos a Cruz Roja Española, como pueden ser redes sociales, blogs y aplicaciones de comunicación, a fin de evitar que pueda comprometerse el buen nombre de la Institución o poner en riesgo la seguridad de los datos personales y/o información confidencial que se encuentra bajo su responsabilidad.

2 OBLIGACIONES Y BUENAS PRÁCTICAS DE LOS USUARIOS

Los usuarios autorizados para el tratamiento de los datos protegidos son uno de los eslabones más débiles de la cadena de seguridad por diversas razones:

- Suelen ser el colectivo más numeroso de los que tienen contacto con los datos protegidos.
- No tienen, en su mayoría, una formación técnica.
- Muchas veces, no son suficientemente conscientes de su responsabilidad en la protección de los datos.

Por estos motivos son elegidos frecuentemente por usuarios malintencionados para realizar ataques a la confidencialidad o integridad de los datos o son protagonistas inconscientes de situaciones de riesgo para la seguridad de tales datos.

Este capítulo pretende abordar en un lenguaje sencillo, evitando términos excesivamente técnicos, las principales amenazas y riesgos para los datos protegidos, que pueden ocurrir a través de este colectivo autorizado al tratamiento de datos personales de Cruz Roja Española.

2.1 El puesto de trabajo

El lugar desde donde los usuarios autorizados acceden a los datos personales para el fin autorizado, es el puesto de trabajo.

Por lo tanto, el puesto de trabajo debe estar debidamente protegido contra intromisiones externas, tanto para salvaguardar la confidencialidad de los datos, evitando que puedan ser accedidos por personas no autorizadas, como para evitar una manipulación que atente contra la integridad o un acceso a los sistemas que provoquen su indisponibilidad.

Los usuarios deben ser responsables de que su puesto de trabajo cumpla esas condiciones, y, para ello, deberán tener en cuenta las siguientes

Recomendaciones:

- Las pantallas de los terminales u ordenadores personales no deberán ser visibles desde zonas de acceso público o por personal que no esté autorizado.

- Las impresoras compartidas no deberán estar ubicadas en zonas de acceso público y los documentos que se impriman y que contengan datos protegidos, deberán ser retirados tan pronto como sea posible.

- Los ordenadores personales deberán estar configurados de forma que quede bloqueado el acceso a los mismos tras un tiempo de inactividad y requieran de una nueva autenticación para desbloquearse (por ejemplo, un salvapantallas que se active después de un tiempo de inactividad y que necesite una clave personal para ser desactivado).

- Los documentos impresos con los que se esté trabajando y contengan datos personales o información sensible, deberán ser guardados bajo llave al final de cada jornada de trabajo.

- Se evitará guardar contraseñas en los cajones o, como ocurre frecuentemente, en pegatinas o post-it en el propio puesto de trabajo.

- El puesto de trabajo no debe tener más acceso remoto que el que esté autorizado a través de la red local de Cruz Roja, es decir, por ejemplo, está totalmente desaconsejado instalar módems telefónicos para el acceso directo al puesto de trabajo desde fuera de las instalaciones.

Esta práctica, que era muy utilizada hace años para acceder desde el hogar al propio puesto de trabajo (aunque en la actualidad ha caído en desuso), fue la causa de muchos accesos fraudulentos o ataques a la disponibilidad de los servidores.

- Los puestos de trabajo deberán estar ubicados en locales protegidos las 24 horas del día, para evitar el acceso a ellos por parte de personas no autorizadas.

Hay que tener en cuenta que los puestos de trabajo no son sólo un riesgo para la seguridad por los propios datos que pueden encontrarse almacenados en el mismo, sino también pueden convertirse en un lugar donde instalar subrepticiamente programas que husmeen la red local o las contraseñas que se teclean en el dispositivo de trabajo para acceder después a los servidores.
A veces, el acceso a un inofensivo puesto de trabajo puede convertirse en la cabeza de puente que permite realizar un ataque mucho mayor a los servidores de la organización.

2.1.1 Resumen de Recomendaciones sobre los puestos de trabajo

La protección física de los puestos de trabajo, así como la evitación de que se conviertan en cabezas de puente para un ataque a la Institución, es una condición vital para la seguridad.

Resumen de Recomendaciones

1. Los puestos de trabajo, pantallas e impresoras, deben estar protegidos de las miradas de personas no autorizadas.

2. No se deben mantener anotaciones sobre contraseñas u otros aspectos de la seguridad en la mesa de trabajo.

3. No se deben mantener copias de ficheros con datos protegidos, ya sea en cualquier soporte informático o papel, sin estar bajo llave.

4. No se debe instalar softwares no autorizados, dado el peligro de que contenga programas malignos, como sniffers o troyanos.

5. El puesto de trabajo no debe tener más acceso remoto que el que esté autorizado a través de la red local de Cruz Roja, siendo, además, dicho acceso remoto, debidamente autorizado por el Departamento de Sistemas.

2.2 El factor humano y las técnicas de engaño

Los datos protegidos deben ser manejados por los usuarios o por las personas que están autorizadas a hacerlo, de acuerdo con el objeto del fichero correspondiente. La experiencia ha demostrado en estos últimos años que, frecuentemente, han sido esas personas el eslabón débil de la cadena de seguridad de los datos.

La utilización de técnicas de engaño, por parte de personas que pretenden el acceso fraudulento a datos protegidos, basadas en la explotación de la ingenuidad o de la escasa concienciación de la necesidad de la protección de los datos por parte de los usuarios, ha sido una constante en la mayor parte de los ataques a la seguridad que se han realizado en los últimos tiempos.

La técnica utilizada es la siguiente:

- Mediante técnicas de engaño, como las que exponemos como ejemplo más adelante, se consigue una información, a veces aparentemente inocua, pero que permite el acceso al entorno protegido. Esa información puede ser, por ejemplo, una contraseña de un PC, una contraseña de dirección de correo o, incluso, alguna información personal sobre alguna persona clave de la Organización.

- Con la obtención y utilización de ese dato se planea un ataque de mayor alcance que, a su vez, permite conseguir otras informaciones o datos de mayor valor.

- Si se continúa con ese proceso, manteniendo oculta esa actividad, se consigue al fin tener acceso a los datos protegidos, aunque éstos se encuentren en un servidor.

Las técnicas de engaño explotan diversos puntos débiles que tiene el factor humano, así como la falta de concienciación sobre la importancia de la protección de los datos. Algunos ejemplos, como los que se mencionan a continuación, pueden ayudar a comprender cómo actúan los usuarios malintencionados.

Ejemplos

- Alguien, con voz decidida y apremiante, llama a un usuario autorizado y le dice que es un técnico del departamento central informático y que están confirmando las contraseñas de seguridad, por lo que le pide que le diga la suya para realizar esa comprobación. Este truco tan burdo, aunque resulte increíble, funciona.

- Una mujer, con voz de secretaria angustiada, llama al departamento central informático, diciendo que su jefe (puede citarse a algún gran jefe de la organización) está enfadadísimo porque en plena presentación delante de muchas personas importantes está haciendo el ridículo por no poder acceder a un sistema al haber olvidado su contraseña. Les urge a que se la den inmediatamente para que pueda continuar su presentación.

- Una persona con aspecto decidido y caracterizado adecuadamente, se presenta en un departamento haciéndose pasar por un técnico de *hardware* del departamento central que viene a revisar determinada instalación o servidor. El hecho de que conozca nombres o datos de personas de la organización puede ayudarle a tener más credibilidad.

- Se recibe un *email*, aparentemente proveniente del departamento central de informática, en el que se aduce una comprobación de seguridad y se conmina al usuario a teclear en un formulario sus contraseñas de seguridad. Naturalmente, este formulario es falso y sus datos son recogidos por el atacante. Este ejemplo de engaño es el que se conoce como ***phising*** en inglés.

Este método de engaño ha proliferado mucho en los últimos años, sobre todo, para obtener códigos de acceso a cuentas bancarias, pero la técnica puede ser utilizada igualmente para la obtención de datos protegidos en las organizaciones.

Estos ejemplos, puede ayudar a comprender el tipo de amenazas que supone la llamada "***ingeniería social***". Evidentemente, es imposible citar todas las posibles técnicas o engaños que se utilizan actualmente, ya que es innumerable y se encuentra en constante cambio, pero, en general, podemos sugerir las siguientes

Recomendaciones:

- Es importante que los usuarios sean conscientes de la importancia de mantener secretas sus contraseñas, incluso aunque sólo sirvan para acceder a su propio PC.

- No debe comunicarse nunca una contraseña por teléfono ni por correo electrónico. Como norma general, no se debe comunicar la contraseña de acceso a nadie, ni siquiera cuando procedan de los administradores o superiores, ya que, normalmente, dicha petición suele ser falsa. No existe razón alguna para que se hagan esas peticiones, por lo que, cuando se recibe una, puede asegurarse que es falsa.

- No deben comunicarse datos personales de usuarios del departamento a desconocidos o personas no acreditadas. A veces, el mero hecho de saber que determinado usuario va a tomarse las vacaciones en determinados días del año, puede ayudar a fraguar un engaño.

- El tratamiento correcto o la destrucción de los desechos informáticos como listados o borrado y debida protección de los soportes como pendrives, CD, etc., que se trata en otro capítulo, puede evitar la obtención de datos que, a su vez, permitan la ejecución de engaños.

2.2.1 Resumen de recomendaciones sobre las técnicas de engaño

Se ha comprobado que una forma frecuente de burlar las barreras tecnológicas de seguridad es acudir a técnicas de engaño basadas en el factor humano y la falta de compromiso de los usuarios con la seguridad de la información.

Resumen de Recomendaciones

1. NO DAR NUNCA LAS CONTRASEÑAS A NADIE POR TELÉFONO NI POR CUALQUIER OTRO MEDIO.

2. DESCONFIAR DE CUALQUIERA QUE, EN NOMBRE DE OTRO, NOS PIDA INFORMACIÓN INTERNA AUNQUE PAREZCA INOCUA.

2.3 Códigos y contraseñas de acceso

La introducción de un código y una contraseña asociada es, por el momento, la forma más generalizada de control del acceso a los sistemas de información. Aunque ya existen técnicas de control de acceso biométrico basadas en la detección de datos fisiológicos de los usuarios, como huellas dactilares, iris del ojo o reconocimiento de voz, todavía no están muy extendidas, siendo la utilización de contraseñas el medio de control de acceso más utilizado, aunque también van ganando terrero la confirmación de la identidad a través de tarjetas inteligentes y certificados electrónicos.

La utilización de contraseñas tiene un grave inconveniente, que es la dificultad que tiene la memoria humana para recordar aquellas que sean complicadas o no basadas en alguna regla nemotécnica. Esto conduce a la paradoja de que, si una contraseña es fácil de recordar para el usuario, será, a su vez, más fácil de averiguar por un atacante y, si es enrevesada y poco nemotécnica, se complica su averiguación por los atacantes, pero también será difícil de recordar por los usuarios.

Por tanto, existe una tendencia por parte de los usuarios a elegir contraseñas fácilmente recordables, sencillas, a veces, lugares comunes o, la mayoría de las veces, datos relacionadas con su entorno familiar. Asimismo, en el caso de que se fuerce a elegir contraseñas más complejas, es casi seguro que éstas se podrán encontrar anotadas en una pegatina en el cajón de su mesa de trabajo.

Recomendaciones sobre el uso y manejo de contraseñas:

- Las contraseñas deberán ser nemotécnicas, pero sólo para el propio usuario y no para el resto de la gente. Por ejemplo, las iniciales de las palabras de una frase utilizada en su casa pero que nadie conoce, el mote de algún amigo de juventud, etc. Nunca deben utilizarse datos personales que puedan ser conocidos por los demás, como la fecha de nacimiento, número de teléfono, nombre de los hijos, cónyuge, la novia o el novio o la mascota de turno.

- Además, esos datos nemotécnicos deben ser deformados de manera sencilla y aderezados con algún número también fácil de recordar.

