Gobierno del Estado de Tabasco

Tabasco cambia contigo

DGTIC
Dirección General de Tecnologías de la Información y Comunicaciones

Manual de Seguridad Informática Básica

Manual de Seguridad Informática Básica

Índice

Introducción

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y, que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

Hay que advertir que la seguridad por ocultación no es un método seguro, por ejemplo, podría pensarse que esconder una copia de la llave de la casa bajo el felpudo de la entrada sería una buena medida contra la posibilidad de quedar uno atrapado fuera de la casa, por culpa de un olvido o pérdida de la llave de uso habitual. Entonces estaríamos fiándonos de la seguridad por ocultación. La vulnerabilidad sería que alguien pudiera entrar en la casa abriendo la puerta con la copia de la llave. Sin embargo, los dueños de la casa creen que la localización de la llave no es conocida públicamente, y que es improbable que un ladrón la encontrara. En este ejemplo, dado que los ladrones suelen conocer los escondites frecuentes, habría que advertir al dueño de la casa contra esta medida, lo mismo puede pasar con un sistema informático.

Un sistema que se apoya en la seguridad por ocultación puede tener vulnerabilidades teóricas o prácticas, pero sus propietarios o diseñadores creen que esos puntos débiles no se conocen, y que es probable que los atacantes no los descubran.

Principios de Seguridad

Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad**: La información sólo debe ser legible para los autorizados.
- **Disponibilidad**: Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Consejos Básicos de Seguridad

Es recomendable seguir una serie de consejos, prácticas y costumbres para maximizar la seguridad informática en la empresa, algunos de ellos son los siguientes:

- Mantener actualizado el equipo (Sistema Operativo y aplicaciones).
- Hacer copias de seguridad con frecuencia.
- Instalar software legal (se obtiene garantía y soporte).
- Usar contraseñas fuertes (evitar nombres, fechas, datos conocidos o deducibles, etc.).
- Utilizar herramientas de seguridad para proteger o reparar el equipo.

- No descargar o ejecutar ficheros desde sitios sospechosos o procedentes de correos sospechosos o no solicitados.
- Analizar con un antivirus todo lo que se descargue.
- No facilitar la cuenta de correo a desconocidos o publicarla en sitios desconocidos.
- No responder a mensajes falsos.
- Observar que la dirección comienza por httpS cuando se este comprando o consultando banca por internet.
- Tener en cuenta que el banco nunca pedirá información confidencial por correo electrónico ni por teléfono.

Seguridad Básica en Internet

Cortafuegos (Firewall)

Un cortafuegos (o firewall en inglés) es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al cortafuegos a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

La instalación y uso de firewall tiene ventajas que repercuten en la seguridad general del sistema informático:

- Protege de intrusiones.- El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- Protección de información privada.- Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

El firewall es posible instalarlo en diferentes niveles y dispositivos en el sistema informático de la empresa:

- Cortafuegos de capa de red o de filtrado de paquetes: Funciona a nivel de red como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte, como el puerto origen y destino, o a nivel de enlace de datos como la dirección MAC.
- Cortafuegos de capa de aplicación: Trabaja en el nivel de aplicación, de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder. Un cortafuegos a de tráfico HTTP suele denominarse Proxy, y

permite que los computadores de una organización entren a Internet de una forma controlada.

- Cortafuegos personal: Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa.

Navegadores Web

Un navegador web (del inglés, web browser) es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de Internet. Esta red de documentos es denominada World Wide Web (WWW). Cualquier navegador actual permite mostrar o ejecutar gráficos, secuencias de vídeo, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces. La funcionalidad básica de un navegador web es permitir la visualización de documentos de texto, posiblemente con recursos multimedia incrustados. Los documentos pueden estar ubicados en la computadora en donde está el usuario, pero también pueden estar en cualquier otro dispositivo que esté conectado a la computadora del usuario o a través de Internet, y que tenga los recursos necesarios para la transmisión de los documentos (un software servidor web). Tales documentos, comúnmente denominados páginas web, poseen hipervínculos que enlazan una porción de texto o una imagen a otro documento, normalmente relacionado con el texto o la imagen.

El seguimiento de enlaces de una página a otra, ubicada en cualquier computadora conectada a la Internet, se llama navegación; que es de donde se origina el nombre de navegador. Por otro lado, hojeador es una traducción literal del original en inglés, browser, aunque su uso es minoritario.

Usar un navegador seguro y mantenerlo actualizado proporciona una base de seguridad mínima que facilita el trabajo a otros programas como antivirus o firewalls.

Nombre	Url
Firefox	http://www.mozilla.org/es-MX/firefox/new/
Chrome (Google)	http://www.google.com/intl/es-419/chrome/

Bloqueador de ventanas emergentes

Un Bloqueador de ventanas emergentes o Anti pop-up es un programa diseñada con el único fin de evitar, bloquear o no mostrar ventanas emergentes. Cuando el usuario navega por Internet se puede ver acorralado de ventanitas, las ventanas emergentes, que pueden salir por delante o por detrás de la ventana activa, también depende de lo que haga el usuario, se dan muchos casos de ventanas que se abre al cierre de otras ventanas.

Correo Electrónico y Spam

El principal problema actual es el spam, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo Rolex, Viagra, pornografía y otros productos y servicios de la calidad sospechosa.

Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es más difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de Spam: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos. Por ahora, el servicio de correo electrónico no puede identificar los mensajes de forma que se pueda discriminar la verdadera dirección de correo electrónico del remitente, de una falsa. Esta situación que puede resultar chocante en un primer momento, es semejante por ejemplo a la que ocurre con el correo postal ordinario: nada impide poner en una carta o postal una dirección de remitente aleatoria: el correo llegará en cualquier caso. No obstante, hay tecnologías desarrolladas en esta dirección: por ejemplo el remitente puede firmar sus mensajes mediante criptografía de clave pública.

Además del spam, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:

- los virus informáticos, que se propagan mediante ficheros adjuntos infectando el ordenador de quien los abre
- el phishing, que son correos fraudulentos que intentan conseguir información bancaria
- los engaños (hoax), que difunden noticias falsas masivamente
- las cadenas de correo electrónico, que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del spam y de mensajes con virus, phishing y hoax.

Precauciones recomendables

Cuando recibamos un mensaje de correo electrónico que hable de algo que desconocemos (aunque nos lo haya mandado alguien que conocemos) conviene consultar su veracidad (por ejemplo a partir de buscadores de la web, tratando de consultar en el sitio web de la supuesta fuente de la información o en webs serias, fiables y especializadas en el tipo de información en cuestión). Sólo si estamos seguros de que lo que dice el mensaje es cierto e importante de ser conocido por nuestros contactos lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla CCO (puede ser necesario poner sólo nuestra dirección de email en la casilla Para) y borrando del cuerpo del mensaje encabezados previos con direcciones de email (para facilitar la lectura es preferible copiar la parte del cuerpo del mensaje sin los encabezados previos y pegarla en un mensaje nuevo -o en el que aparece tras pinchar en reenviar tras borrar todo el texto, repetido a partir de previos envíos-). Así evitaremos la propagación del spam así como la de mensajes con virus (u otro tipo de malware), phishing o hoax. Conviene que hagamos saber esto a nuestros contactos en cuanto nos reenvían mensajes con contenido falso, sin utilizar la casilla CCO o sin borrar encabezados previos con direcciones de correo electrónico.

