



Políticas de la Seguridad de la Información

1 introducción

Cada año aumenta el número de ataques y de incidencias informáticas que generan fuertes pérdidas económicas y de imagen a las empresas de todo el mundo, llegando incluso a provocar la quiebra de muchas de ellas.

De los millones de incidencias provocados por la falta de seguridad informática que se producen anualmente, se estima que sobre el 80% de estas están generadas por actuaciones erróneas de sus usuarios internos, ya sea por malicia o desconocimiento.

Para evitar en gran parte este tipo de incidencias, en centribal consideramos que una parte esencial para la prevención es la educación de los usuarios. Ellos son una parte esencial tanto para el correcto funcionamiento y crecimiento de la empresa, como para asegurar que los procesos en seguridad informática se cumplan.

Esta pequeña guía es un referente que intenta aportar un código de buenas prácticas a los usuarios de cualquier empresa, para evitar, en la medida de lo posible, un riesgo que en muchas ocasiones es fácilmente salvable. Para que pueda llegar de forma entendible y clara a todos los usuarios, sea cual sea su conocimiento informático, creamos esta guía con un léxico nada técnico y sencillo, de forma que independientemente de la educación recibida por el usuario, pueda llevar a la práctica este conjunto de recomendaciones.

Pocas personas, no pertenecientes al mundo de la informática, dan la verdadera importancia que tiene la seguridad en los sistemas electrónicos, pero igual que la educación vial se considera básica y necesaria, la educación en la seguridad informática empresarial se hace cada vez más necesaria dado el incremento de las nuevas tecnologías en nuestras vidas diarias y en especial del mundo empresarial.

1.1. Seguridad Informática

Antes de entrar en materia, creemos conveniente dar una pequeña definición de qué es la seguridad informática. En una definición básica podría decirse que la seguridad informática es la acción directa por la que los técnicos informáticos aseguran que los

Always On Systems Hispania S.L

recursos del sistema de la información de una entidad empresarial se utilizan de manera correcta y en base a lo que se pre-definió previamente, asegurando que el acceso a la información allí contenida, así como su modificación y transmisión, sólo sea accesible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

2. Objetivos

El presente Código de Buenas Prácticas tiene por objeto recopilar los principales aspectos y normas que se deben conocer y aplicar para que todos los usuarios sean conscientes de la necesidad de mantener un nivel de seguridad adecuado en todos los sistemas de información que tengan que utilizar en el desempeño de sus funciones en el ámbito de las competencias laborales, sin perjuicio del cumplimiento del resto de las obligaciones que les pudiera ser de aplicación.

El establecimiento del presente Código de Buenas Prácticas permitirá, además, que los usuarios conozcan sus obligaciones en relación con el uso de los datos personales y concienciarnos de la necesidad de establecer normas y reglas claras que eviten determinadas prácticas y ayuden a garantizar los derechos fundamentales de los clientes en relación con el uso de sus datos personales.

Asimismo, incidirá en el correcto uso de los medios y sistemas de información, consecuencia de la necesidad de optimizar la utilización de dichos medios, y de evitar los efectos de un uso inadecuado.

3. Ámbito de aplicación

Este Código de Buenas Prácticas se aplicará a todos los usuarios de la empresa, sin perjuicio del cumplimiento del resto de las obligaciones que pudiera serles de aplicación.

El presente Código de Buenas Prácticas se aplicará al uso de cualquier sistema de información de la empresa, incluyéndose ordenadores personales, medios de transmisión de información, o equipos de cualquier otro tipo que se pueda poner a disposición de los usuarios.

4. Definiciones

Se determina necesario aclarar y especificar un glosario de términos básico, para que el lector de esta guía pueda entender fácilmente los conceptos nombrados.

Usuario: Son todos los profesionales que prestan sus servicios en la empresa, así como el personal de empresas externas que desarrollen tareas, permanente u ocasionalmente para la empresa.

PSI: Políticas de Seguridad de la Información

Always On Systems Hispania S.L

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

Malware: también conocido como badware, es el código o aplicación que tiene como objetivo infiltrarse o dañar los dispositivos informáticos o la información contenida.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación de la información de carácter personal, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Spam: correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada, enviada masivamente a las direcciones de correo electrónico.

Phishing: o suplantación de identidad es una técnica mediante la cual el atacante nos entrega una dirección web aparentemente válida, pero que tras pulsarla nos muestra una página clonada e idéntica a la real, salvo que el enlace real está alterado. El objetivo de este tipo de ataques es obtener nuestras credenciales, por ejemplo la de la cuenta bancaria.

Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Sistema de información: Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.

Incidencia: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

5. Principios básicos

La información y los sistemas informáticos e infraestructuras utilizados en el ámbito laboral, deben utilizarse aplicando las medidas y normas que permitan alcanzar los niveles de seguridad necesarios para garantizar su protección, salvaguardando la seguridad de la información, y mejorando de esta forma la calidad de los servicios prestados a los clientes.

La empresa proporciona acceso personalizado a los sistemas de información, ya sean físicos o lógicos. Estos medios son instrumentos de trabajo y su objeto es aportar rapidez, eficacia y eficiencia en la prestación de los servicios y ayudar a los usuarios en el desarrollo de sus funciones.

6. Leyes vigentes

Cada país dispone de una legislación vigente en materia de seguridad y protección de los datos de carácter personal. Para el desarrollo de esta guía usaremos de base las leyes españolas en esta materia, ya que disponen de una amplia base en el cumplimiento de la protección de la privacidad. Cada empresa y usuario deberá adaptar esta normativa a la legislación vigente en su país, siendo considerada la española como genérica y beneficiosa para todo el mundo en esta materia.

Reglamento general de protección de datos, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas, y especialmente de su honor e intimidad personal y familiar.

Esta Ley establece que el responsable del fichero, y en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y que eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Se determina que reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos especialmente protegidos, entre otros, el tratamiento de datos relativos a la salud de las personas. De esta forma se exige un reforzamiento en las medidas de seguridad, no solo técnicas sino también en las medidas organizativas y en los requisitos que tendrán que cumplir las personas que intervengan en el uso y tratamiento de estos datos.

El Real Decreto 994/99, de 11 de Junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (Reglamento Seguridad), desarrolla el precepto de la GRPD citado anteriormente y establece las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos, los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervienen en los tratamientos, sujetos al régimen de aplicación de la GRPD.

Los usuarios están obligados a cumplir todas las medidas de seguridad establecidas, así como los requisitos y condiciones que se deban aplicar de acuerdo a las normas y procedimientos existentes y con los controles de seguridad que se encuentren establecidos, haciendo uso de la información a la que tengan acceso sólo para los fines relacionados con el desarrollo de sus competencias y para la realización exclusiva de su trabajo y funciones. Los usuarios podrán ser responsables del incumplimiento de sus obligaciones de conformidad con el régimen jurídico aplicable.

A continuación se citan algunos de los principios que se deberán tener en cuenta en el tratamiento de datos personales:

Always On Systems Hispania S.L

No podrán registrarse datos de carácter personal en ficheros que no reúnan las condiciones de seguridad establecidas en la legislación vigente.

Todas las personas que intervengan en cualquier fase del tratamiento de datos de carácter personal están obligadas al secreto profesional respecto de los mismos y al deber de guardarlos.

Los usuarios que tengan acceso a ficheros con datos de carácter personal deberán extremar las precauciones a fin de evitar cualquier salida de información de los cauces legales establecidos.

En este sentido, se deberá evitar cualquier salida de información a terceros que no esté prevista en la normativa aplicable, ya sea por medio de soporte en papel, correos electrónicos o por cualquier otro tipo de medio o mecanismo, electrónico o no.

Únicamente con la autorización pertinente se podrá comunicar datos a terceros. En cualquier caso, la posible cesión de datos deberá constar en la disposición de creación del fichero, ya sea porque así lo establezca una ley o porque la cesión se realice con consentimiento del interesado.

En el caso de que la cesión de datos esté prevista en la normativa aplicable, será necesario tener en cuenta todas las medidas de seguridad aplicables, respetando las normas establecidas al efecto. En aquellos casos en que sea posible, el usuario debe solicitar la entrega de información disociada, de forma que los datos no puedan ser asociados a identidad alguna, siendo totalmente anónimos.

Los usuarios que requieran para el desarrollo de sus funciones la generación de ficheros temporales con datos de carácter personal en sus ordenadores, serán responsables de su destrucción cuando dejen de ser necesarios para la finalidad que se generaron. En cualquier caso, será necesario que a estos ficheros se les aplique las medidas de seguridad pertinentes.

Cuando un soporte, listado o documento contenga datos personales y vaya a ser desechado, será necesario adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada o impresa en los mismos.