- En general, la contraseña debe ser tan fácil de recordar o deducir para el usuario que no necesite anotarla en ningún papel para recordarla, insistiendo en este punto en que esa facilidad de deducción sea sólo para el usuario y no para terceros.

- Los propios sistemas informáticos deben forzar a los usuarios a:

  - Elegir contraseñas adecuadas, con una longitud mínima o que no se encuentren en los diccionarios de contraseñas usuales.
  - Cambiar la contraseña cada cierto tiempo (3 o 6 meses), así como impedir que se reutilicen contraseñas antiguas.

- Las contraseñas deben ser de uso personal. No deben ser compartidas en ningún caso, ni tampoco deben utilizarse contraseñas únicas para todo un grupo o departamento.

- Si un usuario sospecha que su contraseña ha podido ser accedida o conocida por alguien no autorizado, deberá ponerse en contacto inmediatamente con el departamento de sistemas para proceder al inmediato cambio de la misma.

- Si una persona abandona el departamento o la organización y deja de tener autorización para acceder a los datos protegidos, su contraseña deberá ser anulada inmediatamente para impedir su utilización.

2.3.1 Resumen de recomendaciones sobre uso de contraseñas

Resumen de Recomendaciones

1. **CONFIDENCIALIDAD DE LAS CONTRASEÑAS. LAS CONTRASEÑAS DE ACCESO SÓLO DEBEN SER USADAS Y CONOCIDAS POR LA PERSONAS PROPIETARIAS DE LAS MISMAS Y JAMÁS SER COMPARTIDAS CON NINGUNA PERSONA INTERNA O AJENA A LA ORGANIZACIÓN.**

2. ELEGIR CONTRASEÑAS FÁCILES DE RECORDAR POR UNO MISMO PERO DIFÍCILES DE DEDUCIR POR LOS DEMÁS.

3. NO ANOTAR LAS CONTRASEÑAS NUNCA EN PAPELES O RECORDATORIOS EN NUESTRA MESA DE TRABAJO.

4. CAMBIAR LAS CONTRASEÑAS PERIÓDICAMENTE. NO REPETIR LAS YA USADAS.

5. AVISAR AL DEPARTAMENTO CENTRAL EN CASO DE SOSPECHA DE QUE ALGUIEN HAYA PODIDO ACCEDER O CONOCER NUESTRA CONTRASEÑA.

2.4 Las redes locales

La mayoría, por no decir la totalidad, de los puestos de trabajo hoy en día, son ordenadores personales o PC, conectados a otros ordenadores personales mediante lo que se llama una Intranet o red de área local.

Las redes de área local permiten a los puestos de trabajo compartir recursos comunes, como almacenamiento en disco, impresoras o, lo que es más importante, servidores de aplicaciones. Además, permiten el acceso a otras redes más amplias, como Internet.

Esta capacidad de comunicación de las redes de área local supone un imprescindible instrumento de proceso y comunicación dentro de la Organización, pero, al mismo tiempo, puede también suponer una amenaza para la confidencialidad e integridad de la información y los datos protegidos.

2.4.1 **Los riesgos de las redes locales inalámbricas.**

Las redes inalámbricas de área local, también conocidas como *WLAN* o *WIFI*, se han convertido en objetivos de posibles ataques precisamente porque el tráfico enviado a través del aire puede ser accesible por terceros, incluso aunque no se encuentren físicamente ubicados en la casa u oficina, por tanto, este tipo de redes necesitan mecanismos adicionales para poder garantizar la seguridad. La única forma efectiva de prevenir que la transmisión de los datos no se vea comprometida es utilizando mecanismos de cifrado.

En una red local cableada un intruso debe acceder físicamente al cable o a un puesto de trabajo para "pinchar" la red. En una red inalámbrica, basta con que se coloque a una distancia cercana, aunque sea fuera del edificio protegido o del domicilio particular, para que tenga acceso físico a las señales. De hecho, cualquiera podemos comprobar que, desde nuestra casa, nuestra red WIFI detecta todas las de nuestros vecinos.

El cifrado de los datos no siempre es seguro, sino que depende del tipo de protocolo que se utilice para que sea más o menos robusto y dificultoso descifrarlos. De hecho, uno de los mayores robos de datos confidenciales de la historia se produjo en una cadena de supermercados de EE. UU., que utilizaba una red inalámbrica. Durante dos años, varios individuos no identificados estuvieron escuchando las conversaciones entre los dispositivos inalámbricos de mano utilizados por los empleados de un centro comercial de la firma Marshall en Minessotta y las cajas registradoras y ordenadores de la tienda. Los intrusos utilizaron una antena WIFI y un ordenador portátil ubicados fuera de los locales para hacerse con los datos personales y tarjetas de crédito de miles de clientes.
Este ataque se produjo al aprovechar una debilidad de uno de los protocolos de cifrado de las redes WIFI, el protocolo WEP. Hasta hace poco tiempo, este era el protocolo más utilizado por los módems inalámbricos, incluso en algunos modelos, el WEP era el único protocolo disponible.

Afortunadamente, existe otro protocolo, el WPA2, que no tiene esa debilidad y que ha venido protegiendo las comunicaciones WIFI durante la última década. Éste es el protocolo que se recomienda y que llevan incorporados los módems inalámbricos que se instalan en la actualidad.

Se espera, no obstante, que, para finales del 2019, se implemente un protocolo todavía más seguro, el WPA3, que fue presentado a primeros de año por la Wi-Fi Alliance, la organización sin ánimo de lucro que certifica los estándares de la red WIFI, como sucesor del WPA2 y que viene a reforzar aún más la seguridad, así como solventar los problemas de seguridad que se han detectado en éste último protocolo.

2.4.2 **Resumen de recomendaciones sobre redes locales**

Los peligros de las redes locales

Las redes locales, que facilitan el intercambio y la compartición de recursos, suponen un peligro si no se protegen y controlan adecuadamente ya que cualquier PC puede convertirse en una cabeza de puente para atacar a los servidores de la Organización u otros PCs.

Revisten especial peligrosidad las redes WIFI o inalámbricas, si éstas no están cifradas y no utilizan protocolos de cifrado robustos.

Resumen de Recomendaciones

1. **NO DEBEN INSTALARSE PROGRAMAS PERSONALES O NO AUTORIZADOS EN LOS DISPOSITIVOS DE TRABAJO.**

2. **CUALQUIER DISPOSITIVO HARDWARE O PROGRAMA SOFTWARE QUE SE INSTALE EN UN PUESTO DE TRABAJO DEBE ESTAR PREVIAMENTE AUTORIZADO POR EL DEPARTAMENTO DE SISTEMAS.**

3. **LOS USUARIOS DEBEN SER CONSCIENTES DE QUE SU PUESTO DE TRABAJO PUEDE SER UNA CABEZA DE PUENTE PARA ATAQUES AL RESTO DE LA RED O A LOS SERVIDORES DE LA ORGANIZACIÓN.**

4. **EN EL CASO DE REDES LOCALES INALÁMBRICAS UTILIZAR SIEMPRE CIFRADO Y PROTOCOLO WPA2, NO EL PROTOCOLO WEP QUE HA DEMOSTRADO SER FÁCILMENTE ATACABLE.**

2.5 Internet

Internet es una red global a nivel mundial que utiliza un único protocolo de transmisión (TCP/IP) y que engloba a centenares de miles de redes de área local y ordenadores individuales. Sobre esta red de transmisión global se han diseñado aplicaciones con protocolos propios universales, como el correo electrónico (protocolo SMTP), la aplicación *World Wide Web* (protocolo HTTP) y muchas más, cuyos protocolos se han estandarizado de facto y son utilizadas desde cualquier rincón del mundo.

La Red o Internet fue diseñada a finales de los años setenta, aunque su expansión a nivel mundial no se ha producido hasta mediados de los noventa. Los protocolos que actualmente se utilizan en Internet, como el SMTP para el correo electrónico, fueron diseñados hace más de 30 años.

Inicialmente, Internet fue un proyecto del Departamento de Defensa de EE. UU. para tener una red de comunicaciones segura en caso de enfrentamiento con la Unión Soviética. Es decir, en su diseño no se contaba con enemigos propios, ni se imaginaba que un día fuera una red mundial acechada por hackers, saboteadores o estafadores. Por eso su diseño adolece de muchos puntos débiles que, sin embargo, no es posible abordar eficientemente hoy en día, debido a que se han convertido en protocolos estándar a nivel mundial.

En muchos aspectos, sus protocolos de comunicación no son lo suficientemente robustos y seguros como para enfrentarse a todos los peligros de seguridad que existen en la actualidad.

Por ejemplo, es muy fácil en Internet suplantar la identidad de otro ordenador o la identidad de otro usuario de correo.

La propia estandarización de los protocolos y aplicaciones de Internet a nivel mundial se ha convertido en la principal amenaza para los datos ubicados en ordenadores conectados a Internet por los siguientes motivos:

- El número de posibles atacantes a los datos protegidos se incrementa considerablemente al estar un servidor conectado a Internet. Cualquier persona, desde cualquier lugar del mundo, puede llevar a cabo un ataque.

- Es posible automatizar la búsqueda de posibles servidores susceptibles de ser atacados y, también, automatizar esos ataques, de forma que, basta que un ordenador no esté suficientemente protegido para que sea detectado y atacado automáticamente desde cualquier lugar del mundo.

- Las motivaciones para un ataque que comprometa los datos de un servidor no siempre están relacionadas con el aprovechamiento de esos datos. En la mayoría de los casos, esas motivaciones son de tipo "deportivo", como un cazador que obtiene trofeos por las piezas que captura. Esto hace que el riesgo sea, por tanto, todavía mayor.

Hay dos tipos de conexión de ordenadores a Internet:

- Ordenadores conectados directamente a Internet a través de un proveedor de acceso a Internet, como los ordenadores caseros, que se conectan a través de un módem o líneas ADSL. También puede ser el caso de pequeñas organizaciones (por ejemplo, un pequeño Ayuntamiento) que no tienen red local y utilizan sólo uno o dos ordenadores personales.

- Ordenadores que están conectados a una red de área local que, a su vez, está conectada a Internet a través de un único punto de acceso. Es el caso de la mayoría de las organizaciones o departamentos. En este caso, en el punto de acceso único de toda la red local a Internet se suele colocar un programa, ordenador o conjunto de dispositivos que sirva de barrera para impedir la entrada de intrusos a la red local. Esta "barrera" se denomina "cortafuegos" o *firewall* en inglés.

2.5.1 **Ordenadores conectados directamente a Internet**

Son los más vulnerables, por lo que no se recomienda este tipo de conexión para ningún ordenador que contenga datos que deban ser protegidos.

Cuando un ordenador se conecta directamente a Internet, se convierte en un blanco visible desde cualquier lugar del mundo para ser atacado. Si bien es cierto que este tipo de conexiones suelen ser esporádicas, es decir, no están conectadas todo el día, aun así hay tiempo suficiente para que, en el caso de que nuestro ordenador tenga alguno de los fallos de seguridad usuales, sea detectado y atacado.

Los fallos de seguridad están relacionados con el *software* básico, es decir, con el sistema operativo o los programas de aplicaciones de Internet, como, por ejemplo, el Internet Explorer o el Outlook en el caso de Windows. Como son programas cada vez más complejos, suelen contener fallos de programación que son aprovechados por los atacantes. Cada semana se descubren nuevos fallos de seguridad que dan lugar a nuevas formas de ataque, que, a su vez, dan lugar a parches de seguridad que deben ser aplicados para evitarlas.

Aparte de los clásicos virus que pueden introducirse en el ordenador vía correo electrónico o, incluso, por el mero hecho de visitar una página web contaminada, el mayor peligro es que se nos instale subrepticiamente un programa de los llamados "troyanos". Este tipo de programas son capaces de conectar nuestro ordenador, sigilosamente y utilizando los propios protocolos de Internet, con el ordenador del atacante ubicado en cualquier lugar del mundo, transfiriéndole los datos que se deseen, como contraseñas, datos de nuestro disco duro, los tecleos en nuestro ordenador, etc. Por ello, es difícil mantener la seguridad en un ordenador directamente conectado a Internet.