Cuando el mensaje recibido lleve uno o varios ficheros adjuntos tendremos cuidado, especialmente si el mensaje nos lo manda alguien que no conocemos. Hay peligro de que los archivos contengan virus (u otro tipo de malware). Sólo los abriremos si estamos seguros de su procedencia e inocuidad. Si, tras esto, comprobamos que los ficheros son inofensivos e interesantes para nuestros contactos podremos reenviarlo siguiendo las precauciones del párrafo anterior (en este caso, para que lleguen los ficheros adjuntos es más rápido pinchar en reenviar que crear un mensaje nuevo y volverlos a adjuntar -aunque tendremos cuidado de borrar todo el texto que repite previos reenvíos; quizá pegando después el cuerpo principal del mensaje recibido si tiene información de interés o relacionada con los archivos adjuntos-).

Cuando en un mensaje sospechoso se nos ofrezca darnos de baja de futura recepción de mensajes o de un boletín no haremos caso, es decir, no responderemos el mensaje, ni escribiremos a ninguna dirección supuestamente creada para tal fin (del tipo bajas@xxxxxxx.es o unsubscribe@xxxxxxx.com), ni pincharemos sobre un enlace para ello. Si hiciéramos algo de lo citado confirmaríamos a los spammers (remitentes de correo basura) que nuestra cuenta de correo electrónico existe y está activa y, en adelante, recibiríamos más spam. Si nuestro proveedor de correo lo ofrece podemos pinchar en "Es spam" o "Correo no deseado" o "Marcar como spam". Así ayudaremos a combatir el correo basura.

Servidores FTP

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario normalmente utilizará el FTP para conectarse remotamente a uno y así intercambiar información con él.

Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento web, en el que sus clientes utilizan el servicio para subir sus páginas web y sus archivos correspondientes; o como servidor de backup (copia de seguridad) de los archivos importantes que pueda tener una empresa. Para ello, existen protocolos de comunicación FTP para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol).

El uso de servidores FTP sin seguridad no es recomendado, permite con mucha facilidad el acceso de intrusos desde el exterior (Internet) al interior de la red de la empresa con el consiguiente peligro que representa por fuga de datos sensibles o uso indevido de su sistema informático. El anterior mencionado SFTP añade un nivel extra de seguridad y encriptación que lo hacen más recomendable.

Seguridad a Nivel Usuario

Software malicioso

Con el nombre software malicioso agrupamos todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto. Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos. Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware.

Existen muchísimos tipos de software malicios, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso ciertos bots. Dos tipos comunes de software malicioso es los virus y los gusanos informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismos y en algunas ocasiones mutando, la diferencia entre un gusano y un virus informático radica en la forma de propagación, un gusano opera a través de una red, mientras que un virus lo hace a través de ficheros a los que se añade.

A continuación detallamos, paso a paso, varias tareas habituales para la eliminación de un virus en el ordenador, como la edición del registro y la terminación de procesos.

1. Prueba a restaurar el sistema a un punto de restauración anterior a la aparición de los problemas, para ello sigue los pasos que se indican en el siguiente enlace: Restauración del Sistema.
2. Si de esta manera no has solucionado el problema, prueba a deshabilitar la opción de restauración del sistema, como se indica en el siguiente enlace: Deshabilitar la Opción de Restauración del Sistema.
3. Prueba a realizar un análisis en línea con alguna de las herramientas antivirus que se indican a continuación: Herramientas Antivirus.
4. También puedes realizar un análisis en línea con alguna de las herramientas antiespías que se indican en el siguiente enlace: Herramientas Antiespías
5. Si detectas algún archivo que el antivirus no puede eliminar, deberás hacerlo manualmente. Para ello puedes seguir alguna de las opciones que se indican en el siguiente enlace: Eliminar librerias .DLL y .EXE.
6. Por último, realiza una limpieza del registro de Windows. Para ello sigue las instrucciones del siguiente enlace: Limpiar el Registro de Windows.

Antivirus

Los antivirus son programas cuya función es detectar y eliminar Virus informáticos y otros programas maliciosos.

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.

Actualmente a los antivirus se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

Los virus, gusanos, spyware,... son programas informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen la características de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la información.

Una característica adicional es la capacidad que tienen de propagarse. Otras características son el robo de información, la pérdida de esta, la capacidad de suplantación, que hacen que reviertan en pérdidas económicas y de imagen.

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como pérdida de productividad, baja en el rendimiento del equipo, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir replicándose en otras partes del sistema de información. Las redes en la actualidad ayudan a dicha propagación.

Los daños que los virus dan a los sistemas informáticos son:

- Pérdida de información (evaluable según el caso)
- Horas de contención (Técnicos de SI, Horas de paradas productivas, tiempos de contención o reinstalación, cuantificables según el caso+horas de asesoría externa)
- Pérdida de imagen (Valor no cuantificable)

Hay que tener en cuenta que cada virus es una situación nueva, por lo que es difícil cuantificar a priori lo que puede costar una intervención. Tenemos que encontrar métodos de realizar planificación en caso de que se produzcan estas contingencias.

Herramientas Antivirus

Existen dos formas diferentes de utilizar un antivirus condicionado por dónde esté instalado - en el escritorio de forma local o en un servidor externo para acceder en línea - y en función de las ventajas e inconvenientes, utilizaremos una u otra tal.

Los antivirus de escritorio se suelen utilizar en modo residente para proteger al ordenador en todo momento de cualquier posible infección, ya sea al navegar por Internet, recibir algún correo

infectado o introducir en el equipo algún dispositivo extraíble que esté infectado. No necesitan que el ordenador esté conectado a Internet para poder funcionar, pero sí que es necesario actualizarlos frecuentemente para que sean capaces de detectar las últimas amenazas de virus. Recomendamos tener sólo un antivirus de escritorio en el ordenador, ya que tener varios antivirus puede ocasionar problemas de incompatibilidad entre ellos.

Nombre	Disponibilidad	URL
AVG	Gratuito	http://free.avg.com/ww-es/homepage
Avast	Gratuito	http://www.avast.com/es-mx/
Clam AV	Libre	http://www.clamav.net/

Los antivirus en línea son útiles para analizar el ordenador con un segundo antivirus cuando sospechamos que el equipo puede estar infectado. Para ejecutarlos es necesario acceder con el navegador a una página de Internet.

Si bien son muy útiles para realizar un escaneo del ordenador y, de este modo, comprobar que no está infectado, no sirven para prevenir infecciones, esto sólo lo hacen los antivirus de escritorio.

Nombre	Disponibilidad	URL
Trend Micro	Gratuito	http://la.trendmicro.com/
McAfee Free Scan	Gratuito	http://home.mcafee.com/downloads/free-virus-scan

Software Espía

Los programas espías o spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.
Pueden tener acceso por ejemplo a: el correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, qué tiempos se está en ellas y con qué frecuencia se regresa; qué software está instalado en el equipo y cuál se descarga; qué compras se hacen por internet; tarjeta de crédito y cuentas de banco.

Principales síntomas de infección son:

- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto, la mayoría de temas pornográficos y comerciales (por ejemplo, la salida al mercado de un nuevo producto).
- Barras de búsquedas de sitios como la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no se pueden eliminar.
- Creación de carpetas tanto en el directorio raíz, como en "Archivos de programas", "Documents and Settings" y "WINDOWS".
- Modificación de valores de registro.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Es notable que tarda más en iniciar el computador debido a la carga de cantidad de software spyware que se inicia una vez alterado el registro a los fines de que el spyware se active al iniciarse la computadora.
- Al hacer click en un vínculo y el usuario retorna de nuevo a la misma página que el software espía hace aparecer.
- Botones que aparecen en la barra de herramientas del navegador y no se pueden quitar.
- Aparición de un mensaje de infección no propio del sistema, así como un enlace web para descargar un supuesto antispyware.
- Al acceder a determinados sitios sobre el escritorio se oculta o bloquea tanto el panel de control como los iconos de programas.
- Denegación de servicios de correo y mensajería instantánea.