Los usuarios que requieran realizar tratamientos de datos de carácter personal fuera de los sistemas de información de la empresa, deberán solicitar el permiso pertinente que en caso de considerarse justificado y necesario, deberá contener las medidas necesarias para proteger esa información.

Cualquier incidencia o anomalía que pudiera afectar a la seguridad de los datos personales deberá ser comunicada al departamento técnico.

Always On Systems Hispania S.L

Los accesos a los sistemas de información podrán ser monitorizados y registrados para auditar el uso de los mismos, en cuanto a la auditoría del cumplimiento de las medidas de seguridad de datos de carácter personal y al registro de los accesos a dichos datos.

7. Pautas generales

La empresa provee a los usuarios de los recursos técnicos e informáticos necesarios para el correcto desarrollo de sus funciones y actividades. Los equipos informáticos y la información no deberán ser utilizados en ningún momento para fines particulares.

Los usuarios deben acceder exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad y únicamente a la información a la que esté autorizado.

Debe prestarse atención al contenido de los ordenadores personales, evitando almacenar en ellos documentos que contengan datos personales sin las debidas medidas de seguridad.

Cada vez que se utilicen dispositivos de almacenamiento externo, debe permitirse la comprobación del estado de los archivos contenidos por la aplicación de antivirus.

Deberá evitarse dejar información confidencial desatendida en el puesto de trabajo, ya sean CDs, listados o información visible en la misma pantalla del ordenador, documentos en papel de clientes y proveedores, o cualquier otro dispositivo de almacenamiento. La información confidencial o relativa a datos personales se deberá almacenar siempre en lugares seguros con las debidas medidas de seguridad y bajo llave.

En periodos vacacionales prolongados o de más de 3 días laborales, debe informarse al departamento técnico para que pueda inhabilitar la cuenta de usuario durante ese periodo.

Los usuarios serán responsables de la custodia y respaldo de toda la información que almacenan localmente en discos duros de su ordenador y en su puesto de trabajo.

Está prohibido el uso de aplicaciones de videoconferencia, mensajería y de chateo con aplicaciones no autorizadas por la empresa y/o con cuentas ajenas a la entidad empresarial.

No pinchar en enlaces obtenidos por correos electrónicos que puedan generar dudas de su autenticidad.

Únicamente se podrá distribuir información empresarial a las personas autorizadas y se deberá evitar que las personas que no deban tener acceso a esa información puedan llegar a ella o conocerla.

8. Cumplimiento del presente Código

Todos los usuarios de la cualquier entidad empresarial deberán cumplir el presente Código de Buena Conducta. El incumplimiento de cualquier de los puntos de comportamiento contenidas en el presente Código podrá dar lugar a la correspondiente responsabilidad disciplinaria, además de las correspondientes aplicaciones de las normas reguladoras del régimen jurídico propio del usuario.

Es importante entender que la empresa que incumple este código es la responsable directa de los prejuicios que puedan ocasionar sus usuarios finales por sus malas prácticas, si bien es cierto que, una vez depurada la responsabilidad, el autor causante de dicha problemática será el último responsable, pudiendo la empresa exigir responsabilidades acordes a los daños causados por sus malas actuaciones.

9. Políticas de usuario

Los usuarios deben ser en todo momento personales y nunca ser usados por más de una persona. Esto es algo imprescindible de cara al No-Repudio, es decir, la depuración de responsabilidad de las acciones de los usuarios.

Pueden existir listas de distribución o grupos genéricos, por ejemplo por departamentos, pero nunca debe ser transmitida o realizada ninguna acción directa con este tipo de cuentas.

Un claro ejemplo son las cuentas de correo electrónico. Muchas empresas disponen de cuentas como info@empresa.com, rrhh@empresa.com, marketing@empresa.com, etc.

En muchas ocasiones estas cuentas son imprescindibles, pero siempre deben disponer de la firma del usuario final de cada uno de los departamentos.

Otra buena práctica, es usar este tipo de cuentas genéricas como mail de recepción o listas de distribución, de forma que el mail llegue a todo el departamento involucrado, pero cada usuario responda con una cuenta personal y única.

EN la definición de las políticas de usuario incorpora el **nombre corporativo**, creado con la primera letra del nombre y el primer apellido. *Por Ejemplo Ivan Palmieri seria ipalmieri@centribal.com*

Además, en fase de definición de la cuenta de correo siempre tendremos esta formula <nombre.corporativo>+@+<dominio.compaña> *por ejemplo* ipalmieri@centribal.com

En caso de nombres corporativos repetidos se definirá al uso la posibilidad de modificar dicha política a discreción del responsable de seguridad.