Como norma general, deberemos mantener nuestro software permanentemente actualizado con los últimos parches de seguridad (algunos sistemas operativos, como Windows XP o 2000, lo hacen automáticamente), pero, en general, no debemos ubicar datos personales protegidos en ese tipo de ordenadores que vayan a conectarse directamente a Internet.

2.5.2 **Ordenadores en redes locales conectadas a Internet**

Es el caso más usual en organizaciones, incluso de pequeño tamaño. Lo más importante de este tipo de conexión es que los ordenadores no suelen estar directamente visibles desde el resto de Internet y son, por tanto, más difíciles de atacar.

La conexión a Internet de todos los ordenadores de una red local, incluso aunque sean centenares o miles, se realiza, a través de un único ordenador, al punto de acceso. En ese punto de acceso se instala también un ordenador intermediario (también llamado "proxy de red") y un sistema de barrera de entrada y filtrado de peticiones que intercepte posibles ataques ("cortafuegos" o *firewall*).

El mantenimiento y actualización del "cortafuegos" de una red local es responsabilidad del departamento central de seguridad de la organización. Los "cortafuegos" deben ser permanentemente actualizados para que detecten nuevas técnicas de ataque. Al igual que los antivirus, deben incorporar periódicamente nuevas actualizaciones.

La técnica que utiliza un "cortafuegos" es analizar todos los mensajes provenientes de Internet y dirigidos a cualquier ordenador de la red local, buscando indicios de un posible ataque malintencionado. En caso de que el mensaje sea sospechoso, se intercepta y se graba un aviso para el administrador de la red.

2.5.3 **Resumen de recomendaciones sobre Internet**

Conexión a Internet

Casi todos los ataques a servidores que se producen hoy en día tienen su origen en Internet. Internet hace que el número de posibles atacantes se haya disparado respecto a hace unos años. Además existen formas de automatizar los ataques, con lo que el riesgo es aún mayor.

Resumen de Recomendaciones

1. **NUNCA SE DEBE CONECTAR UN SERVIDOR O UN ORDENADOR DIRECTAMENTE A INTERNET.**

2. **CUALQUIER SERVIDOR O INCLUSO CUALQUIER ORDENADOR PERSONAL DE UNA ORGANIZACIÓN DEBE ESTAR EN UNA RED LOCAL PROTEGIDA Y AISLADA DE INTERNET MEDIANTE UN CORTAFUEGOS O "FIREWALL".**

2.6 El correo electrónico

El correo electrónico es, hoy en día, una de las principales vías de entrada a nuestros ordenadores personales de virus o programas dañinos que pueden afectar a la seguridad de los datos protegidos. Los tipos de amenazas que pueden acecharnos a través del correo electrónico son de diversos tipos, como se puede ver a continuación.

2.6.1 Los bulos (*hoaxes*)

Se trata de falsas noticias con apariencia real que se propagan a través de los correos electrónicos. A pesar de su apariencia inocua, pueden provocar colapsos de la red. Su técnica consiste en avisar de un peligro, más o menos real, y recomendar que se reenvíe ese aviso a todos los conocidos.
La malignidad de estos bulos radica, precisamente, en esos reenvíos masivos. Si cada persona que lo recibe lo reenvía, con su mejor intención, a 20 o 30 conocidos, se puede producir un efecto multiplicador que puede colapsar servidores y líneas. Como ejemplos, se podrían citar los siguientes bulos:

Ejemplos

- Aviso de nuevo virus que no es detectado por los antivirus.
- Carta de apoyo a cualquier causa humanitaria.
- Chistes o noticias graciosas o *links* a páginas chocantes.

Nunca, en ningún caso, deben realizarse reenvíos masivos de cualquier correo electrónico, aunque puedan parecer verídicos o, incluso, aunque lo sean. Se deberá reenviar el correo recibido sólo al administrador de seguridad de la red. Existe una base de datos a nivel mundial que recoge los bulos o hoaxes que se han detectado hasta la fecha.

2.6.2 **Correos trampa para obtener contraseñas (phishing)**

Son correos electrónicos que, en apariencia, provienen del servicio de seguridad de un banco y del propio departamento de seguridad de la organización. En ellos se indica que, para comprobar la seguridad de las contraseñas, se acceda a una página web, que, aparentemente, es la del departamento de seguridad, en donde un formulario pide que se tecleen de nuevo las contraseñas. De esta forma, los propietarios de esa falsa página web pueden capturarlas y utilizarlas para acceder a la información y los datos protegidos.


Por ello, en ningún caso se deben teclear las contraseñas en ningún formulario que no sea el oficial de entrada a los sistemas propios.

2.6.3 **Virus o programas malignos ("malware") anidados en correos electrónicos.**

La ejecución de cualquier programa anidado en un correo enviado por un desconocido, o incluso por un conocido, puede provocar la instalación en nuestro ordenador de un virus u otro programa maligno ("malware"), como un "troyano". De hecho, la mayor parte de los navegadores, como el Explorer de Windows, avisan de ese peligro cuando intentamos ejecutar un programa anidado en un correo. Lo que ocurre es que, a menudo, no damos importancia a esos avisos y, mecánicamente, damos orden de que se ejecute.

El software maligno puede distribuirse rápidamente en una red, infectando el equipo del usuario y distribuyéndose a sus contactos. Esto es debido a que el software maligno puede parecer que procede de un origen legítimo, y entonces es más probable que los usuarios lo cliquen o descarguen los programas.

El peligro es totalmente real y, además, frecuentemente, no producirá ningún resultado visible inmediato, ya que el programa que se instale subrepticiamente no delatará su presencia hasta que haya conseguido su objetivo más adelante.

Por ello, nunca se debe ejecutar un programa anidado o pinchar un enlace o visualizar un archivo adjunto a un correo electrónico, si no se está seguro de su procedencia. En general, si es un correo no relacionado con nuestro trabajo o de origen desconocido, no debe abrirse bajo ningún concepto. Además, se debe tener instalado un antivirus actualizado que pueda detectar posibles programas malignos que vayan a ser ejecutados.

2.6.4 **El peligro del correo basura ("Spam").**

El correo basura o *spam* se está convirtiendo en una plaga que amenaza hoy en día el funcionamiento de los servidores de correo y que puede llegar a paralizar el servicio o dificultarlo en gran medida.

Correo basura es todo aquel correo no demandado ni autorizado por el receptor, que, normalmente, consiste en anuncios de servicios y empresas sin escrúpulos que trabajan en Internet.

Cada día se mueven en el mundo miles de millones de esos correos no demandados, que inundan los buzones de los receptores y dificultan la llegada de los correos útiles y autorizados.

Cualquier dirección de correo que caiga en manos de estas empresas, especializadas en el envío de *spam* es, a su vez, revendida a otras empresas similares y así sucesivamente, por lo que, una vez que una dirección ha caído en sus manos, la recepción de correo *spam* diario se incrementa continuamente, pudiendo ser, incluso, centenares o miles los mensajes recibidos en esa dirección cada día, impidiendo la lectura de los correos deseados y sobrecargando el propio servidor de correo.

Una dirección de correo puede entrar en esas listas de víctimas por varias razones:

- Porque esa dirección aparezca en alguna página pública de Internet. Hay buscadores automáticas que detectan direcciones de correo en páginas HTML y las capturan.

- Porque la clave o password de esa dirección de correo sea débil, es decir, fácil de averiguar. Por ejemplo, que la clave sea el propio nombre de la dirección. En este caso, esa dirección de correos podría ser utilizada para reenviar *spam* a terceros.

- Que se haya dado la dirección y esa empresa la haya vendido en el mercado mundial de direcciones para correo basura.

Existen programas que analizan y detectan correo sospechoso de ser *spam*, tanto en los servidores como en los ordenadores personales. Son de mucha utilidad, ya que permiten eliminar un gran porcentaje del correo basura.

Un correo basura, además, puede ser portador de virus o "troyanos" o ser una trampa para obtener fraudulentamente claves de acceso u otra información. Por tanto, nunca se debe leer un correo sospechoso de ser spam y mucho menos ejecutar ningún enlace que lleve ni responder al supuesto emisor.

La práctica totalidad de los correos basura llevan direcciones falsas de remitente, aunque, aparentemente, puedan parecer reales, ya que aprovechan la facilidad del correo en Internet para aparecer con un alias, es decir, un nombre que no se corresponde con el propietario real de la dirección de correo.

Esta debilidad del protocolo SMTP de correo es utilizada por programas de correo basura para enviar correos no deseados que, aparentemente, provienen de un amigo, persona conocida o empresa públicamente conocida, con lo que incitan al receptor a no desconfiar y a leerlos.

2.6.5 Resumen de recomendaciones sobre correo electrónico

El correo electrónico un peligro para la seguridad

El correo electrónico es hoy en día la primera vía de acceso de programas malignos a nuestros ordenadores personales. Además, pueden ser un peligro para la disponibilidad de las redes globales a poder colapsarlas por su uso indebido.

Resumen de Recomendaciones

1. NUNCA EJECUTAR PROGRAMAS ADJUNTOS A CORREOS ELECTRÓNICOS DE DESCONOCIDOS.

2. NO SE DEBEN REALIZAR, EN NINGÚN CASO, REENVÍOS MASIVOS QUE PUEDAN PROVOCAR UN EFECTO CASCADA QUE COLAPSE LAS REDES.

3. REENVIAR, SÓLO AL RESPONSABLE DE SEGURIDAD, AQUELLOS CORREOS SOSPECHOSOS.

4. NUNCA ENVIAR DATOS CONFIDENCIALES O CONTRASEÑAS POR CORREO ELECTRÓNICO, A NO SER QUE VAYAN CIFRADOS.

5. CUIDAR LA PROPIA DIRECCIÓN DE CORREO PARA QUE NO CAIGA EN LISTAS DE CORREO BASURA.

2.7 Listados y desechos informáticos

La proliferación de la información, que es una consecuencia de la, cada vez mayor, potencia y capacidad de nuestros ordenadores, se está convirtiendo en un problema de seguridad que puede afectar a seguridad de los datos de carácter personal.

Nuestros ordenadores son tan potentes y tan capaces que "rebosan" información; y esa información acaba muchas veces en los contenedores o en los vertederos públicos al alcance de cualquiera que quiera aprovecharla.

La basura que generan nuestros ordenadores y que puede contener información confidencial puede ser de tres tipos: papel impreso, soportes de información como disquetes o discos ópticos, o discos fijos magnéticos encastrados en nuestros ordenadores obsoletos desechados. Los tres tipos son potencialmente peligrosos si no se eliminan con las precauciones necesarias.

2.7.1 **Listados e impresos**

Varios de los escándalos relacionados con la confidencialidad de datos personales ocurridos en nuestro país se han producido por depositar en la basura papel impreso que contenía datos confidenciales. Recordemos los listados recuperados en contenedores de un organismo oficial, o las fichas con comentarios xenófobos del departamento de personal de una cadena de supermercados.

No es fácil deshacerse de forma segura de los desechos de papel de nuestros ordenadores. Como recomendaciones generales podemos sugerir las siguientes:

Recomendaciones:

- Imprimir lo menos posible. Muchas veces imprimimos por vicio, por la comodidad efímera de tocar el documento y leerlo recostados en el sillón. La vida de muchos documentos puede y debe ser meramente electrónica. Se escribe en un ordenador, se envía por email a otro, se lee, y se archiva o se borra. Sin papel.

- En las empresas u organizaciones cuyo presupuesto lo permita, se debe tener una máquina destructora de documentos para eliminar, al menos, los documentos más confidenciales o que contengan datos personales.