Precauciones recomendables

Cuando recibamos un mensaje de correo electrónico que hable de algo que desconocemos (aunque nos lo haya mandado alguien que conocemos) conviene consultar su veracidad (por ejemplo a partir de buscadores de la web, tratando de consultar en el sitio web de la supuesta fuente de la información o en webs serias, fiables y especializadas en el tipo de información en cuestión). Sólo si estamos seguros de que lo que dice el mensaje es cierto e importante de ser conocido por nuestros contactos lo reenviaremos, teniendo cuidado de poner las direcciones de correo electrónico de los destinatarios en la casilla CCO (puede ser necesario poner sólo nuestra dirección de email en la casilla Para) y borrando del cuerpo del mensaje encabezados previos con direcciones de email (para facilitar la lectura es preferible copiar la parte del cuerpo del mensaje sin los encabezados previos y pegarla en un mensaje nuevo -o en el que aparece tras pinchar en reenviar tras borrar todo el texto, repetido a partir de previos envíos-). Así evitaremos la propagación del spam así como la de mensajes con virus (u otro tipo de malware), phishing o hoax. Conviene que hagamos saber esto a nuestros contactos en cuanto nos reenvían mensajes con contenido falso, sin utilizar la casilla CCO o sin borrar encabezados previos con direcciones de correo electrónico.

Cuando el mensaje recibido lleve uno o varios ficheros adjuntos tendremos cuidado, especialmente si el mensaje nos lo manda alguien que no conocemos. Hay peligro de que los archivos contengan virus (u otro tipo de malware). Sólo los abriremos si estamos seguros de su procedencia e inocuidad. Si, tras esto, comprobamos que los ficheros son inofensivos e interesantes para nuestros contactos podremos reenviarlo siguiendo las precauciones del párrafo anterior (en este caso, para que lleguen los ficheros adjuntos es más rápido pinchar en reenviar que crear un mensaje nuevo y volverlos a adjuntar -aunque tendremos cuidado de borrar todo el texto que repite previos reenvíos; quizá pegando después el cuerpo principal del mensaje recibido si tiene información de interés o relacionada con los archivos adjuntos-).

Cuando en un mensaje sospechoso se nos ofrezca darnos de baja de futura recepción de mensajes o de un boletín no haremos caso, es decir, no responderemos el mensaje, ni escribiremos a ninguna dirección supuestamente creada para tal fin (del tipo bajas@xxxxxxx.es o unsubscribe@xxxxxxx.com), ni pincharemos sobre un enlace para ello. Si hiciéramos algo de lo citado confirmaríamos a los spammers (remitentes de correo basura) que nuestra cuenta de correo electrónico existe y está activa y, en adelante, recibiríamos más spam. Si nuestro proveedor de correo lo ofrece podemos pinchar en "Es spam" o "Correo no deseado" o "Marcar como spam". Así ayudaremos a combatir el correo basura.

Phishing

Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Dado el creciente número de denuncias de incidentes relacionados con el phishing se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica, campañas para prevenir a los usuarios y con la aplicación de medidas técnicas a los programas.

Respuesta social

Una estrategia para combatir el phishing adoptada por algunas empresas es la de entrenar a los empleados de modo que puedan reconocer posibles ataques phishing. Una nueva táctica de phishing donde se envían correos electrónicos de tipo phishing a una compañía determinada, conocido como spear phishing, ha motivado al entrenamiento de usuarios en varias localidades, incluyendo la Academia Militar de West Point en los Estados Unidos. En un experimento realizado en junio del 2004 con spear phishing, el 80% de los 500 cadetes de West Point a los que se les envió un e-mail falso fueron engañados y procedieron a dar información personal.

Un usuario al que se le contacta mediante un mensaje electrónico y se le hace mención sobre la necesidad de "verificar" una cuenta electrónica puede o bien contactar con la compañía que supuestamente le envía el mensaje, o puede escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de phishing. Muchas compañías, incluyendo eBay y PayPal, siempre se dirigen a sus clientes por su nombre de usuario en los correos electrónicos, de manera que si un correo electrónico se dirige al usuario de una manera genérica como ("Querido miembro de eBay") es probable que se trate de un intento de phishing.

Respuestas técnicas

Hay varios softwares anti-phishing disponibles. La mayoría de estos programas trabajan identificando contenidos phishing en sitios web y correos electrónicos; algunos software anti-phishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el phishing recibidos por el usuario.

Muchas organizaciones han introducido la característica denominada preguntas secreta, en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Las páginas de Internet también han añadido herramientas de verificación que permite a los usuarios ver imágenes secretas que los usuarios seleccionan por adelantado; sí estas imágenes no aparecen, entonces el sitio no es legítimo. Estas y otras formas de autentificación mutua continúan siendo susceptibles de ataques, como el sufrido por el banco escandinavo Nordea a finales de 2005.

Muchas compañías ofrecen a bancos y otras entidades que sufren de ataques de phishing, servicios de monitoreo continuos, analizando y utilizando medios legales para cerrar páginas con contenido phishing.

El Anti-Phishing Working Group, industria y asociación que aplica la ley contra las prácticas de phishing, ha sugerido que las técnicas convencionales de phishing podrían ser obsoletas en un futuro a medida que la gente se oriente sobre los métodos de ingeniería social utilizadas por los phishers. Ellos suponen que en un futuro cercano, el pharming y otros usos de malware se van a convertir en herramientas más comunes para el robo de información.

Contraseñas Seguras

En el control del acceso para todo, se realiza una relación entre seguridad y conveniencia. Es decir, si algún recurso está protegido por una contraseña, entonces la seguridad se incrementa con la consecuente pérdida de conveniencia para los usuarios. La cantidad de seguridad es inherente dada una política para contraseñas en particular que es afectada por diversos factores que se mencionarán a continuación. Sin embargo, no existe un método que sea el mejor para definir un balance apropiado entre seguridad y conveniencia.

Algunos sistemas protegidos por contraseñas plantean pocos o ningún riesgo a los usuarios si éstos se revelan, por ejemplo, una contraseña que permita el acceso a la información de una Web site gratuita. Otros plantean un modesto riesgo económico o de privacidad, por ejemplo, un password utilizado para acceder al e-mail, o alguna contraseña para algún teléfono celular. Aún así, en otras situaciones se pueden tener consecuencias severas si la contraseña es revelada, tales como las usadas para limitar el acceso de expedientes sobre tratamientos del SIDA o el control de estaciones de energía.

Estudios en la producción de sistemas informáticos han indicado por décadas constantemente que cerca de 40% de todas las contraseñas elegidas por usuarios se conjeturan fácilmente.

- Muchos de los usuarios no cambian la contraseña que viene predeterminada en muchos de los sistemas de seguridad. Listas de estas contraseñas están disponibles en el Internet.
- Una contraseña puede ser determinada si un usuario elige como contraseña una pieza de información personal que sea fácil de descubrir (por ejemplo: número de ID de estudiante, el nombre del novio/a, el día de cumpleaños, número telefónico, etc.). Los datos personales sobre individuos están ahora disponibles en diferentes fuentes, muchas de ellas están en línea, y pueden ser obtenidas frecuentemente por alguien que use técnicas de ingeniería social, como actuar como un trabajador social que realiza encuestas.

- Una contraseña es vulnerable si puede ser encontrada en una lista. Los diccionarios (frecuentemente de forma electrónica) están disponibles en muchos lenguajes, y existen listas de contraseñas comunes.
- En pruebas sobre sistemas en vivo, los ataques de diccionarios son rutinariamente acertados, por lo que el software implementado en este tipo de ataques ya se encuentra disponible para muchos sistemas. Una contraseña muy corta, quizás elegida por conveniencia, es más vulnerable si un hacker puede obtener la versión criptográfica de la contraseña. Las computadoras son en la actualidad lo suficientemente rápidas para intentar todas las contraseñas en orden alfabético que tengan menos de 7 caracteres.

