- Cada vez que se **visita** un **sitio web**, se **suministra** de forma rutinaria una **información** que puede ser **archivada** por el **administrador** del sitio.
- Al **sitio web** le resulta **trivial averiguar** la **dirección** de **Internet** de la [1]**máquina** desde la que se está accediendo, [2]**sistema operativo**, etc.
- Con ayuda de las "**cookies**" se puede **personalizar** aún más la **información** recabada acerca de los **visitantes**, **registrando** las **páginas más visitadas**, **preferencias**, **tiempo** de la visita, **software instalado**, etc.
- Un **navegador web**, en favor de la máxima usabilidad, **permite** que se **acceda** a **información** aparentemente **inofensiva**.
- La **dirección IP pública** con que se **conecta** el **usuario**.
  - Tu **dirección IP** es **xxx.xxx.xxx.xxx**.
  - Tu **navegador** está **utilizando 128 bits** de **clave secreta SSL**.
  - El **servidor** está **utilizando 1024 bits** de **clave pública SSL**.
- La **resolución** de la **pantalla**.
- Qué **páginas** se **leen** y cuáles no, qué **figuras** se **miran**, cuántas **páginas** se han **visitado**, cuál fue el **sitio** recientemente **visitado**.
- El **valor** del **campo** "**User-Agent**".
- El **idioma** y **zona GMT*** del **sistema operativo**.
- Si se **aceptan** o **no** "**cookies**".

Algunas **recomendaciones** para mantener una **navegación segura** son:

- **Acceder** únicamente a **sitios** de **confianza**.
- **Mantener actualizado** el **navegador** a la última versión disponible del fabricante.
- **Configurar** el **nivel** de **seguridad** del navegador **según** sus **preferencias**.
- **Descargar** los **programas** desde **sitios oficiales** para **evitar suplantaciones maliciosas**.
- **Configurar** el **navegador** para **evitar ventanas emergentes**.
- **Utilizar** un **usuario sin permisos** de "**Administrador**" para navegar por Internet e **impedir** la **instalación** de **programas** y **cambios** en los **valores** del **sistema**.
- **Borrar** las "**cookies**", los **ficheros temporales** y el **historial** cuando se **utilicen equipos ajenos** para **no dejar rastro** de la **navegación**.
- **Desactivar** la posibilidad "**script**" en navegadores web.
- En la medida de lo posible, **emplear máquinas virtuales** para **navegar** por **Internet**.

Además, hay que tener en cuenta que los **sistemas** de **navegación anónima permiten** el **uso** de algunos servicios de **Internet** de forma **desvinculada** de la **dirección IP origen** de la comunicación.

- **Anonimizadores**: actúan como un **filtro** entre el **navegador** y **sitio web** que se desea visitar o al conectarse al anonimizador, se **introduce** la **URL** a **visitar** y entonces éste **se adentra** en la **red filtrando cookies**, **javascripts**, etc.
- **Servidores Proxy**: actúa de **pasarela** entre la **máquina cliente** e **Internet**, actúa de **intermediario**, se encarga de **recuperar** las **páginas web en lugar** del **usuario** que navega.
- **Túneles de Cifrado** (TOR): por las cuales los **datos de navegación**, debidamente **cifrados**, **atraviesan múltiples nodos hasta** llegar a su **destino**.

Correo electrónico (Nº 7)

Actualmente el **correo electrónico** sigue siendo una de las **herramientas más utilizadas** por cualquier entorno corporativo para el **intercambio** de **información** a pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros.

El **incremento** y **efectividad** de la **ingeniería social** para **engañar** a los **usuarios** por medio de **correos electrónicos** ha **modificado** el paradigma de la **seguridad corporativa**.

Actualmente los **cortafuegos perimetrales*** y la **securización** de los **servicios** expuestos a **Internet no** son **contramedidas suficientes** para **proteger** una organización de **ataques externos**.

Algunas **recomendaciones** para utilizar el **correo electrónico** de forma segura:

- **No abrir** ningún **enlace ni descargar** ningún **fichero adjunto** procedente de un **correo** electrónico que presente cualquier **indicio** o **patrón fuera** de lo **habitual**.
- **No confiar** únicamente en el **nombre** del **remitente**. El **usuario** deberá **comprobar** que el propio **dominio** del **correo** recibido es de confianza.
- **Antes** de **abrir** cualquier **fichero descargado** desde el **correo**, hay que **asegurarse** de la **extensión** y **no fiarse** del **icono** asociado al mismo.
- **No** hacer **clic** en ningún **enlace** que **solicite datos personales** o **bancarios**.
- **Tener** siempre **actualizado** el **sistema operativo**, las **aplicaciones ofimáticas** y el **navegador**.
- **Utilizar herramientas de seguridad** para mitigar virus de manera **complementaria** al software **antivirus**.
- **Evitar** hacer **clic** directamente en cualquier **enlace** desde el propio cliente de **correo**.
- **Utilizar contraseñas robustas** para el acceso al correo electrónico. Las contraseñas deberán ser **periódicamente renovadas** y si es posible utilizar **doble autenticación**.
- **Cifrar** los **mensajes** de **correo** que contengan **información sensible**.