- Exigir a las empresas de reciclado una garantía de destrucción de nuestros impresos, así como una garantía de custodia hasta su destrucción. Ya hay muchas compañías que ofrecen este tipo de contratos, como explicamos más adelante.

2.7.2 **Soportes removibles**

En un CD-ROM completamente lleno caben ¡200.000 folios! (600 Mb). Bien es cierto que no todos los CD están completamente llenos pero aún así, imaginemos la cantidad de información que puede ser tirada a la basura cuando desechamos uno de esos soportes. Y en los DVD la capacidad es mucho mayor.

En muchas ocasiones, además, este tipo de soportes son utilizados para realizar copias de seguridad. Y en éste caso los peligros son mucho más elevados, ya que en una copia de seguridad puede estar absolutamente toda la información relevante de nuestro ordenador.

El control de nuestros soportes removibles, comienza por su correcta identificación y etiquetado. Un CD o DVD sin etiquetar es una bomba de relojería que acabará en la basura a disposición de cualquier curioso.

Por último la recomendación obvia es la de borrar el contenido de aquellos soportes que reutilicemos o inutilizar los que tiremos a la basura. Pero destruir o inutilizar este tipo de soportes no es nada fácil.

Por eso lo recomendable es no tirarlos nunca a una papelera o a la basura, sino depositarlos en un contenedor a la espera de ser recogidos para su destrucción.

Existen destructores de documentos que son capaces de triturar soportes extraíbles. De todas formas, la mejor solución es recurrir a las empresas de destrucción de documentación para que procedan a su triturado y destrucción.

2.7.3 **Ordenadores obsoletos**

La llamada Ley de Moore establece que la potencia de los ordenadores se duplica cada 18 meses, y el *software*, cada vez más complejo y sofisticado, necesita de ordenadores adecuados para ejecutarse convenientemente. Lo cual nos lleva a un hecho, por otra parte muy celebrado por los fabricantes de hardware, y es que tenemos que cambiar de ordenadores cada dos o tres años como máximo.

El reciclado de ordenadores obsoletos se ha convertido ya en una pesadilla en muchos países desarrollados. Aparte de la lógica preocupación por la contaminación medioambiental, el hecho no sería preocupante para la confidencialidad de los datos sino fuera porque cada ordenador obsoleto lleva consigo, y de forma nada fácil de extraer o de borrar, un disco duro en el que pueden haber decenas de Gigabytes de información, es decir la información que habría en ¡decenas de millones de folios impresos!

¿Cómo destruir los datos de un disco duro? La destrucción de los datos de un disco duro no es en absoluto fácil. Existe una manera obvia de acabar con ellos, consiste en destruir físicamente el disco, pero es una tarea ardua, ya que hay que desmontar el disco, extraerlo del ordenador y acabar con él.

Se impone por tanto proceder a una limpieza de los discos, que destruya la información pero no inutilice el ordenador. Mucha gente piensa que para destruir los datos basta con borrar un archivo o un documento, mediante la orden de borrado de su sistema operativo (por ejemplo SUPR y vaciar papelera de reciclaje en Windows), o proceder al formateado del disco.

Hay que decir que estos procesos dejan intactos los datos ya que, lo único que hacen es eliminar los apuntadores que se dirigen a ellos y que permiten recuperarlos desde órdenes normales de nuestro sistema operativo, o, en el caso del formateado, rescribir las cabeceras físicas de los registros sin eliminar los datos. De esta forma, cualquiera con una cierta experiencia informática y, utilizando herramientas software adecuadas que existen en el mercado, puede acceder y recuperar la información.

La única forma más o menos segura de eliminar esa información consiste en rescribir todos los rincones del disco con información nueva. Existen en el mercado programas que sobrescriben los datos de nuestros discos desechados, utilizando técnicas seguras que impiden, incluso, su recuperación mediante los métodos descritos.

Por último, una recomendación que puede ser muy útil en cualquier caso y que minimiza el riesgo de que nuestros datos puedan ser recuperados de un disco desechado, es utilizar rutinariamente el cifrado para todos nuestros archivos confidenciales.

El cifrado de clave pública combinado con el cifrado simétrico, tal como lo utilizan muchos programas de seguridad, como, por ejemplo, PGP, o los propios sistemas operativos actuales, es sumamente seguro, fácil de usar y se ejecuta de forma inmediata.

2.7.4 **Empresas de destrucción de documentación confidencial**

Una buena práctica para deshacerse de forma segura de los desechos informáticos que puedan contener información confidencial, consiste en contratar a una empresa especializada en la destrucción de documentación confidencial.

Estas empresas, que son fáciles de encontrar a través de Internet o las mismas Páginas Amarillas, se comprometen por contrato a recoger y destruir la documentación, soportes, etc., que generemos. En el contrato se eligen las condiciones de seguridad que queremos que se apliquen a nuestros desechos.

Normalmente, las empresas proporcionan unos contenedores herméticos donde colocaremos todos los desechos, y que serán periódicamente recogidos y sustituidos por otros. Los contenedores son transportados en camiones cerrados al centro de destrucción de documentación de la empresa y allí son triturados y mezclados para impedir su reconstrucción.

2.7.5 **Resumen de recomendaciones sobre desechos informáticos**

Los subproductos del tratamiento informático de los datos, como son los listados desechados, soportes extraíbles o los propios ordenadores obsoletos, suponen un riesgo para la confidencialidad de los datos.

Resumen de Recomendaciones

1. **IMPRIMIR EN PAPEL SOLAMENTE LO IMPRESCINDIBLE.**

2. **NO TIRAR NUNCA A LA PAPELERA SOPORTES COMO PENDRIVES, DVD, DISQUETES O CDS.**

3. **CONTRATAR, PARA SU ELIMINACIÓN, A UNA EMPRESA DE DESTRUCCIÓN DE DOCUMENTACIÓN.**

4. **"SANITIZAR", ES DECIR ELIMINAR LOS DATOS DEL DISCO DURO DE AQUELLOS ORDENADORES OBSOLETOS QUE SE VAYAN A RETIRAR O DONAR.**

2.8 Ficheros de trabajo y temporales

Uno de los riesgos más frecuentes para la seguridad de los datos personales está relacionado con la facilidad con la que es posible copiar los datos en ficheros temporales o de trabajo, para realizar tratamientos temporales de los mismos.

Hoy en día los datos de cualquier aplicación informática, aunque estén ubicadas en servidores centrales, se muestran y son accedidos desde ordenadores personales. Una práctica muy usual, pero peligrosa desde el punto de vista de la seguridad, consiste en realizar copias de esos datos en archivos temporales del PC, para efectuar luego tratamientos propios, de cálculo o prospección, con los mismos, utilizando, por ejemplo, Hojas de Cálculo.

La copia de estos datos en ficheros temporales se puede realizar mediante procedimientos previamente establecidos e integrados que tienen algunas aplicaciones, o incluso simplemente copiando y pegando con el portapapeles de Windows.

El peligro para la seguridad proviene de que muchas veces esos ficheros "temporales" no son borrados al acabar su tratamiento, y permanecen y proliferan en el disco duro de los PC. Al no estar previstos en las normas de seguridad, éstos ficheros escapan a los controles correspondientes, convirtiéndose por tanto en una fuente de peligro para la confidencialidad de los datos protegidos.

Como recomendaciones básicas para disminuir estos riesgos podemos citar:

- Evitar en lo posible que las aplicaciones de tratamiento de datos personales permitan la transferencia a ficheros temporales. Es decir, que no contengan en su diseño ninguna opción para realizar esa transferencia automática desde el servidor a archivos temporales de los PC.

- Aun así, y como siempre se puede recurrir al "copiar y pegar", se deberá adoptar la norma de utilizar siempre ficheros en el directorio/temp del disco duro, y nunca en otro. Esto evitará la dispersión de esos ficheros peligrosos por todo el disco duro de nuestro PC.

- Al acabar el tratamiento local de los datos se deberán borrar todos los ficheros del directorio/temp del disco duro.

Otra posibilidad, para aquellos casos en que necesitemos, por razones de tratamiento, mantener copias temporales de datos protegidos en nuestros PCs, consiste en cifrar los ficheros. Para ello podemos utilizar herramientas de cifrado como las que describimos en el apartado correspondiente.

2.8.1 Resumen de recomendaciones sobre ficheros temporales

Uso de ficheros temporales

El uso de ficheros temporales para el tratamiento de datos protegidos mediante hojas de cálculo u otros programas, suponen un peligro para la seguridad, al escapar del control general al que se somete al fichero registrado.

Resumen de Recomendaciones

1. **EVITAR EN LO POSIBLE ESTOS TRATAMIENTOS PROVISIONALES NO PREDEFINIDOS EN LA APLICACIÓN.**

2. **SI NO HAY MÁS REMEDIO, O LA PROPIA APLICACIÓN LO PERMITE, UTILIZAR SIEMPRE UN MISMO FICHERO TEMPORAL (TEMP), PARA EVITAR LA PROLIFERACIÓN DE COPIAS EN EL DISCO DURO.**

3. **BORRAR SIEMPRE EL FICHERO TEMPORAL AL ACABAR UNA SESIÓN DE TRABAJO.**

2.9 Ordenadores y memorias portátiles

Otra amenaza para la seguridad de los datos confidenciales es la utilización de ordenadores portátiles y los dispositivos de almacenamiento tipo *pendrive* que permiten almacenar gran cantidad de información en un dispositivo minúsculo.

Es evidente la enorme utilidad de estos dispositivos portátiles, pero a la par es también evidente el del riesgo de pérdida, o robo que suponen, dada su portabilidad y reducido tamaño. Por eso es importante ser conscientes de este riesgo y adoptar medidas de seguridad que lo minimicen.

2.9.1 **Memorias pendrive o flash USB**

Hoy en día existen memorias *pendrive* USB de hasta 256 GBytes de memoria. Una capacidad equivalente a unos 512 de los primitivos CD-ROM. Es decir, en un minúsculo dispositivo de unos centímetros de longitud y algunos gramos de peso, caben 256.000 millones de caracteres! El equivalente a 200 millones de páginas impresas, o 500.000 libros de 400 páginas cada uno. Podemos imaginar la cantidad de información confidencial que puede contener unos de esos dispositivos, así como el desastre que podría suponer su pérdida accidental, o el robo de uno de esos dispositivos.

De hecho varios de los últimos episodios graves de pérdida de datos confidenciales han sido debidos a la pérdida o robo de algunos de esos dispositivos que contenían información confidencial.

El riesgo de un dispositivo de almacenamiento es proporcional a su capacidad de almacenamiento e inversamente proporcional a su tamaño. A mayor capacidad y menor tamaño, muchísimo mayor riesgo de pérdida o de robo.

Por eso es importante ser consciente del riesgo que representan estos dispositivos y adoptar las medidas adecuadas para minimizar dicho riesgo.

Como recomendaciones básicas para disminuir estos riesgos podemos citar:

- Evitar el uso de memorias *pendrive* para almacenar datos confidenciales. En el caso de hacerlo, borrarlos tras ser transferidos a otro ordenador o dispositivo.

- Tener siempre bajo control esos dispositivos. Dado su reducido tamaño es muy útil acoplarlos a una cinta que permita localizarlos y evite su pérdida. Todos ellos llevan un enganche adecuado para acoplar esas cintas.

Pero la recomendación más importante es la de cifrar los datos y archivos que se graben en esos dispositivos. Los datos grabados en un *pendrive* con los ficheros cifrados no podrán ser vistos por nadie que lo encuentre accidentalmente tras una pérdida o que lo haya robado deliberadamente.

Cabe decir que, actualmente, existen en el mercado pendrives que ya vienen cifrados de fábrica, por lo que toda la información que se introduce en el mismo, es protegida de forma automática, facilitándose así su seguridad.