Una contraseña débil sería una que fuese muy corta o que fuese la predeterminada, o una que pudiera se adivinada rápidamente al buscar una serie de palabras que es posible encontrar en diccionarios, nombres propios, palabras basadas en variaciones del nombre del usuario. Una contraseña fuerte debe ser suficientemente larga, al azar, o producible solo por el usuario que la eligió, así, el 'adivinar' requerirá un largo tiempo. La cantidad de tiempo juzgada para ser 'demasiado larga' variará de acuerdo al atacante, sus recursos, la facilidad con la que la contraseña se pueda descubrir, y la importancia de esta para el atacante. Por lo tanto, una contraseña de un estudiante quizás no valga la pena para invertir más de algunos segundos en la computadora, mientras que la contraseña para acceder al control de una transferencia de dinero del sistema de un banco puede valer varias semanas de trabajo en una computadora.

'Fuerte' y 'débil' tienen significado solamente con respecto a tentativas de descubrir la contraseña de un usuario, ya sea por una persona que conoce al usuario, o una computadora que tratara de usar millones de combinaciones. En este contexto, los términos pueden tener una precisión considerable. Pero nótese que una contraseña 'fuerte' en este sentido puede ser robada, truqueada o extraída del usuario, ya sea mediante la extracción del historial de un teclado, grabada mediante aparatos de comunicación, o copiada de notas dejadas por olvido.

Ejemplos de contraseñas débiles incluyen las siguientes: administrador, 1234, "nombre del usuario", xx/xx/xx - fechas importantes, ya que la mayoría de estas se encuentran en o bases de datos o diccionarios (dictionary search attack). Ejemplos de contraseñas fuertes serían las siguientes: tastywheeT34, partei@34!, y #23kLLflux. Estas contraseñas son largas y usan combinaciones de letras mayúsculas y minúsculas, de números y de símbolos. No son fácilmente encontrados en listas de contraseñas y son suficientemente largas para provocar que una búsqueda burda sea impractica en la mayoría de las circunstancias. Nótese que algunos sistemas no permiten símbolos como #, @ y ! en contraseñas y son más difíciles de encontrar en algunos teclados diseñados para ciertos países. En estos casos, agregar uno o dos caracteres (letra o número) puede ofrecer una seguridad equivalente. También nótese que, al haberse publicado estos ejemplos de contraseñas, estos ya no son buenas opciones: ejemplos de discusiones públicas sobre contraseñas obviamente son buenos candidatos para incluirse en las listas de diccionarios para atacar sistemas.

El método más efectivo para generar contraseñas es seleccionar suficientes caracteres al azar, aunque este tipo de contraseñas son las más difíciles de recordar. Algunos usuarios desarrollan frases o palabras compuestas que tienen letras al azar como iniciales de varias palabras. Otra manera de elaborar contraseñas al azar que sean más memorables es usar palabras al azar o sílabas en lugar de letras al azar.

Memorias personales son recomendables en ocasiones, es decir, cosas que sean memorables a una persona en particular, pero no para otras, por ejemplo: la contraseña yt21cvpppv, es difícil de recordar, pero se deriva de la frase "Yo tenía 21 cuando visite París por primera vez", posiblemente fácil de recordar. Sin embargo, si la primera visita a Paris fue un hecho muy trascendente para un usuario en particular, puede ser posible que la contraseña se adivine del conocimiento del usuario, y por lo tanto esta no sería una opción sensata para utilizarse como contraseña. Según Bruce Schneier la contraseña más utilizada es password1.

Seguridad Aplicada a la Oficina

La seguridad del entorno es una parte básica e importante, relacionada con la seguridad general, un acceso indebido, una mala estructura o unas políticas inadecuadas pueden conducir a una fuga de información o a una pérdida de datos perjudiciales para la empresa.

Existen casos publicados en la prensa de extravíos importantes de datos que podrían llegar a implicar el cierre de la empresa o importantes sanciones.

A continuación se detallan las partes más importantes, tanto de seguridad física como de comportamiento general de los empleados para poder garantizar un entorno seguro.

Seguridad en Redes Wireless (Wi-Fi)

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.
- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total. Esto no ocurre, por ejemplo, en móviles.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema Wi-Fi es la pérdida de velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- La desventaja fundamental de estas redes existe en el campo de la seguridad.
- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o muy vulnerables a los crackers), sin proteger la información que por ellas circulan. Uno de los puntos débiles (sino el gran punto débil) es el hecho de no poder controlar el área que la señal de la red cubre, por esto es posible que la señal exceda el perímetro del edificio y alguien desde afuera pueda visualizar la red y esto es sin lugar a dudas una mano para el posible atacante.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son:

- Utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP y el WPA, que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos
- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente fáciles de conseguir con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

Dispositivos Fijos y Móviles

Máquinas y Dispositivos de Escritorio

Los ordenadores y dispositivos de escritorio (Impresoras, faxes, pequeños concentradores, concentradores usb, etc) son uno de los puntos más difíciles de controlar, pues dependen totalmente del uso o mal uso que el usuario nal pueda realizar de ellos o sobre ellos. La única solución en este caso es la implantación de una política clara y comprensible para el usuario nal de uso de los dispositivos que están a su cargo.

Es importante responsabilizar de alguna forma al usuario nal del hardware que está a su cargo, sin que esto suponga una carga añadida a su trabajo normal. Hay que encontrar el punto justo entre la facilidad y exibilidad en el uso de los dispositivos a cargo del usuario nal y la seguridad física de estos dispositivos.

Ordenadores Portátiles

Debemos tener en cuenta la portabilidad de estos dispositivos, lo que los hace susceptibles de ser robados con facilidad, sobre todo cuando se encuentran fuera de la empresa.

Debe crearse una política de uso y responsabilidad para las personas que utilizan ordenadores portátiles de la empresa y sobre todo para las personas que tienen que llevarse estos dispositivos fuera de la empresa. Lo más importante, aparte del valor económico de los portátiles, son los datos que pueden contener, datos que en muchos casos pueden ser importantes e incluso vitales para la empresa. Por eso debe responsabilizarse seriamente a los usuarios de los portátiles que sacan de la empresa, manteniendo un control de entrada/salida de estos dispositivos y de la integridad física de los mismos. En caso de robo el usuario debe comunicar con absoluta inmediatez a la empresa el evento que se ha producido, para que esta pueda minimizar los riesgos que implica el robo de los datos que ese portátil pueda contener.

Como regla general los portátiles que deban abandonar la empresa no deberían contener ningún tipo de dato importante o comprometido para la empresa, en caso de que el usuario necesite acceso a estos datos pongamos desde su domicilio particular puede ser más conveniente la instalación de una linea ADSL y que conecten de forma segura a los servidores de la empresa y trabajen de forma remota. Si el usuario debe de usar estos dispositivos en otras empresas o en trabajos de campo deberán protegerse de todas las formas posibles los datos críticos que puedan contener, encriptándolos con sistemas seguros y permitiendo sólo el acceso al trabajador por medio de claves intransferibles de las que este deberá ser responsable. La única solución es la responsabilización de forma seria del usuario de la integridad física de la máquina, teniendo una política muy clara de lo que el usuario puede hacer o no hacer con el ordenador.