Virtualización (Nº 8)

La **virtualización** es la **recreación** de un **recurso físico** (hardware) o **lógico** (software), por **medio** de un **hipervisor*** que **permite** su **ejecución** por **más** de un **entorno** al **mismo tiempo**.

En el entorno de **máquinas virtuales**, el **hipervisor** permite el **uso simultáneo** del **hardware** en **más** de un **sistema operativo**.

El **apogeo** de la **virtualización** ha llegado con la **utilización** de la **nube**, donde este **sistema** de **reparto** de los **recursos** se hace casi **indispensable**.

La **seguridad** en la **virtualización** tiene la misma premisa que cualquier otro sistema, que es la **minimización** de la **superficie** de **ataque**.

Como norma general, es conveniente **seguir** las siguientes **indicaciones** a la hora de **configurar** un **host*** de máquinas virtuales:

- **Tener instaladas** en el sistema operativo las **últimas actualizaciones de seguridad**.
- **Tener** la **última reversión disponible** del programa de virtualización.
- Si es posible, **tener** al menos **1 adaptador de red** en exclusiva para la infraestructura de virtualización.
- **Crear** un **entorno** de **laboratorio aislado** del entorno de producción.
- **Disponer** de un **grupo de seguridad** para gestionar la plataforma de seguridad.
- **Proteger** los **dispositivos de almacenamiento** en los que guardan los archivos de recursos y de definición de la máquina virtual.

- **Mantener estancos** a los **administradores** de los **guest*** **respecto** a los de **host**.

Para la **creación** de **guest**, se recomienda seguir las siguientes **normas**:

- **Hacer** un **esquema previo** de lo que será la **infraestructura** de **virtualización**.
- **Dimensionar** la creación de **máquinas virtuales** a las **necesidades** reales y a los recursos de **hardware** disponibles en el host.
- **Cifrar** los **ficheros** de **máquinas virtuales**, **instantáneas** y **discos duros virtuales** destinados al **almacenamiento** de la plataforma de virtualización.
- **Instalar** las **últimas actualizaciones de seguridad** en cada sistema operativo guest.
- **Valorar** la **instalación** de los **agentes de hipervisor**, tipo **Guest Additions**, y en caso de hacerlo, mantenerlos **actualizados**.
- **Asegurar** con **antimalware** y **firewalls** todos los sistemas operativos invitados.
- **Conectar DVD**, **CD** y **medios de almacenamiento externos solo** cuando sea **necesario** y **desactivar** tras su uso.
- **Mantener activas** solamente las **máquinas virtuales imprescindibles**.
- **Usar** para la **conexión** con la **red corporativa** o con **Internet** una **interfaz** de **red virtual diferenciada** que se deberá **desactivar** cuando **no** se vaya a **utilizar**.
- **Cifrar** los medios de **almacenamiento externos** que contengan **ficheros de virtualización de respaldo** y custodiarlos convenientemente.

Seguridad en dispositivos móviles y redes inalámbricas (Nº 9)

El **incremento** de **posibilidades** y **capacidades** que llevan asociados los **dispositivos móviles** en la actualidad **implica** igualmente **mayores riesgos** para la **seguridad** de los mismos.

Se deben tener en cuenta los siguientes **aspectos** a la hora de usar **dispositivos móviles** para **garantizar** la **seguridad**:

- **Establecer** un **método seguro** para **desbloquear** el **terminal**.
- Es recomendable **eliminar** las **previsualizaciones** de los **mensajes** y extremar las **medidas** cuando **no** se disponga del **teléfono al alcance**.
- **Deshabilitar** las **conexiones inalámbricas** (WiFi, Bluetooth, etc.) y todas aquellas innecesarias mientras **no** vayan a **utilizarse**.
- Mantener **actualizado** el **software** del dispositivo y **utilizar** una **configuración de seguridad aprobada** por el **responsable TIC** de la entidad.
- Tener **cuidado** con el **acceso** y las **solicitudes de permisos** de las **aplicaciones** que se ejecuten en el **teléfono**.
- **Ignorar** y **borrar mensajes** (SMS, MMS u otros) de **origen desconocido** que invitan a descargar contenidos o acceder a sitios web.
- **Activar** el **acceso** mediante **PIN** a las conexiones **Bluetooth** y configurar el **dispositivo** en **modo oculto**. **No aceptar conexiones** de **dispositivos no conocidos**.
- **Descargar aplicaciones** únicamente desde las **tiendas oficiales**. **En ningún caso**, descargar software de sitios **poco fiables** y en todo caso **solicitar** al **responsable TIC** de la entidad las **aplicaciones necesarias**.
- **Utilizar** una **red privada virtual** (VPN16) para **proteger** el **tráfico de datos** desde el **dispositivo** móvil **hasta** la infraestructura de la **entidad**. Siempre es una buena práctica para **evitar** la posible **monitorización*** por parte de intrusos.
- **Evitar** en lo posible el **uso** de **impresoras**, **faxes** o **redes WiFi públicas**, como las ofrecidas en hoteles o aeropuertos, **salvo** que se disponga de las **herramientas** necesarias para **asegurar** sus **comunicaciones**.
- **Limitar** la **compartición** de las **imágenes** en la **red** o bien **utilizar aplicaciones** que **eliminen** dicha **información**.

- **Separar** las **comunicaciones personales** de las **profesionales** es una buena práctica de seguridad.
- **Implementar** la **gestión centralizada** de dispositivos **móviles** mediante el **empleo** de **agentes MDM** (Mobile Device Management)*.
- Para manejar información sensible, **utilizar** únicamente **soluciones aprobadas** por el **responsable** de **seguridad TIC** de la entidad.

Seguridad en redes inalámbricas (Nº 10)

Si se **trabaja** con una **red inalámbrica**, para **maximizar** la **seguridad** en la red **WiFi** es necesario prestar atención a las **siguientes recomendaciones**:

- **Cambiar** la **contraseña** de **acceso** por **defecto** para la administración del Punto de Acceso.
- **Modificar** el **SSID*** **configurado** por **defecto no** empleando **nombres** que pudieran **identificar** a la **entidad** y que permitan pasar **desapercibidos** con el entorno.
- **Ocultar** el identificador **SSID** al **exterior dificulta obtener** el **nombre de la red**, aunque la **trazabilidad** de los clientes sigue siendo **posible** con independencia de la **ocultación** del **SSID**.
- **Activar** el **filtrado** de **direcciones MAC*** de los dispositivos **WiFi** para **permitir** que se **conecten** a la **red** los **dispositivos** con las **direcciones MAC especificadas**.
- **Configurar WPA2-AES** en el **modo** de **confidencialidad** de datos, **obteniendo autenticación** y **cifrado** de datos robusto.
- **Limitar** la **cobertura WLAN**. Una **antena multidireccional** ubicada en el **centro** de la **casa**/**oficina** es la opción más común.
- **Desconectar** la **red** cuando **no** se **utilice**. Si bien **no** es **práctico** hacerlo **diariamente**, es muy **recomendable** durante **largos períodos** de **inactividad**.
- **Desactivar UPnP** (Universal Plug and Play)* cuando su uso no sea necesario, para **evitar** que un **código dañino** de la propia red **lo utilice** para **abrir** una **brecha** en el **cortafuegos** del **router** y **permitir** así que otros atacantes **accedan a él**.
- **Actualizar** el "**firmware**" del **router** periódicamente, pues muchas de las actualizaciones y parches que se van incorporando afectan a la seguridad.
- **Usar** direcciones **IP estáticas** o **limitar** el número de **direcciones reservadas** (DHCP) cuando sea posible, para **evitar** que **usuarios no autorizados** puedan **obtener** una **dirección IP** de la **red local**.
- **Activar** el **cortafuegos** del **router**, para que sólo los usuarios y los servicios autorizados puedan tener acceso a la red.
- **Activar** la opción de **registro** (login) para el **router** y **analizar** periódicamente el **historial de accesos**.
- Es recomendable **cambiar** el **DNS** que por **defecto** trae configurado el router por otro que **preserve** la **privacidad** del **usuario** y **mejore** su **seguridad**, por ejemplo, **DNSCrypt**.

Mensajería instantánea (Nº 11)

Las **aplicaciones** de **mensajería instantánea** permiten enviar **mensajes de texto mediante** la conexión a **Internet** (**WhatsApp** y **Telegram** son las más conocidas).