Asimismo, es necesario destacar que esos dispositivos no son totalmente seguros para el almacenamiento permanente de información. Las memorias flash son muy sensibles a los campos electromagnéticos intensos y a otro tipo de interacciones externas que pueden alterar su contenido, por lo que su utilización sólo es recomendada para el almacenamiento temporal de datos. De hecho no se garantiza su recuperación pasados más de diez años, por lo que nunca deben ser utilizados para copias de respaldo a largo plazo.

2.9.2 **Ordenadores portátiles**

Todos los riesgos citados respecto a las memorias flash USB son, por supuesto, igualmente aplicables a los ordenadores portátiles. Un ordenador portátil puede tener mayor capacidad de almacenamiento que una memoria USB y, además, contiene no sólo archivos sino aplicaciones para el tratamiento de los datos.
Es por tanto un dispositivo de alto riesgo para la seguridad de la información confidencial y los datos personales.

Obviamente, el mayor riesgo de un ordenador portátil es su pérdida o su robo o sustracción. Por ese motivo, las recomendaciones son las mismas que para cualquier dispositivo de almacenamiento portátil de información: evitar en lo posible su uso para el almacenamiento permanente de datos confidenciales y cifrar su contenido.

Es un hecho cada vez es más frecuente el uso de ordenadores portátiles en empresas y organizaciones, incluso sustituyendo a los ordenadores fijos, de forma que se utilizan los mismos portátiles cuando se está en el puesto de trabajo, conectándolos a la red local mediante un puerto de acceso.

Por ese motivo es más importante aún la utilización de sistemas de bloqueo automático y contraseñas para su acceso, así como el cifrado de ficheros de forma rutinaria y no excepcional. La utilización de contraseñas de acceso y cifrado de ficheros eliminan o, en el peor de los casos, limitan los daños de una pérdida accidental o robo de un dispositivo u ordenador portátil, al impedir el acceso a los datos confidenciales contenidos en el mismo.

En casos extremos en los que existan datos confidenciales que sólo se encuentren grabados en un ordenador portátil perdido o sustraído, el problema no es solamente evitar que esos datos sean vistos por personas no autorizadas, sino conseguir su recuperación dado que no se tiene una réplica de los mismos.

Existen sistemas y productos que instalados en los ordenadores portátiles permiten ayudar a su localización y recuperación en caso de pérdida u sustracción. Muchos de ellos vienen ya instalados de serie en los modelos recientes. Todos se basan en la utilización de Internet (o incluso de la red GSM de telefonía).

De forma silenciosa, sin que el usuario no autorizado (es decir el que ha sustraído el PC) se entere, se conecta a un servidor de la compañía de seguridad, comunicando su dirección IP, o su localización vía GPS, mediante la que la policía, una vez advertida por la compañía, puede proceder a su localización y recuperación.

Otros sistemas proceden a la transmisión de los ficheros que se haya indicado a un servidor de respaldo en cuanto detectan que han sido robados o perdidos, así como su borrado de forma remota. Esa detección puede basarse en diferentes parámetros que se configuren como que haya pasado más de un cierto tiempo desde que se le ha tecleado una determinada contraseña, hasta que detecte haber sido transportado a más de X kilómetros de un determinado punto. Cada vez son más sofisticados los sistemas de detección y protección de portátiles y serán cada vez más útiles en el futuro, ya que la tendencia será la de su, cada vez, mayor proliferación.

2.9.3 Recomendaciones sobre ordenadores y memorias portátiles

Ordenadores y memorias portátiles

Las memorias y ordenadores portátiles han proliferado en los últimos tiempos y su uso es cada vez más extendido.

El riesgo de estos dispositivos es muy alto debido a su enorme capacidad de almacenamiento y su reducido tamaño.

Resumen de Recomendaciones

1. **EVITAR EN LO POSIBLE EL ALMACENAMIENTO PERMANENTE DE DATOS CONFIDENCIALES EN ESOS DISPOSITIVOS.**

2. **EN CASO DE TENER QUE HACERLO, BORRARLOS DESPUÉS DE HABER SIDO TRANSMITIDOS A OTRO ORDENADOR O DISPOSITIVO FIJO.**

3. **UTILIZAR EL CIFRADO AUTOMÁTICO DE FICHEROS PARA GRABAR DATOS PERSONALES EN ORDENADORES PORTÁTILES Y EN MEMORIAS PENDRIVE QUE NO VAYAN A SER COMPARTIDAS Y, EN LA MEDIDA DE LO POSIBLE, UTILIZAR PENDRIVES CIFRADOS. EN CASO DE PÉRDIDA O SUSTRACCIÓN LOS DATOS NO PODRÁN SER ACCEDIDOS.**

4. EN EL CASO DE ORDENADORES PORTÁTILES, UTILIZAR SISTEMAS DE BLOQUEO AUTOMÁTICO ASÍ COMO CONTRASEÑA PARA SU ACCESO. DEL MISMO MODO, CONVIENE INSTALAR Y CONTRATAR UN SERVICIO DE LOCALIZACIÓN PARA RECUPERAR EL DISPOSITIVO EN CASO DE PÉRDIDA O SUSTRACCIÓN, ASÍ COMO DE BORRADO REMOTO DE SU CONTENIDO.

2.10 Programas de cifrado y firma electrónica

El cifrado es una técnica que, aunque es muy compleja en su funcionamiento, es sumamente sencilla de utilizar mediante los programas especializados que existen en la actualidad.

El cifrado es sin duda una de las mejores herramientas con las que podemos contar en la actualidad para proteger la confidencialidad y la integridad de los datos personales.

Excepto en el caso de pequeños departamentos u organizaciones, se debe dejar en manos de los administradores informáticos la selección, contratación e instalación de un producto para la generación de claves, cifrado y firma electrónica.

Normalmente, estos productos, como PGP que fue uno de los pioneros, utilizan la criptografía de clave asimétrica o de clave pública y se integran automáticamente con los programas de correo (como Outlook), los manejadores de archivos (como Windows Explorer) e incluso los procesadores de texto, de forma que su uso es muy sencillo para los usuarios. Todos los sistemas operativos actuales llevan integrada la facilidad de generación de claves asimétricas y cifrado automático de ficheros.

Cada usuario tiene una frase secreta mediante la que esos productos de cifrado acceden a su clave privada, que está guardada en modo cifrado en los ordenadores donde trabaja ese usuario.

En muchos sistemas operativos como Windows, la clave de cifrado, que puede ser de centenares de bytes e imposible de memorizar, está protegida por la propia clave nemotécnica de acceso al ordenador. Es decir, está a disposición del usuario para cifrar ficheros o enviar *emails* firmados, desde el mismo momento en que se ha accedido con la clave correcta al ordenador.

Si se quiere cifrar un fichero basta con indicarlo cuando se crea. El fichero se descifrará automáticamente cuando accedamos a él, de forma que no notaremos ninguna diferencia con el acceso a un fichero no cifrado.

Si lo que se quiere es, por ejemplo, enviar un mensaje cifrado a otro usuario, del cual tenemos su clave pública, el propio programa de correo accede al directorio de claves públicas, recoge la de ese usuario y cifra el correo para él. De igual forma, si se recibe un correo cifrado para uno mismo, el propio programa de correo lo descifra automáticamente utilizando nuestra clave privada.

Si lo que se quiere es firmar digitalmente un correo, o un archivo, de forma que nadie pueda falsificarlo ni retocarlo y que además todo el mundo sepa que ha sido escrito por uno mismo, el producto de cifrado integrado en nuestro programa de correo o en el manejador de archivos nos pedirá nuestra frase secreta y accederá a nuestra clave privada para realizar el trabajo.

En resumen, el uso de programas de cifrado y firma electrónica es sumamente fácil para los usuarios, por lo que no se debe tener miedo a utilizarlos, eso sí, bajo la dirección del Departamento de Sistemas.

2.10.1 Resumen de Recomendaciones sobre cifrado y firma electrónica

Uso del cifrado y la firma electrónica

El uso del cifrado y la firma electrónica es sumamente fácil para los usuarios e incrementa la seguridad de los datos.

Resumen de Recomendaciones

1. **DEJAR QUE SEAN LOS ADMINISTRADORES INFORMÁTICOS (DEPARTAMENTO DE SISTEMAS) QUIENES SELECCIONEN, CONTRATEN E INSTALEN LOS PRODUCTOS DE CIFRADO Y FIRMA ELECTRÓNICA.**

2. **UTILIZAR DE FORMA SISTEMÁTICA EL CIFRADO Y LA FIRMA ELECTRÓNICA EN LOS CORREOS Y EN LOS DOCUMENTOS QUE CONTENGAN DATOS PROTEGIDOS DE CUALQUIER TIPO.**

2.11 Uso de antivirus

Los antivirus son programas especializados que se pueden instalar en nuestros ordenadores personales, en los servidores (especialmente de correo), o en ambos.

Su misión es localizar e interceptar cualquier programa maligno (virus, "troyano", gusanos de red, etc.) antes de que se instale en nuestros ordenadores y, además, realizar búsquedas masivas de programas malignos que hubieran podido instalarse en nuestros PC.

Normalmente son programas de pago pero, en el caso de organizaciones o empresas, son los departamentos centrales los que deciden qué programas antivirus se van a utilizar y efectúan su compra o acuerdo para su uso en toda la organización. En estos casos no se debe instalar un antivirus por nuestra cuenta sin consultar con el departamento central de Sistemas.

Hoy en día es prácticamente una insensatez trabajar en un ordenador que no esté protegido por un antivirus. La lucha contra los virus se ha hecho tan sofisticada que sólo puede ser abordada por programas altamente especializados.

Hasta hace pocos años, la única vía de acceso de los programas malignos (que entonces eran sólo los virus) eran los disquetes. Hoy en día, la principal vía de acceso es el correo electrónico, seguido del acceso a páginas webs, transferencia de ficheros por red y, por último, a través de la utilización de CD.

Los programas antivirus llevan consigo una base de datos de patrones de virus con los que son capaces de reconocerlos. Estas bases de datos deben ser permanentemente actualizadas ya que son decenas los nuevos virus que se crean y se distribuyen cada día. Normalmente, los propios programas antivirus se conectan a través de Internet a su sede central y actualizan diariamente su base de datos de patrones automáticamente. Un antivirus actualizado puede contener en su base de datos, hoy en día, los patrones de unos 50.000 virus y ese número va en aumento.

Los antivirus son capaces de interceptar cualquier entrada de datos a nuestro sistema, ya sea a través de correo electrónico, acceso remoto a ficheros, ejecución de un programa, acceso a una página web o entrada de datos por CD, y analizar su contenido para comprobar la existencia de programas malignos. También pueden actuar como "cortafuegos" vigilando el establecimiento de conexiones sospechosas que pudieran estar producidas por un "troyano" instalado en nuestro ordenador.

Además, los antivirus pueden ser programados para realizar exploraciones periódicas masivas de nuestros PC a fin de localizar y eliminar programas malignos.

2.11.1 **Resumen de recomendaciones sobre uso de antivirus**

El peligro de los virus y programas malignos

Los virus y programas malignos son uno de los principales peligros para la Disponibilidad, pero también para la Confidencialidad e Integridad de los datos, como en el caso de los programas Troyanos.

Resumen de Recomendaciones

1. TENER SIEMPRE UN PROGRAMA ANTIVIRUS INSTALADO EN NUESTRO ORDENADOR PERSONAL.

2. SI SE PERTENECE A UNA ORGANIZACIÓN, NO INSTALAR UN ANTIVIRUS POR NUESTRA CUENTA, SINO ATENERSE AL QUE SE HAYA ESTABLECIDO POR EL DEPARTAMENTO CENTRAL.

3. MANTENER SIEMPRE ACTUALIZADA LA BASE DE DATOS DE PATRONES DE NUESTRO ANTIVIRUS. UN ANTIVIRUS DESACTUALIZADO NO SIRVE PARA NADA.

4. UTILIZAR LA OPCIÓN DE EXPLORACIÓN PERIÓDICA DE NUESTRO ANTIVIRUS PARA DETECTAR PROGRAMAS MALIGNOS EN NUESTROS DISCOS DUROS.