Los portátiles que salen de la empresa pueden volver con virus, software no deseado, errores cometidos por el usuario o simplemente con programas y datos borrados. Para protegerse de este tipo de eventos hay dos soluciones, una de ellas es el adquirir software antivirus, □rewalls personales, software de control de acceso al portátil que impida la instalación de software y medidas similares; la otra opción es el control a la salida del portátil de su contenido por medio de un backup, que se volverá a comprobar cuando el portátil vuelva a la empresa para comprobar la integridad de los datos.

Dispositivos de mano (Teléfonos Móviles, Palms, Pocket Pcs, etc...)

Para los dispositivos de mano solo debemos decir que deben tomarse exactamente las mismas medidas que para los portátiles, aunque teniendo en cuenta que normalmente no contienen datos tan críticos para la empresa como los portátiles, aunque son mucho más fáciles de robar. Es bastante común este caso, el robo de un dispositivo de mano con todos los datos de un empleado, que luego pueden ser usados, pues suelen contener números de teléfono internos de la empresa, datos sobre la empresa y en los casos más aterradores incluso passwords de acceso a los sistemas.

Lo mejor que se puede hacer es no mantener nunca datos importantes en este tipo de dispositivos, sobre todo passwords de acceso, y el aconsejar también que si uno de estos dispositivos es robado o perdido se realice un informe donde se indique que datos susceptibles de ser usados para hacking social o informático pudiera contener el dispositivo.

Comunicaciones y Suministros de Energía

Los Suministros de Energía de la Oficina

El suministro de energía suele tener dos partes, una parte externa que provee y gestiona la compañía eléctrica y que llega justo hasta el punto donde se encuentra el sistema de tari□cación, detrás del cual se suele encontrar nuestro sistema de protecciones y todo nuestro cableado y dispositivos, la parte interna.

La parte externa está protegida por un fusible y un limitador de potencia que instala la compañía eléctrica y que deben estar calculados para la potencia que vaya a consumir nuestra oficina. Normalmente no deberemos preocuparnos por estos dispositivos, que suelen estar sobredimensionados para evitar cortes de energía y que tienen como principal función la protección de la red eléctrica de la compañía.

Es imprescindible comprobar que existen todos los dispositivos de protección necesarios para la oficina y que estos permitan aislar un problema eléctrico lo máximo que sea posible. Idealmente deberíamos tener protecciones de forma que un problema eléctrico afecte lo mínimo posible a los sistemas de hardware y a la red. Los sistemas que consuman gran potencia, como los grandes sistemas SAI (Sistema de alimentación ininterrumpida) deberían tener su propia protección, normalmente interna en forma de fusibles u otro tipo de protecciones.

Deberá estudiarse también las protecciones como fusibles, automáticos y diferenciales que tengamos en cada una de las concentraciones de hardware, como centros de computación, racks o armarios con varios sistemas montados. Todos los dispositivos de protección deben estar homologados y la instalación debe cumplir con el reglamento de baja tensión del país donde nos encontremos. Esto nos asegurará una cierta protección contra dispositivos e instalaciones defectuosos. Es importante asegurarnos de que la instalación eléctrica cumple estas condiciones, solicitando la documentación necesaria para comprobarlo.

Sistemas SAI

Es imprescindible el asegurar un suministro estable y continuo de energía eléctrica al hardware, utilizando normalmente sistemas SAI (Sistema de alimentación ininterrumpida) que regularán la tensión evitando los picos de voltaje que pueda traer la red y proporcionarán un tiempo de autonomía por medio de baterías en caso de cortes del suministro eléctrico.

Los sistemas de alimentación ininterrumpida (SAI) son imprescindibles en la seguridad física de un sistema informático. La mayoría de los sistemas operativos responden mal a las caídas repentinas y puede producirse perdida de datos importantes si no se usan sistemas de archivos con Journaling como Ext3, Reiserfs, XFS, JFS o similares.

Para evitar puntos de fallo es conveniente el no depender únicamente de un sistema SAI para todo el hardware a proteger, siendo más conveniente la instalación de varios SAI que puedan suministrar energía a parte del sistema en el caso de que uno de los SAI fallara.

Hay que tener en cuenta siempre que no sólo es necesario proveer de un suministro estable y continuo de energía a los ordenadores y a los sistemas de almacenamiento, deberemos proporcionar el mismo tratamiento al hardware de red, incluidos concentradores, enrutadores,

pasarelas y todos los dispositivos que sean necesarios para el funcionamiento normal de la empresa. Estas medidas pueden incluir también otro tipo de hardware como impresoras láser o fotocopiadoras.

Los Enlaces de Comunicaciones de la Oficina

Los sistemas de comunicaciones suelen ser públicos. La mayoría de los edi□cios usarán sistemas públicos de comunicaciones, como puede ser la red telefónica para el transporte de voz y datos o las conexiones ADSL/Cable/etc que usan medios compartidos para la transmisión de datos.

El caso de los sistemas de comunicaciones deberemos buscar la mayor seguridad y protección en los sistemas y además siempre que sea posible tener redundancia en los sistemas de comunicaciones para prever el caso de que uno de los enlaces falle. Las compañías telefónicas que suelen ser las que proveen los servicios no suelen proporcionar ningún tipo de certeza de que nuestras comunicaciones van a mantenerse, por lo que estamos a expensas de las averías o fallos que se puedan producir en las redes públicas para tener comunicaciones.

Es aconsejable por tanto mantener más de una linea y además con diferentes compañías, de forma que tengamos siempre comunicación telefónica aunque alguna de las compañías falle. Las compañías que usan la red telefónica clásica comparten el medio físico para mandar los datos, pero en cambio las compañías de cable suelen tener su propia red para proporcionar la conectividad, por lo que puede ser interesante la contratación de una linea con una compañía tradicional y otra con una compañía de cable para tener dos redes independientes.

Copias de Seguridad, Backups y Redundancia de Datos

Hoy en día los datos almacenados en los sistemas informáticos son un elemento imprescindible para el funcionamiento de cualquier empresa.

Mantenerlos seguros y fácilmente recuperables es una tarea importante a no menospreciar. Es fundamental poder acceder a los datos siempre que sea necesario, y la única forma de asegurar con un porcentaje aceptable de seguridad que nuestros datos estarán disponibles es proveer algún tipo de redundancia para estos datos. Existen diferentes niveles para asegurar una buena replicación de los datos.

Redundancia de datos en el hardware

Es aconsejable la redundancia a nivel interno de hardware en los sistemas primarios encargados de almacenar los datos, básicamente es aconsejable un sistema con RAID (conjunto de discos redundantes) para asegurar una replicación mínima en caso de fallo, ya sea RAID 0, RAID 1 o RAID 5 (en función del número de discos), sobre hardware o sobre software. Con el precio continuamente decreciente de los discos duros un sistema de RAID basado en software sale por un precio reducido, y esto nos proporcionará redundancia en el hardware sin aumentar excesivamente el presupuesto.

Redundancia de sistemas de almacenamiento

Los sistemas de alta disponibilidad consisten en varias máquinas que proporcionan la misma funcionalidad y se sincronizan permaneciendo siempre todas en el mismo estado. Si la máquina que está proporcionando el servicio falla otra de las máquinas ocupa su lugar y el sistema puede seguir funcionando. Con dos o tres máquinas proporcionando la misma funcionalidad podemos obtener tasas de □abilidad muy altas, sobre todo cuando hablamos de integridad de datos.
La replicación de los datos de un servidor de archivos principal en otros servidores de archivos secundarios (preferentemente alojados en otra oficina) es otra opción recomendable para proporcionar seguridad física en los sistemas de almacenamiento o en servidores de aplicaciones.
Los sistemas de alta disponibilidad suponen una inversión superior a mantener copias de seguridad en otros servidores, pero son los más aconsejables. Si no es posible instalar sistemas de alta disponibilidad, es muy aconsejable programar copias de seguridad en servidores localizados lejos del servidor principal a través de la red para no perder nunca datos.