Además, el **uso compartido** de la **información personal** y la **escasa percepción** de **riesgo** que los usuarios tienen con la seguridad las han convertido en un **entorno atractivo** para **intrusos** y **ciberatacantes** que **intentan obtener datos** e **información** de sus **usuarios**.

Uno de los **fallos** más comunes en las aplicaciones de mensajería es la **forma** que utilizan para **borrar** las **conversaciones almacenadas** en el **teléfono** ya que **no** implica la **eliminación directa** de los **mensajes**, sino que estos quedan **marcados** como **libres**, de tal forma que **puedan ser sobrescritos** por **nuevas conversaciones** o **datos** cuando sea necesario siendo **accesible** por **técnicas forenses**.

Además, hay que tener en cuenta las **implicaciones** cuando se tenga **activa** la **opción** de **copia de seguridad** (almacenando una posible conversación ya borrada) que **podría ser recuperada** en un futuro.

Durante el establecimiento de **conexión** con los **servidores**, se puede **intercambiar** en texto claro **información sensible** acerca del usuario quedando **expuesta** a cualquiera en el caso de **utilizar** redes **WiFi públicas** o de **dudosa procedencia**:

- **Sistema operativo** del cliente.
- **Versión de la aplicación** en uso.
- **Número de teléfono** registrado.

Al **utilizar** una conexión basada en **redes privadas virtuales** (VPN), todos los **datos enviados** y **recibidos** pasan **cifrados** entre el **emisor** y el **receptor**, **añadiendo** una **nueva capa de seguridad** para **evitar** posibles **atacantes** que estén interceptando el tráfico de red.

Por otro lado, la **base de datos** de **conversaciones**, **ficheros**, **mensajes**, así como otros datos que manejan este tipo de aplicaciones **se almacena** de **forma local dentro** del **teléfono** y existen multitud de aplicaciones que por ejemplo para WhatsApp **permiten** de una forma sencilla el **descifrado** de la **información** contenida.

Aunque la **información** se **almacena cifrada** en **local**, **existen** multitud de **aplicaciones** que por ejemplo para WhatsApp **permiten** de una forma sencilla el **descifrado** de la **información** contenida, tanto en **versión local** para un equipo, como **a través** de una **aplicación** en el teléfono o **interfaz web**.

Para **evitar** que un **atacante** pueda tener **acceso** a toda la **información privada** que se **almacena** en el **teléfono** hay que prestar especial **atención** a qué [1]**aplicaciones** de terceros se **instalan**, así como el [2]**acceso físico** de otra persona **al terminal**.

En el caso de **intercambio** de **datos** con **redes sociales**, como WhatsApp y Facebook, y **a pesar** de que los **mensajes**, **fotos** e información de **perfil no** serán **objetivos a compartir**, otra información como **número de teléfono**, **contactos**, **hora** de última **conexión**, así como tus **hábitos de uso** de la aplicación pueden ser **compartidos**.

Insistiendo en las recomendaciones indicadas para dispositivos móviles, será necesario adoptar determinadas **precauciones** en el uso de **aplicaciones** de **mensajería instantánea** como:

- **Mantener** el **teléfono bloqueado**. De esta forma, se reducirá el riesgo si el dispositivo cae en las manos equivocadas.
- Sería recomendable **eliminar** las **previsualizaciones** de los **mensajes** y extremar las **medidas** cuando **no** se disponga del **teléfono** al **alcance**.
- En la medida de lo posible, se **recomienda** la **configuración** de las aplicaciones para **solo recibir mensajes** de **personas autorizadas**.
- **Desactivar** la **conectividad adicional** del teléfono cuando no se vaya a utilizar, como podría ser la conexión WiFi o Bluetooth, ya que además de reducir el consumo de batería, reduce la posible superficie de ataque sobre el dispositivo.
- **Utilizar aplicaciones** de mensajería instantánea cuyo **código fuente** esté [1]**abierto** a la comunidad y haya sido [2]**revisado**.

Redes sociales (Nº 12)

Comunicarse, **compartir información**, mantener un **contacto** por interés o afinidad, **relacionarse**, formar una **identidad** y **reputación**, **reivindicarse**, **protestar**, **manipular**... son múltiples los **objetivos** buscados a la hora de **utilizar** una u otra **red social**.

No obstante, el **éxito** alcanzado, las enormes **posibilidades** que brindan y su **uso masivo**, han hecho situarse a las redes sociales en el **punto de mira** de los **ciberatacantes** que **no dudan** en **explotar** los **riesgos** y **vulnerabilidades** que tienen.