2.12 Riesgos en el acceso a servicios Webs

Inicialmente, el lenguaje utilizado en las páginas webs de Internet era el Hiper Text Management Language o HTML. Este es un lenguaje especialmente diseñado para mostrar textos e imágenes con formatos atractivos y sobre todo permitir los enlaces o *links* con otras páginas, lo que se llama hipertexto.

Sin embargo, hace ya tiempo que las páginas web se han sofisticado y, aprovechando nuevas facilidades del HTML, han incluido llamadas a otros lenguajes y productos que permiten mayor vistosidad de los contenidos. Todos podemos apreciar cómo, al entrar en una página de cualquier periódico digital, los anuncios son cada vez más elaborados, incluyendo efectos audiovisuales de gran impacto. Todo esto no se realiza con el lenguaje HTML, sino que es el lenguaje HTML de la página quien llama a ejecución a pequeños programas en otros lenguajes que son los que realizan esos efectos. Ejemplos de estos programas y procesadores son el Flash, el Acrobat, o los programas applets en lenguaje Java.

El riesgo para la seguridad de nuestros datos al visitar páginas webs proviene de esos programas adicionales que se ejecutan en nuestros ordenadores.

Fallos de seguridad en los navegadores webs (como Internet Explorer, Firefox, etc.) pueden facilitar que un código malicioso anidado en esos pequeños programas, infiltre en nuestros ordenadores programas "troyanos" -llamados así por el famoso caballo de Troya- que transmitan subrepticiamente datos privados de nuestro sistema a otros servidores en Internet. Es, por tanto, muy importante asegurarse que el software y los productos adicionales que nos "bajamos" de Internet son los productos originales, certificados por el sitio web o compañía correspondiente y que están libres de código malicioso.

Para ello, los navegadores siempre nos piden autorización cada vez que intentamos "bajarnos" algún programa de Internet y nos recomiendan que nos aseguremos de la autenticidad de los mismos. La autenticidad de un sitio web puede ser garantizada mediante el mecanismo de la PKI, o infraestructura de clave pública, que garantiza que la página web accedida corresponde efectivamente a la empresa propietaria y no se trata de una falsificación. En cualquier caso, la recomendación debe ser evitar "bajar" productos cuando se tenga la más mínima duda sobre la autenticidad de los mismos.


Además, es muy recomendable instalar inmediatamente las actualizaciones automáticas que todos los nuevos navegadores obtienen de Internet para reparar "agujeros de seguridad" que se hayan detectado recientemente.

Otro mecanismo de navegación en páginas web que resulta ser polémico, son las llamadas *cookies*. Las *cookies* son pequeños archivos de texto que se almacenan en nuestro ordenador cuando visitamos algunos sitios web de Internet, donde se guardan algunos de los datos que hemos tecleado en esa visita, de forma que, la próxima vez que accedamos a ese sitio, el servidor pueda conocer nuestras preferencias anteriores y facilitarnos la navegación.

Las cookies son, por tanto, un mecanismo útil y que es utilizado por muchos sitios de Internet. Por ejemplo, una *cookie* pude contener cuál es nuestro idioma, cuál es el sistema operativo de nuestro ordenador, qué palabras clave hemos buscado últimamente en ese sitio web o la clave que hemos utilizado para entrar en él.


Es muy recomendable hacer periódicamente una limpieza del historial de navegación de nuestro navegador, lo que incluye limpiar las páginas visitadas, eliminar las cookies y archivos temporales, de forma que nadie que accediese a nuestro ordenador puede conocer los sitios visitados o nuestros hábitos.

Hay que resaltar que las *cookies* no contienen ningún dato que previamente nosotros no hayamos tecleado, que sólo se guardan en nuestro ordenador, que no contienen código ejecutable y, por lo tanto, son inofensivas desde el punto de vista de una posible "infección", así como que no pueden ser accedidas por otro servidor que no sea el que dio la orden de crearlas.

Todo esto nos da una idea de la baja peligrosidad de las *cookies* desde el punto de vista de la seguridad de la información. Sin embargo, es cierto que contienen datos personales sobre nuestra identidad o nuestras preferencias de navegación y que se graban sin que muchas personas sean conscientes de ello.


La Agencia Española de Protección de Datos en su "*Guía sobre el uso de las cookies*", recomienda que los sitios oficiales que manejen *cookies* lo adviertan mediante una leyenda en los términos de la normativa en materia de protección de datos (Según art. 22.2 LSSI) y permitan la elección de una navegación sin *cookies*.

2.12.1 **Resumen de recomendaciones para evitar riesgos en el acceso a los servicios Web.**

Riesgos en el acceso a servicios web

Las páginas web son cada vez más sofisticadas e incluyen la ejecución de programa y productos que pueden ser un riesgo para nuestros ordenadores.

Resumen de Recomendaciones

1. **ASEGURARSE DE LA AUTENTICIDAD DE LOS SITIOS QUE VISITAMOS Y DESDE DONDE NOS "BAJAMOS" PRODUCTOS ADICIONALES DE NUESTROS NAVEGADORES.**

2. **EN CASO DE DUDA, NO INSTALARLOS. EL PROPIO NAVEGADOR NOS AVISA DE LA DUDOSA AUTENTICIDAD DE UN SITIO AL ACCEDER A ÉL PARA BAJARNOS ALGÚN SOFTWARE.**

3. **INSTALAR INMEDIATAMENTE LAS ACTUALIZACIONES DE SEGURIDAD DE NUESTRO SISTEMA Y DE NUESTRO NAVEGADOR QUE SE HAYAN DETECTADO AUTOMÁTICAMENTE.**

4. **LIMPIAR PERIÓDICAMENTE EL HISTORIAL DE NAVEGACIÓN DE NUESTRO NAVEGADOR.**

2.13 Redes Sociales y Blogs.

Cuando hablamos de protección de datos personales estamos dando por supuesto que los propietarios titulares de esos datos o afectados quieren protegerlos del acceso no autorizado de terceros. Pero es precisamente el compartir sus datos personales lo que lleva a las personas a convertirse en usuarios de las redes sociales, lo que plantea nuevos retos para la protección de datos personales.

Los *blogs* (abreviatura inglesa de bitacora log o libro de bitácora) y las redes sociales, son dos fenómenos cuya razón de ser es precisamente la publicación de datos personales para que sean conocidos por un gran número de personas.

Aunque los *blogs* comenzaron por ser páginas de Internet en las que periodistas primero, famosos después, publicaban diariamente sus pensamientos u opiniones, lo cierto es que cualquiera puede publicar su propio *blog* y de hecho son muchas las personas desconocidas que mantienen su diario en la red. La publicación de opiniones puede ser más o menos inocua, pero el problema es cuando en esos *blogs* se publican datos personales propios o ajenos, de personas de su entorno, que pueden poner en peligro incluso la seguridad personal.

Lo mismo se puede aplicar a las redes sociales, o foros dedicados, como su nombre indica, a poner en comunicación a personas, para hacer amigos o establecer relaciones con otras personas e intercambiar noticias y archivos.

El problema es que muchas veces no se es consciente de los peligros que conlleva la publicación de datos personales en esas redes sociales.

Ejemplos

- Una vez publicado algo se pierde control sobre lo publicado. Nuestra publicación podrá ser copiada y difundida por millones de ordenadores.
- Aunque se pueda "borrar" o "modificar" lo ya publicado, sus copias podrán ya estar circulando sin nuestro control por Internet.

- El material, sobre todo fotográfico pero también audiovisual, que se publique puede ser manipulado o retocado y utilizado para fines espurios, incluso para chantajes.

2.13.1 **Recomendaciones generales para el uso responsable de redes sociales y Blogs.**

Las redes sociales, así como los foros, blogs y otros sistemas que facilitan la comunicación social en Internet, pueden ser un peligro para la seguridad y privacidad, si no son utilizados con precaución.

Recomendaciones

- Es conveniente utilizar alias para identificarse en los foros y redes sociales, evitando publicar datos personales como dirección, teléfono, o dirección de correo electrónico personal.

- Nunca publicar datos o fotografías de terceras personas sin su autorización.

- Hay que ser conscientes de que un dato publicado en Internet va a escapar de nuestro control, y no podrá ya ser modificado o cancelado.

- Cualquier mensaje o comentario enviado o publicado desde la dirección de un empleado, voluntario de Cruz Roja a una red social, grupo de noticias o foro, debe incluir una cláusula que precise que las opiniones ahí expresadas son sólo opiniones personales, y que no tiene por qué ser la opinión de Cruz Roja, salvo en el caso en el que la publicación forme parte de las actividades propias de la organización

2.13.2 **Buenas prácticas para la creación y gestión de cuentas profesionales en redes sociales y blogs.**

Es preciso tener en cuenta que el uso de redes sociales para fines profesionales o con fines publicitarios, promocionales y/o humanitarios no es equiparable a la de los usuarios que forman parte de ella actuando en un ámbito puramente personal o familiar, en tanto en cuanto, a éstos últimos, les resulta aplicable la llamada "*exención doméstica*" contenida en el artículo 2.1.c) del Reglamento General de Protección de Datos (Reglamento UE 2016/679, RGPD) según el cual "*El presente Reglamento no se aplica al tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*",

Tal y como señala la **Agencia Española de Protección de Datos (AEPD)** en numerosas resoluciones y el **Grupo de Trabajo del artículo 29** (órgano consultivo independiente de la UE sobre protección de los datos y la vida privada), en su **Dictamen 5/2009**, sobre redes sociales, si un usuario del servicio de redes sociales actúa en nombre de una empresa o asociación o utiliza la red, principalmente, como una plataforma con fines comerciales, políticos o sociales asume todas las obligaciones de un **responsable de datos** que está revelando datos personales a otro responsable de datos (el servicio de redes sociales) y a terceros (otros usuarios de Servicios de Redes Sociales). En estas circunstancias, el usuario necesita el consentimiento de las personas afectadas.

Por consiguiente, si se crea una cuenta o perfil en una red social en nombre de Cruz Roja Española, ésta, en calidad de responsable del tratamiento de datos, deberá asumir aquéllas obligaciones que el RGPD impone a éstos. Ahora bien, teniendo en cuenta que dicho tratamiento se efectúa en el marco de una determinada red social, en la que las reglas de funcionamiento y privacidad son impuestas por el proveedor de la red, algunas de estas obligaciones se limitan a aquéllos aspectos en los que el responsable sí tiene libertad para actuar, según ha establecido la AEPD.

Dentro de estas obligaciones figuran, en primer término, la información que debe proporcionarse a los usuarios sobre el tratamiento de sus datos personales, así como la obtención del consentimiento de las personas físicas.

Con carácter general, debe entenderse que el consentimiento en el ámbito de una red social se entenderá otorgado por el hecho de convertirse en "amigo" o "seguidor" de la página en cuestión. De este modo, deberá informarse por el titular de la página, a aquellos que pretendan convertirse en "amigos", de la finalidad o finalidades de la recogida de datos, y de la identidad y dirección del responsable, así como de la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación, oposición, limitación y olvido ante el mismo.

En cuanto a la forma en que debe proporcionarse dicha información, debe tomarse en consideración que el RGPD exige que se realice con carácter previo a la obtención del consentimiento, lo que implica que quienes deseen hacerse "amigos" de Cruz Roja Española en una red social, deberán conocerla antes de efectuar dicha acción. Una posible solución propuesta por la AEPD, sería ubicarla en el espacio de la cuenta que facilita la red social para introducir la información personal del titular de la página. Ello sin perjuicio de que dicha información se complemente con enlaces a la política de privacidad de la Web de Cruz Roja Española.

Asimismo, la gestión de contenidos en perfiles o páginas corporativas y la administración de las mismas deben atender los siguientes criterios, con la finalidad de generar información clara, oportuna, y acorde con las actividades y fines de Cruz Roja Española.