Sistemas de backup

Los sistemas de backup son una necesidad inexcusable hoy en día en cualquier empresa que maneje una cantidad de datos medianamente grande. Teniendo esto en cuenta y suponiendo que disponemos de un sistema de backup □able debemos tener en cuenta otra serie de consideraciones. La primera es la seguridad física de los backups y la mejor solución que se aconseja es mantener los backups lejos de los sistemas que contienen los datos de los que hemos hecho backup. De nada sirve hacer backups si cuando los necesitamos no funcionan.

Debemos comprobar que los backups que hemos realizado pueden ser restaurados correctamente, o estaremos con□ando en un sistema que no podemos asegurar que funciona correctamente. La seguridad física de las cintas o dispositivos de backup debe ser una preocupación y por tanto se debe tener previsto cualquier incidente que se pueda producir, como incendios, terremotos, robos y así cualquier evento que se nos pueda ocurrir.
El sistema más e□caz para mantener los backups seguros es mantenerlos fuera de la oficina, o al menos mantener una copia de estos, ya sea en otro edi□cio o en un centro de almacenamiento de backups. Estos últimos son centros que proporcionan almacenamiento de las cintas de backup con todas las medidas de seguridad física imaginables y que son una buena alternativa a el mantenimiento de los backups cerca de las máquinas de las que se ha hecho backup. Puede contratarse uno de estos servicios y mandar los backups o copias de estos a uno de estos servicios, que velará por la seguridad de nuestros backups.

Como regla general deberemos mantener al menos una copia de los backups principales fuera del edi□cio, o incluso mantener fuera todos los backups. Medidas como el almacenamiento de los backups en el domicilio particular son contraproducentes, pues no suelen tener ni las medidas de seguridad necesarias ni la capacidad de mantener un entorno óptimo para los backups.

Acceso al Software y al Hardware

La relación de los usuarios (empleados) con el software y el hardware determina en gran medida la seguridad de una empresa. La responsabilidad y conocimientos que estos muestran al interaccionar con los sistemas informáticos son incluso más importantes que todos los sistemas de seguridad qué se puedan instalar. En el apéndice A se incluye un documento dónde se detallan las

responsabilidades básicas de un empleado y el nivel de responsabilidad deseado para asegurar un correcto nivel de seguridad informática.

Acceso Físico al Hardware

El acceso físico al hardware sea este computadoras o dispositivos de red deberá ser restringido, teniendo en cuenta las necesidades de cada departamento o usuario.

Los equipos de red importantes como routers, pasarelas y concentradores deberán estar en un lugar donde exista un control de acceso. Los dispositivos de red que permitan un acceso remoto deberán ser protegidos por medio de claves y cortafuegos para limitar el acceso. Es esencial el control físico de estos dispositivos porqué algunos de ellos permiten modificar la con□guración cuando se tiene acceso físico a ellos.

Las maquinas de usuario □nal donde han de trabajar los empleados son las más importantes y las más difíciles de proteger, porqué normalmente han de estar situadas en el entorno del usuario, donde están expuestas. Se intentará siempre que sea posible que el usuario □nal trabaje de forma remota sobre los servidores de la empresa, implementando soluciones de acceso remoto a las aplicaciones y los datos, o manteniendo las máquinas en una localización segura donde el usuario no pueda manipularlas sino es necesario.

Sistemas de Almacenamiento Externo: Discos y Memorias USB

Los sistemas de almacenamiento USB son un punto incomodo en la seguridad informática de una oficina. Para empezar tenemos lo que puede venir en ellos: virus, software pirateado, todo tipo de software o datos poco recomendables para un lugar de trabajo, juegos, etc. Luego tenemos todo lo que se puede llevar en ellos: datos de la empresa, software cuya licencia ha sido adquirido por la empresa, software bajado de Internet, etc.

Si lo que más nos preocupa (tenemos antivirus, □rewall, control de software, etc) es que el usuario pueda replicar datos y sacarlos de la empresa sólo podemos hacer dos cosas, la primera es mantener los datos lejos del usuario, la segunda es inhabilitar los puertos USB y los sistemas serie o paralelo, ya sea mediante métodos software o hardware.

La recomendación es mantener los datos en los servidores y que los usuarios trabajen sobre los datos de forma remota, mantener los datos alejados del usuario □nal y así evitar que estos puedan ser replicados. Todos los demás sistemas son útiles pero no e□caces. Se pueden quitar las grabadoras de CDs, las disqueteras, incluso evitar el uso de los puertos USB o similares, pero un usuario decidido a sacar los datos de su máquina, ya sea por desconocimiento, para facilitar su trabajo o por simple malicia conseguirá hacerlo.

Sistemas de Captación de Datos: Keycatchers

Los keycatchers son dispositivos utilizados para captar datos, se interponen entre el teclado y el ordenador para captar las pulsaciones del usuario, grabando los datos que se introducen, buscando sobre todo la adquisición de claves que el usuario pueda teclear. Son dispositivos aparatosos y fáciles de detectar, aunque también son fáciles de instalar y volver a quitar. Un dispositivo de estos

simplemente instalado diez minutos en la máquina de trabajo del personal de un banco puede proporcionar al hacker las claves para acceder al sistema interno de la empresa, números de tarjetas de crédito, números de cuenta y otro tipo de datos secretos.

Hay muchos otros sistemas de captación de datos. Desde dispositivos que se intercalan en el cable de red y graban los datos en bruto que luego se pueden decodi□car y estudiar hasta simplemente un intruso conectando un portátil a la red interna para obtener los datos y passwords que circulen a través de la red. Otro tipo de dispositivos son los que captan datos de redes wireless, que pueden decodi□car el sistema de encriptación y obtener datos y passwords.

Seguridad del Password de la Bios

La seguridad que proporcionan las passwords de bios es una seguridad absolutamente □cticia. Muchos administradores confían ciegamente en la seguridad de los sistemas asegurados mediante passwords de bios, sobre todo cuando se intenta impedir el arranque desde disquetera o desde CDROM. La seguridad que proporciona el password de bios es mínima si no tenemos una seguridad física su□ciente sobre el sistema en cuestión. Si un intruso consigue abrir la caja del ordenador puede simplemente activar el puente de borrado de la bios y nuestro password se borrará.

Por todas estas técnicas y por muchas otras que existen simplemente no debemos con□ar en los password de bios. Si alguien tiene acceso al interior de nuestra máquina podrá hacer lo que quiera con ella. Puede borrar el bios, cambiarlo por otro, instalar una disquetera o un CDROM. La seguridad física de la caja por tanto es fundamental si queremos asegurar que la con□guración de la máquina no va a ser cambiada.

Apéndice A

NOMBRE Y APELLIDOS: ……
FECHA: ……
PUESTO DE TRABAJO: ……

FUNCIONES Y OBLIGACIONES DEL PERSONAL DE

……..(Nombre Empresa)……..

Las funciones y obligaciones de cada una de las personas que forman parte de JURISWEB INTERACTIVA, S.L. (en adelante, "la Empresa") y que tengan acceso a los sistemas de información de la Empresa, así como a los datos de carácter personal contenidos en sus ficheros serán las siguientes:

Confidencialidad:

1. Cada trabajador es plenamente consciente de que el uso inadecuado, la copia o la difusión de la información no autorizada puede conducir a la Empresa hacia una situación de riesgo. Por ello, mediante la firma del presente documento, el trabajador entiende y acepta cumplir en todo momento con las normas aquí especificadas o que se indiquen en cada momento por los responsables de la Empresa.

2. Toda la información albergada en la red corporativa de la Empresa, bien de forma estática o bien circulando en forma de mensajes de correo electrónico, tiene carácter confidencial.