Criterios para la gestión de contenidos en perfiles o páginas corporativas:

- Sólo deberán ser publicados en las cuentas institucionales aquellos mensajes y contenidos que hagan referencia a las actividades de Cruz Roja Española u ofrezcan información sobre los programas y proyectos de la misma.
- Se deberá restringir la publicación de "comentarios a título personal" que puedan perjudicar la imagen pública y el buen nombre de la Institución y de su personal o que contradigan sus principios rectores y valores del movimiento internacional de Cruz Roja y la Media Luna Roja.
- Se debe igualmente impedir la publicación de cualquier tipo de dato personal o información relativa a personas físicas pertenecientes o ajenas a la Institución, sin el debido consentimiento de éstas.
- Se deberá evitar la publicación de información errónea, confusa, contradictoria o de fuentes no identificadas.
- No se podrá publicar información relativa decisiones deliberaciones de carácter interno y confidencial que tome Cruz Roja en el ejercicio de sus funciones.

- Podrán publicarse herramientas y aplicaciones que sirvan a los usuarios y seguidores para estar informados sobre las actividades, programas y proyectos de Cruz Roja y contribuyan a su expansión a través de las redes sociales.

2.13.3 Resumen de los criterios indispensables para la apertura de cuentas corporativas en redes sociales y blogs.

A continuación, exponemos un resumen de los criterios que deben seguirse para la apertura de cuentas en nombre de Cruz Roja Española en redes sociales y blogs.

Resumen de los criterios indispensables para la apertura de cuentas corporativas en redes sociales y blogs.

1. LAS CUENTAS DEBEN ESTAR SIEMPRE ASOCIADAS A CRUZ ROJA. NO SE PERMITE UTILIZAR EL LOGO, MARCA E IMAGEN DE CRUZ ROJA O LA MEDIA LUNA ROJA EN PERFILES Y CUENTAS PERSONALES EN LAS REDES SOCIALES.

2. EN EL APARTADO DE LA CUENTA DESTINADA A PROPORCIONAR LA INFORMACIÓN RELATIVA AL TITULAR DE LA CUENTA, SE DEBE INCLUIR LA INFORMACIÓN PERTINENTE SOBRE EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR PARTE DE CRUZ ROJA ESPAÑOLA, INCLUYENDO TAMBIÉN UN ENLACE A LA POLÍTICA DE PRIVACIDAD DE SU PÁGINA WEB: POLÍTICA DE PRIVACIDAD

3. SI LOS DATOS RECABADOS A TRAVÉS DE UNA RED SOCIAL VAN A SER INCORPORADOS A LAS BASES DE DATOS DE CRUZ ROJA O VAN A UTILIZARSE PARA CONTACTAR CON LOS USUARIOS FUERA DE LA RED SOCIAL, DICHOS TRATAMIENTOS DE DATOS EXCEDEN DEL ÁMBITO DE LA RED SOCIAL, POR LO QUE ES NECESARIO INFORMAR A LOS USUARIOS INCLUYENDO, EN SU CASO, CASILLAS INDEPENDIENTES PARA RECABAR EL CONSENTIMIENTO DE FORMA EXPRESA.

4. EL PERSONAL QUE PARTICIPE EN SOCIAL MEDIA (GESTIÓN DE REDES SOCIALES CON FINES CORPORATIVOS) DEBE CONOCER Y CUMPLIR LA "NORMATIVA INTERNA DE PROTECCIÓN DE DATOS PARA EL PERSONAL, VOLUNTARIOS Y COLABORADORES DE LA CRUZ ROJA ESPAÑOLA". HTTP://WWW.CRUZROJA.ES/NORMATIVA-SI/CR-NORMATIVA.HTML

5. ES PRECISO TENER ESPECIAL CUIDADO EN NO IMPORTAR NINGUNA LISTA DE CONTACTOS AL CREAR UNA PÁGINA EN UNA RED SOCIAL, YA QUE ENTONCES EXISTIRÍA UNA CESIÓN DE DATOS Y ÉSTA PODRÍA ACCEDER A LOS DATOS DE PERSONAS QUE NO SON USUARIOS REGISTRADOS DE LA MISMA.

6. SE DEBE NOMBRAR A UN ADMINISTRADOR Y RESPONSABLE DE LA PÁGINA (COMMUNITY MANAGER) QUE DEBE GESTIONAR EL PERFIL SOCIAL A TRAVÉS DE UN SISTEMA DE PERMISOS.

7. CRITERIOS PARA LA ASIGNACIÓN DE CLAVES DE ACCESO A LOS PERFILES: COMO MEDIDA PARA GARANTIZAR EL CONTROL DE ACCESO, ES INDISPENSABLE QUE LA DIRECCIÓN DE CORREO ELECTRÓNICO Y LA CONTRASEÑA PARA ACCEDER AL PERFIL SEAN FACILITADAS POR EL DEPARTAMENTO DE SISTEMAS.

8. CLAVES PARA CADA USUARIO: LAS CLAVES DE ACCESO DEBEN SER PERSONALES E INTRANSFERIBLES PARA CADA PERSONA QUE TENGA ACCESO Y GESTIONE LA CUENTA CORPORATIVA, DE ESTE MODO EVITAMOS (I) LA PÉRDIDA DE CLAVES Y FALTA DE CONTROL DE LAS CUENTAS (II) LA IMPOSIBILIDAD DE GESTIONAR PERFILES SI UNA PERSONA ABANDONA LA ORGANIZACIÓN.

2.14 Riesgos en el uso de la aplicación WhatsApp.

La utilización de WhatsApp en el ámbito profesional está absolutamente desaconsejada por las autoridades en materia de seguridad de la información y protección de datos.

Ello es debido a los fallos de seguridad que dicha aplicación presenta, así como al hecho de que vulnera la confidencialidad de la información.

2.14.1 Vulneración por WhatsApp de la normativa europea en materia de protección de datos.

Hay que tener en cuenta que, cuando utilizamos WhatsApp, estamos aceptando la política de privacidad impuesta por este servicio que tiene sus raíces en EEUU, país con un marco legal en materia de protección de datos y seguridad de la información muy diferente al de Europa.

Cabe decir que WhatsApp está siendo investigada por el tratamiento de los datos que ofrece y por la información que comparte, con fines publicitarios, con la aplicación Facebook. Dicha actuación y el consiguiente cambio en su política de privacidad, alarmaron a las autoridades europeas en materia de protección de datos.

Así, en España, la Agencia Española de Protección de Datos (AEPD), en fecha 2 de Marzo de 2018 y tras llevar a cabo una investigación que se inició dos años antes, ha sancionado a las entidades WhatsApp, INC y Facebook, INC al pago de una multa de 300.000€ cada una, por la infracción del art. 11 de la Ley Orgánica 15/1999, de Protección de Datos (LOPD), al considerar que la cesión de datos de sus clientes entre ambas entidades, derivada de su unión en el año 2014, se viene realizando sin el consentimiento de éstos y sin darles la oportunidad de oponerse a dicha cesión. (Procedimiento Sancionador **PS/00219/2017).**

En dicha resolución, la AEPD viene a afirmar que la política de seguridad de la aplicación no es lo suficientemente clara al respecto de la utilización de los datos de sus usuarios y su comunicación a Facebook, así como que la aceptación de dicha cesión se impone como obligatoria para poder hacer uso de la aplicación o para realizar su instalación en los dispositivos, en el caso de nuevos usuarios.


Por lo tanto, tenemos que tener claro, desde un principio, que, en el momento en que se utiliza el servicio de WhatsApp, perdemos el control, no solo de nuestros datos personales, sino de aquellos datos de contactos que se encuentren almacenados en nuestro dispositivo.

2.14.2 **Incumplimiento por WhatsApp de las medidas de seguridad para mantener la confidencialidad de las comunicaciones.**

Por otra parte, WhatsApp no cumple con las medidas de seguridad necesarias para mantener la confidencialidad de la información que se transmite a través de la aplicación. En este sentido el CNI, en el estudio denominado '*Riesgo de uso de WhatsApp*' viene a afirmar que esta plataforma se ha convertido en uno de los "*entornos más atractivos para intrusos y ciberatacantes*" en España. "*Desde sus inicios, los creadores de WhatsApp han descuidado algunos elementos básicos en cuanto a la protección de la aplicación y de los datos personales que se gestionan en esta aplicación*", denuncia también el CCN (Centro Criptológico Nacional), que apunta a una decena de agujeros graves de seguridad.

La "carencia más importante" de WhatsApp, según los especialistas del CNI, está en el "proceso de alta y verificación de los usuarios". Según el informe, la debilidad de la seguridad en este paso ha "*propiciado que los intrusos se puedan hacer con la cuenta de usuario de otra persona, leer los mensajes que reciba e incluso enviar mensajes en su nombre*".

La segunda falla detectada por los servicios de inteligencia del Ministerio de Defensa es el "***secuestro de cuentas*** *aprovechando fallos de la red*", en este caso la conocida como SS7. Las brechas de seguridad en esa red hacen factible que un atacante se haga pasar por un usuario y consiga sin demasiados problemas el código de verificación de WhatsApp, pudiendo así "secuestrar" la cuenta ajena. La situación es muy peliaguda: "*al tratarse de un fallo de red, y no de la aplicación en sí misma, no existe una forma directa de resolver estos fallos de seguridad*".

Igualmente preocupante para el CCN es el "***borrado inseguro de las conversaciones".*** El documento avisa que el uso de "técnicas forenses" hace inútil el borrado clásico de los mensajes, porque éstos continúan en la memoria del móvil hasta que son sobre-escritos y porque, tanto en Iphone como en Android, los textos quedan registrados, al hacerse las copias de seguridad. Los espías avisan que solo desinstalar la aplicación y borrar las copias de seguridad harán que desaparezcan las conversaciones.

También los responsables de la ciberseguridad nacional se muestran inquietos con la facilidad con que se puede "difundir" a extraños "información sensible durante la conexión inicial". Las nuevas codificaciones de estos datos –afirma el informe- no han comportado una "mejora sustancial de seguridad", que sigue siendo muy vulnerable a cualquier experto con una aplicación para desencriptarlas.

Igualmente vulnerable es la "base de datos" en la que WhatsApp almacena todas las conversaciones, con independencia de las 'nubes' y las memorias de los terminales. El tipo de memoria usada por la aplicación, llamada SQLite y el actual cifrado de esos mensajes (.crypt12) son pan comido para los 'piratas', según el CNI: "*Existen multitud de aplicaciones que permiten de una forma sencilla el descifrado de la información, tanto en una versión para un equipo, como a través de una aplicación en el teléfono o el interfaz de una web*", apunta el dossier.

Por todo lo expuesto, se debe restringir el uso de la herramienta WhatsApp a nivel corporativo y para las comunicaciones de Cruz Roja Española con sus voluntarios / socios, al asumir un elevadísimo riesgo en la confidencialidad y seguridad de la información compartida a través de la aplicación.

2.14.3 Creación de grupos en WhatsApp desde teléfonos corporativos.

Otro factor que determina que el uso de WhasApp a nivel corporativo esté restringido, es el elevado riesgo de sanción que conlleva la creación incontrolada de grupos en la aplicación, así como la incorporación de miembros a dichos grupos sin la debida diligencia y cumplimento de los deberes de información y recogida de consentimiento para el tratamiento de datos personales que impone la normativa actual.

En este sentido, la AEPD ha emitido varias resoluciones sancionando a entidades por incorporar usuarios a un grupo sin su autorización. En el ámbito doméstico no es preciso recabar el consentimiento, pero en el profesional sí, ya que se produce la cesión de datos personales (el nombre y número de teléfono) a los demás integrantes del grupo y se considera, además, que el dato se utiliza para una finalidad distinta para la que fue recabado por el responsable.