Tratamiento de los datos de carácter personal:

1. Cada trabajador única y exclusivamente podrá utilizar aquellos datos de carácter personal a los que tenga acceso en virtud de sus funciones para dar cumplimiento a sus obligaciones laborales, quedando expresa y completamente prohibida cualquier otra utilización.

2. Cada trabajador no podrá borrar, destruir, dañar, alterar o modificar cualquiera de los datos de carácter personal que contengan las bases de datos de la Empresa sin la autorización expresa de los responsables de la misma, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

3. Cada trabajador no podrá realizar copias, transmisiones, comunicaciones o cesiones de los datos de carácter personal propiedad de la Empresa sin la autorización expresa de los

responsables de la misma, siempre y cuando no sea en ejercicio de las funciones que le han sido encomendadas.

4. Cada trabajador tendrá la obligación de comunicar y/o subsanar cualquier anomalía, error, imprecisión o fallo que detectara en los ficheros de datos de carácter personal propiedad de la Empresa.

5. Todos los datos de carácter personal titularidad de la Empresa que sean objeto de tratamiento por parte de los trabajadores, así como cualquier otro documento de trabajo, deberán ubicarse y/o tratarse en los Servidores. Los trabajadores de la Empresa no podrán alojar ningún tipo de información en sus ordenadores personales.

6. Los trabajadores no podrán utilizar sistemas de comunicación para transmitir datos de carácter personal si éstos no han sido autorizados por parte de la Empresa. En este sentido, queda expresamente prohibida la transmisión de datos de carácter personal de nivel alto si no es por sistemas de transmisión seguros y que hayan sido autorizados por la Empresa de forma expresa.

Claves de acceso o identificadores de usuario:

1. Cada trabajador que en el desarrollo de sus funciones laborales realice actividades en las cuales sea necesario acceder a los ficheros de datos de carácter personal propiedad de la Empresa, dispondrá de un nombre de usuario que le identifique única y exclusivamente a él y de una clave o contraseña personal que le permita, durante el proceso de acceso a los datos, autenticarse como usuario autorizado.

2. Dicho nombre de usuario o identificador, así como la correspondiente contraseña, será personal e intransferible.

3. Cada trabajador será responsable de conservar de forma confidencial y segura su nombre de usuario (identificador único) y su contraseña personal. En los supuestos que el trabajador tuviera la certeza o sospechara que alguien está utilizando dichos identificadores o contraseñas, deberá solicitar a la Empresa que le asigne un identificador y contraseña nuevos.

4. Dicho identificador único y la contraseña sólo podrán utilizarse dentro de los locales y oficinas de la Empresa. Queda expresamente prohibido el acceso desde fuera de los locales de la Empresa sin la autorización expresa de los responsables de la misma.

Documentos de trabajo:

1. Todos los documentos, en cualquier tipo de formato, que realice el trabajador o que éste reciba para el desarrollo de sus funciones, son propiedad de la Empresa y no podrán utilizarse para otras funciones que no sean las que tenga expresamente asignadas el trabajador.

2. Ningún trabajador podrá eliminar documentos e información sin la previa autorización de los responsables de la Empresa.

3. Queda expresamente prohibido enviar cualquier tipo de documento a personas no autorizadas. Tampoco está autorizado guardar o tratar documentos en dispositivos electrónicos que no estén previamente autorizados por la Empresa de forma expresa.

Titularidad y uso de los equipos y programas informáticos:

1. La red corporativa, los sistemas informáticos y los terminales utilizados por cada trabajador son propiedad de la Empresa.

2. Los recursos informáticos de la Empresa, en particular los ordenadores, correos electrónicos, redes y conexiones, no deberán en ningún caso utilizarse para propósitos distintos de los expresamente previstos, que no son otros que aquellos relacionados con la actividad que el trabajador desarrolle para la Empresa. Está estrictamente prohibido cualquier uso con fines comerciales y/o personales de dichos recursos no relacionados con las funciones propias de cada trabajador, siempre que ello pueda suponer un perjuicio para la Empresa.

3. Queda prohibido el uso de programas informáticos distintos de los expresamente autorizados y/o instalados previamente por la Empresa. El trabajador será personalmente responsable de los daños y perjuicios que puedan ocasionarse por la instalación y utilización de programas distintos a los anteriormente referidos, y en especial en aquellos casos en los que se utilicen programas que carezcan de la correspondiente licencia de uso, más conocidos como 'copias piratas' de software de pago.

4. Queda prohibido introducir voluntariamente programas, virus, macros o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la Empresa o de terceros. El trabajador tendrá la obligación de no desactivar los anti-virus y sus actualizaciones que la Empresa ponga a su disposición para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

Uso de ordenadores personales:

1. Cada trabajador de la Empresa habrá de tener presente en todo momento las siguientes 5 reglas básicas para el uso de su ordenador personal:

    - No deben abrirse mensajes electrónicos de origen desconocido.
    - No deben aceptarse documentos ni archivos provenientes de desconocidos o que tengan un origen poco fiable.
    - No deben escribirse los números secretos en ningún documento del disco duro del PC ni en las ventanas de recordatorio del PC.
    - No deben utilizarse claves o contraseñas triviales o de fácil deducción.
    - No deben facilitarse datos personales o financieros si no se está en un entorno seguro y con proveedores de confianza.

2. El uso que el trabajador hará de los medios puestos a su disposición por la Empresa (ordenador, impresoras, etc.) será únicamente tendente a la realización de los trabajos y/o actividades reflejadas en el contrato de trabajo o que hayan sido encargadas expresamente por los responsables de la misma.

3. El ordenador es un bien propiedad de la Empresa, que en cualquier momento puede ser utilizado o revisado por otros trabajadores. La información contenida en el ordenador es de la Empresa y el trabajador no la utilizará nunca para fines personales o particulares.

Uso de otros equipos personales: Palm's, Memory Sticks, etc:

1. El uso dentro de los locales y oficinas de la Empresa por parte de cualquier trabajador de agendas electrónicas (Palm's, etc.), Memory Sticks o cualquier otro equipo electrónico susceptible de ser conectado a la red o de almacenar información electrónicamente deberá ser previamente autorizado por parte de los responsables de la Empresa.

Navegación en Internet:

Navegar por Internet tiene muchas ventajas, pero es importante tener bien protegido el ordenador. Según la importancia de la información que éste contenga, el trabajador de la Empresa al conectarse a Internet, además de cuidar los aspectos básicos de protección del ordenador, deberá seguir todas las indicaciones de la Empresa y aplicar todas o alguna de las siguientes medidas de seguridad, medidas de prudencia para una navegación más segura:

- No dejar desatendido su ordenador mientras esté conectado.
- Apagar el ordenador siempre que no se esté utilizando.
- Navegar por sitios web conocidos.
- No aceptar la ejecución de programas cuya descarga se active de forma no solicitada.
- No compartir discos o impresoras en Internet.
- Conocer la existencia de hoaxes (virus engañosos).
- Además, otro tema importante para una navegación segura es la protección de datos, ya sean personales, de contacto, financieros o de cualquier otro tipo. Para ello, el trabajador de la Empresa deberá:
- Mantener el anonimato en cuanto a datos personales y profesionales en los formularios de petición de datos de sitios web. Proporcionar datos reales sólo cuando sea imprescindible para obtener un servicio (por ejemplo, cuando tenga que recibirse un envío postal).
- Introducir datos financieros sólo en sitios web seguros (en concreto, el uso de PIN bancarios debe restringirse únicamente a la página del banco o caja que ha originado el PIN siempre que esté en páginas con el protocolo HTTPS).
- No utilizar las mismas contraseñas en los sistemas de alta seguridad que en los de baja seguridad.
- Extremar el cuidado al proporcionar información sensible a solicitantes no autorizados o cuya identidad no pueda ser verificada fehacientemente.
- No proporcionar datos personales en sitios web que no garanticen el cumplimiento de la legislación vigente (LOPD) y/o que no tengan un sitio web seguro (SSL).
- Al usar ordenadores compartidos con otros trabajadores, extremar el cuidado de las medidas de protección básicas: desconexión de sesiones, etc.