Así, la AEPD se ha pronunciado recientemente en el sentido de considerar que los grupos de WhatsApp creados desde números de teléfono profesionales o corporativos, con independencia de su finalidad, no pueden encuadrarse en el ámbito personal y, por tanto, amparase en la llamada "Excepción Doméstica" para eludir las obligaciones que impone la normativa en materia de protección de datos. Igualmente, se ha establecido que la responsabilidad de la creación de un grupo de WhatsApp recae sobre la persona física o jurídica titular del número de teléfono desde el que dicho grupo ha sido creado (Resoluciones **R/03041/2017 y R/03041/2017).**

Por lo tanto, la incorporación de una persona, perteneciente o ajena a la Institución, a un grupo de WhastApp creado desde un teléfono corporativo, sin que dicha persona haya sido debidamente informada de esta finalidad de tratamiento de sus datos personales y sin que haya consentido expresamente su inclusión en dicho grupo, constituye no sólo un tratamiento ilícito de dichos datos, sino también una cesión o comunicación no consentida de los mismos a los demás integrantes del grupo, recayendo la responsabilidad por ambas infracciones sobre Cruz Roja Española.

2.14.4 **Resumen de recomendaciones sobre WhatsApp.**

La aplicación WhatsApp no constituye un medio seguro de comunicación por lo que su utilización debe limitarse al ámbito personal y, en ningún caso, estar relacionado con las actividades desarrolladas en Cruz Roja Española.

Asimismo, no pueden crearse grupos de WhatsApp desde teléfonos corporativos puesto que ello representa un grave riesgo de incumplimiento de la normativa de protección de datos y, por lo tanto, de sanción para la Institución.

Resumen de Recomendaciones

1. **La utilización de la aplicación WhatsApp debe hacerse únicamente en el ámbito personal y nunca en el marco de las actividades de Cruz Roja Española.**

2. En ningún caso pueden transmitirse a través de este medio, datos referentes a Cruz Roja o información confidencial de la Institución o datos personales que se encuentren bajo su responsabilidad, ya que se infringiría el deber de secreto.

3. No se pueden crear grupos de WhatsApp desde un teléfono propiedad de Cruz Roja Española.

4. La creación de dichos grupos debe hacerse siempre desde teléfonos particulares y limitarse su utilización para cuestiones personales como envío de mensajes banales u organizar quedadas entre voluntarios/empleados. En estos casos, el responsable de la creación del grupo siempre será el administrador del mismo, por lo que deberá asegurarse, antes de incluir a una persona en el mencionado grupo, que la misma quiere ser incluida.

2.15 Desarrollo de aplicaciones (APPS) en el entorno de Cruz Roja Española.

El desarrollo de aplicaciones en el entorno corporativo de Cruz Roja Española, debe hacerse SIEMPRE dentro del marco controlado por la Institución y en coordinación y con la aprobación de Oficina Central.

No se deben crear Aplicaciones y apps móviles de forma irregular o incontrolada, ya que ello representaría una serie de graves riesgos para Cruz Roja, a saber:

- Incumplimiento de las normas de Privacidad y Seguridad en las aplicaciones y apps móviles.
- La aplicación como servicio de la Sociedad de la Información, debe igualmente ajustarse a lo establecido en la LSSI-CE.
- Registro de Marca y Nombre de la aplicación, así como el registro del dominio correspondiente, en su caso, o el diseño de un logo característico, deben hacerse siempre a nombre de Cruz Roja, al ser ésta la titular de la APP.
- Propiedad intelectual. Como programa informático o software, la aplicación se encuentra protegida por la Ley, debiendo regularse adecuadamente la protección y titularidad de los derechos de propiedad intelectual sobre la misma.
- Responsabilidad Penal de Cruz Roja Española (reforma Código penal LO 1/2015) ante cualquier violación de derechos de propiedad industrial/intelectual de terceros cometida por sus empleados.

Dichos riesgos vendrían derivados del "afloramiento "de programas y aplicaciones que estuvieran en uso en las delegaciones y centros de Cruz Roja, sin las debidas garantías de seguridad y legalidad, lo que los haría vulnerables a cualquier intrusión, con el consecuente riesgo de fuga de información.

Además, es preciso tener en cuenta que el RGPD incluye, ante cualquier nuevo tratamiento de datos personales que pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, en particular, si utiliza nuevas tecnologías, la obligatoriedad de llevar a cabo una **Evaluación de Impacto en la Protección de Datos Personales.**

Por lo tanto, La Oficina Central y, en particular, el Departamento de Protección de Datos de Cruz Roja Española, debe llevar a cabo una Evaluación de Impacto sobre la Privacidad de cualquier nueva aplicación o APP móvil que se desarrolle bajo su responsabilidad, emitiendo el correspondiente informe que acredite el cumplimiento de esta obligación.

2.15.1 **Resumen de recomendaciones sobre APPS.**

El desarrollo y creación de aplicaciones y apps móviles conlleva una serie de obligaciones y riesgos para Cruz Roja Española, tanto desde el punto de vista de la privacidad, como de la debida protección del software y los elementos a él vinculados.

Resumen de Recomendaciones

1. **NO DEBEN CREARSE O DESARROLLARSE APLICACIONES Y APPS MÓVILES SIN EL CONOCIMIENTO Y CONTROL DE OFICINA CENTRAL. CUALQUIER PROYECTO EN ESTE SENTIDO, DEBE SER COMUNICADO A OFICINA CENTRAL PARA SU COORDINACIÓN Y DIRECCIÓN POR EL DEPARTAMENTO DE SISTEMAS.**

2. **LAS IDEAS Y PROYECTOS DEBEN SER EVALUADAS PREVIAMENTE EN CUANTO A LOS RIESGOS QUE REPRESENTAN PARA LA PROTECCIÓN DE DATOS DE LOS DESTINATARIOS DE LAS MISMAS, ESTABLECIÉNDOSE LAS MEDIDAS OPORTUNAS PARA LA ELIMINACIÓN O MITIGACIÓN DE DICHOS RIESGOS.**

3. **UNA VEZ EVALUADA LA IDONEIDAD Y VIABILIDAD DE LAS APLICACIONES, ÉSTAS DEBEN INCARDINARSE DENTRO DE LOS ESTÁNDARES DE LOS SISTEMAS DE INFORMACIÓN DE CRUZ ROJA ESPAÑOLA, EN CUANTO A SU SEGURIDAD, RENDIMIENTO Y DISPONIBILIDAD.**

3 OBLIGACIONES Y BUENAS PRÁCTICAS DE LOS USUARIOS DE FICHEROS MANUALES

3.1 Los ficheros manuales

Los riesgos y amenazas en el caso de los ficheros manuales son menos numerosos, menos complejos y menos sofisticados que en el caso de los ficheros automatizados o informatizados, pero no por ello menos importantes.

Básicamente, son tres las áreas en las que se deben centrar los buenos hábitos o prácticas de los usuarios de ficheros manuales: la organización del fichero o sus criterios de archivo, la salvaguarda física de los soportes y la destrucción de las copias o soportes desechados.

3.2 Criterios de Archivo

Para que un conjunto de datos de carácter personal sea considerado un fichero manual conforme al RGPD, deberá estar organizado conforme a criterios determinados relativos a personas físicas que permitan acceder, sin esfuerzo desproporcionado, a sus datos personales.

Un criterio de archivo es el método utilizado para la localización y acceso a los datos. Todo fichero manual debe tener un criterio de archivo determinado.

Ejemplos de criterios de archivo:

- Ordenar los documentos en archivadores o carpetas por orden alfabético del nombre de los sujetos. Si una carpeta tuviese que contener soportes físicos de datos (por ejemplo, cintas de audio o video) que no cupiesen físicamente en esa carpeta, se almacenarán esos soportes en estanterías separadas y se indicará en la carpeta la localización del soporte en la estantería.
- Ordenar los documentos por orden cronológico de entrada o dentro de carpetas clasificadas por DNI de los individuos.

De esta forma, el criterio de archivo de un fichero manual deberá garantizar, al menos:

- La fácil localización de toda la información relativa a una persona mediante algún dato identificativo de la misma, como nombre y apellidos, DNI, etc., u otros datos que, aunque no identifiquen unívocamente, permitan recuperar un número reducido de expedientes en los que se pueda buscar secuencialmente de forma rápida.

- La fácil sustitución, modificación o destrucción de todos los datos referentes a una persona. Esta condición es necesaria para poder ejecutar los derechos de rectificación y cancelación. Para que sea posible esta sustitución, modificación o cancelación, es necesario que los datos pertenecientes a cada persona estén grabados en soportes independientes y fácilmente sustituibles o modificables.

  Un ejemplo de un archivo que no cumpliría esta condición sería un libro de hojas no removibles en donde fueran escribiéndose datos de múltiples personas. En ese caso, no sería posible sustituir o destruir los datos de una persona sin afectar a todo el libro o, al menos, a los datos de otras personas incluidos en el archivo. Otro ejemplo podría ser la mezcla en una única cinta de audio o video de varias grabaciones correspondientes a varias personas.

También es conveniente el mantenimiento de criterios de archivo redundantes que permitan identificar que falta un documento o que existe un documento indebidamente insertado. Esto se puede hacer manteniendo un índice de documentación, en soporte separado, de forma que, si se extravía o se extrae indebidamente una carpeta, se pueda detectar, o que se pueda también detectar una adición fraudulenta de una carpeta o soporte.

Archivo de datos históricos disociados. En algunos casos, y cuando ha pasado un tiempo determinado, muchos datos de un fichero manual pueden ser destruidos o pueden pasar a un fichero histórico por razones de diversa índole, como estadísticas, epidemiológicas, etc. En estos casos, se deberán disociar estos datos, es decir, se deben eliminar todos aquellos datos que puedan identificar unívocamente a las personas y mantener solamente los datos genéricos válidos a esos efectos.

3.3 Salvaguarda física del fichero manual

Los soportes físicos deberán guardarse en contenedores apropiados, archivos o armarios con dispositivos que obstaculicen su apertura. Cuando no sea posible, se adoptarán medidas para impedir el acceso a personas no autorizadas.

Del mismo modo, todos los soportes físicos de un fichero manual que contenga datos personales especialmente protegidos (datos de salud, violencia de género, religión, creencias, origen racial, vida sexual etc..), deberán ser guardados en locales especialmente protegidos, mediante puertas dotadas de sistemas de apertura con llave, código de acceso o vigilancia permanente.

Estos locales protegidos deberán tener garantizado el acceso del personal de seguridad o emergencias, como policía o bomberos, para que, en caso de emergencia, puedan poner a salvo los soportes.

Otro tipo de empleados, no relacionados con el fichero, como pueden ser el personal de limpieza o mantenimiento, sólo deberán poder acceder a los locales, para cumplir sus funciones, durante los horarios normales de trabajo.

3.4 Manejo y destrucción de documentos y soportes

Cualquier copia de soportes del fichero, como fotocopia de documentos, duplicación de cintas de video o audio o de cualquier otro tipo, deberá estar autorizada por el responsable del fichero o persona delegada.

Dada la facilidad con que hoy en día es posible realizar copias de archivos y soportes de cualquier tipo, ya sea documentación en papel o en soportes electrónicos, debe imponerse la disciplina de no realizar esas copias más que en casos absolutamente imprescindibles.

Recomendaciones:

- Deberá habilitarse un procedimiento para controlar el uso y destrucción posterior de estas copias de archivos y soportes. Se recomienda el uso de destructores de documentación o la contratación de una empresa destructora de residuos que garantice por contrato la destrucción de los soportes, de forma similar a las recomendaciones de las buenas prácticas de los ficheros automatizados.

- De igual modo se recomienda que sólo se conserve en papel la documentación estrictamente necesaria, debiendo adoptarse la costumbre de escanear los documentos y almacenarlos informáticamente en los Sistemas de Cruz Roja, dotados de las medidas adecuadas de seguridad (sin olvidar la eliminación del fichero temporal creado con motivo del escaneado, una vez se ha ubicado el archivo en el expediente informático).