- La Empresa dotará de acceso a Internet a todos los trabajadores que dispongan de un puesto de trabajo con conexión a la red corporativa cuando así lo requieran para sus funciones.
- Está prohibido expresamente el uso de Internet para finalidades personales en horario de trabajo. El trabajador conoce que las conexiones a Internet se registran, ya que únicamente se pueden utilizar para finalidades relacionadas con el trabajo desarrollado en la Empresa.

Uso del correo electrónico:

1. Los trabajadores de la Empresa podrán utilizar el correo electrónico, la dirección de e-mail, con libertad razonable, para el desempeño único y exclusivo de las actividades propias de su función laboral en su puesto de trabajo.
2. Siempre que se precise realizar un uso de estos medios que exceda el habitual, envíos masivos o de especial complejidad, utilizarán los cauces adecuados, de acuerdo con los responsables de la Empresa, para no causar daños en el desarrollo normal de las comunicaciones y en el funcionamiento de la red corporativa.
3. Con carácter general, los trabajadores de la Empresa no podrán utilizar el correo electrónico para fines particulares, ya que el correo electrónico es un bien propiedad de la Empresa que se facilita únicamente para poder realizar las tareas laborales. Asimismo, el correo electrónico del trabajador podrá ser consultado por cualquier otro empleado para el correcto desarrollo de la actividad de la Empresa.
4. Bajo ningún concepto podrán los trabajadores utilizar el correo electrónico que la Empresa pone a su disposición para realizar envíos masivos de mensajes ni realizar cualquier tipo de envío, sin relación alguna con el desempeño profesional y que interfiera las comunicaciones del resto de trabajadores o perturbe el normal funcionamiento de la red corporativa.
5. El incumplimiento de estas normas determinará la utilización por la Empresa de las restricciones que considere oportunas en la utilización de estos medios y, en su caso, la aplicación del régimen disciplinario legalmente aplicable.
6. Cuando existan indicios de uso ilícito o abusivo por parte de un trabajador, la Empresa realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoria en el ordenador del trabajador o en los sistemas que ofrecen el servicio. Su realización será siempre en horario laboral, se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de otro trabajador de la Empresa.

Uso de programas de ordenador:

1. El trabajador deberá mantener siempre actualizados tanto el sistema operativo como los programas instalados por la Empresa en su ordenador, con las correcciones recomendadas por los fabricantes, que habitualmente van actualizando sus programas a medida que, a través del uso masivo de los mismos, se detectan errores.
2. Los fabricantes también suelen ir ampliando las medidas de seguridad y por ello es importante, tanto para la correcta estabilidad del sistema como para su seguridad ante posibles ataques, ir introduciendo todas las correcciones recomendadas.
3. La Empresa no permite a sus trabajadores la instalación de programas de ordenador. El trabajador se compromete a no utilizar en la Empresa software que provenga de terceros y del que no sea licenciatario legítimo, siendo de su propia responsabilidad el uso o la instalación de programas de ordenador por su propia iniciativa en cualquier terminal de la Empresa, realizado sin la autorización debida por parte de los responsables.

Antivirus:

1. Es de sobra sabido que los virus son programas que se instalan en el ordenador, habitualmente de forma oculta al propietario, con fines maliciosos (por ejemplo, destruir archivos o el disco, propagarse a otros ordenadores o provocar un mal funcionamiento del ordenador), y que las formas en las que se propagan son muy variadas y evolucionan con el tiempo. Para evitar posibles infecciones de virus, el trabajador deberá:

    - Disponer de un software antivirus siempre actualizado (debe actualizarse periódicamente, no basta con que sea más o menos nuevo). Para actualizarlo, deben consultarse las instrucciones del fabricante del programa, siguiendo las indicaciones de los responsables de la Empresa.
    - Verificar los documentos recibidos del exterior (vía correo electrónico, disquete, descargas, etc.) con el antivirus.
    - Ejecutar sólo aquellos programas de los que conozca su origen, tenga plena garantía y en ningún caso vulneren la propiedad intelectual.

2. El correo electrónico es una de las vías más importantes de transmisión de virus, ya que no garantiza el origen del envío, hecho que conlleva algunos riesgos inherentes, como el posible acceso al contenido del correo por parte de terceros, la suplantación del remitente o el envío de virus. Para utilizarlo corriendo los riesgos mínimos, el trabajador habrá de seguir las siguientes medidas:

    - No ejecutar directamente los ficheros anexos a un correo electrónico, es mucho más seguro extraerlos previamente a un directorio del ordenador y analizarlos con el antivirus.
    - En caso de recibir correos no solicitados será necesario la confirmación del envío con el remitente del mismo o borrar el mensaje.
    - No participar en correos encadenados. Existe un gran número de correos que contienen falsas noticias acerca de virus. Las casas comerciales y centros de alerta legítimos tienen como norma redirigir a servidores web donde dan información de forma fiable y detallan las acciones a tomar. No deben reenviarse correos indiscriminadamente.
    - Nunca se desactivará el antivirus del ordenador.

Conexiones inalámbricas:

Ningún trabajador podrá activar o desactivar conexiones inalámbricas que permitan o impidan acceder a la red local de la Empresa sin el consentimiento expreso y por escrito de los responsables.

Fdo.

Glosario

- **RAID**: En informática, el acrónimo RAID (originalmente del inglés Redundant Array of Inexpensive Disks, 'conjunto redundante de discos baratos', en la actualidad también de Redundant Array of Independent Disks, 'conjunto redundante de discos independientes') hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor throughput (rendimiento) y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.

- **SAI**: Un Sistema de Alimentación Ininterrumpida, o más conocido por sus siglas en inglés UPS (Uninterruptible Power Supply: 'suministro de energía ininterrumpible') e incorrectamente generalizado como No break, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de las UPS es la de mejorar la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de Corriente Alterna. Las UPS dan energía eléctrica a equipos llamados cargas críticas, que pueden ser aparatos médicos, industriales o informáticos, que como se ha dicho antes, requieren tener siempre alimentación y que ésta sea de calidad debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

- **Keycatchers**: És un keylogger por hardware, keylogger (deriva del inglés: Key (Tecla) y Logger (Registrador); registrador de teclas) es una herramienta de diagnóstico utilizada en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de internet.

- **BIOS**: El sistema Básico de entrada/salida Basic Input-Output System (BIOS) es un código de software que localiza y carga el sistema operativo en la R.A.M.; es un software muy básico instalado en la placa base que permite que ésta cumpla su cometido. Proporciona la comunicación de bajo nivel, el funcionamiento y configuración del hardware del sistema que, como mínimo, maneja el teclado y proporciona salida básica (emitiendo pitidos normalizados por el altavoz de la computadora si se producen fallos) durante el arranque. El BIOS usualmente está escrito en lenguaje ensamblador. El primer término BIOS apareció en el sistema operativo CP/M, y describe la parte de CP/M que se ejecutaba durante el arranque y que iba unida directamente al hardware (las máquinas de CP/M usualmente tenían un simple cargador arrancable en la ROM, y nada más). La mayoría de las versiones de MS-DOS tienen un archivo llamado "IBMBIO.COM" o "IO.SYS" que es análogo al CP/M BIOS.