10. Políticas de contraseñas

Las aplicaciones y servicios requieren la utilización de una cuenta de usuario y una contraseña que identifica al usuario de manera única y le permite el acceso con los privilegios oportunos. Las cuentas de usuario y contraseñas no son transferibles y no se deberán prestar a otros usuarios bajo ningún concepto, independientemente del cargo que nos lo solicite, ya sea el gerente, el administrador de la red o cualquier otro. Este es el mecanismo utilizado para verificar la identidad de los usuarios en el acceso a los sistemas de información empresarial, y el uso de estos nos hacen responsable directo de su uso.

Son los usuarios quien deben mantener estas credenciales en secreto, informando inmediatamente al departamento técnico en caso de pérdida o compromiso de la misma, para que se modifique lo antes posible.

En todos los servicios y sistemas, el uso de un usuario y contraseña se hacen necesarios. Para garantizar que esta sea realmente segura, la contraseña debe cumplir una serie de requisitos.

Estos requisitos deben de estar regulados por políticas de grupo por parte de los administradores del sistema. Si no es el caso, debemos entender que ante cualquier incidente, seremos responsables ante cualquier fallo o delito causado por nuestras cuentas, por lo que debemos tomar conciencia de la importancia de disponer de una alta seguridad.

Las contraseñas deben de ser robustas:

Para que nuestras contraseñas sean fuertes, difíciles de adivinar o calcular, debemos cumplir las siguientes directrices, definiendo tales contraseñas según la definición de INCIBE “contraseñas robustas”:

- deben contener al menos ocho caracteres;
- deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);
- no deben contener los siguientes tipos de palabras:
 - palabras sencillas en cualquier idioma (palabras de diccionarios);
 - nombres propios, fechas, lugares o datos de carácter personal;
 - palabras que estén formadas por caracteres próximos en el teclado;
 - palabras excesivamente cortas.
- tampoco utilizaremos claves formadas únicamente por elementos o palabras que puedan ser públicas o fácilmente adivinables (ej. nombre +

- fecha de nacimiento);

Las políticas aplicadas para la generación y el mantenimiento de las credenciales de acceso de los empleados son políticas locales definibles solo por un usuario administrador, están configuradas con las siguientes características:

- mínimo 8 caracteres
- combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);
- caducan cada 2 meses
- el sistema impide el uso de la misma contraseña utilizada anteriormente en un historial de 12 contraseñas

Directiva	Configuración de seguridad...
Almacenar contraseñas con cifrado reversible	Deshabilitada
Exigir historial de contraseñas	12 contraseñas recordadas
La contraseña debe cumplir los requisitos de complejidad	Habilitada
Longitud mínima de la contraseña	8 caracteres
Vigencia máxima de la contraseña	60 días
Vigencia mínima de la contraseña	0 días

11. Acceso a la red empresarial

Para el correcto desempeño de la actividad, todos los usuarios dispondrán de unas credenciales de acceso (usuario y contraseña), que se ajustarán a las normas y procedimientos establecidos por el administrador de Sistemas o en último caso por el responsable de la Seguridad Informática. El acceso a cualquier recurso de la red interna debe exigir la presentación de credenciales de acceso válidas, correctas y vigentes. La custodia de dichas credenciales es en todo momento responsabilidad de cada usuario.

El acceso a los recursos e información contenidos en la red empresarial desde dispositivos externos, debe realizarse mediante métodos seguros y encriptados, principalmente mediante comunicación directa por redes VPN seguras.

Para acceder a los recursos de la red empresarial, sólo se usarán aquellas conexiones que hayan sido implantadas corporativamente, no estando permitida la utilización de otros medios de conexión sin la debida autorización.

La instalación de aplicaciones no autorizadas en los equipos empresariales, genera una sanción administrativa de carácter medio al usuario responsable de dicha instalación. El departamento técnico tiene la potestad de borrar de inmediato, cualquier aplicación que considere perjudicial para el correcto funcionamiento de las redes informáticas de la empresa.

El acceso a los recursos empresariales, deben siempre ser accedidos desde dispositivos autorizados por el departamento técnico, ya sean portátiles, tablets, dispositivos móviles u otros. En ningún caso usaremos dispositivos personales, ni accederemos a las redes de la empresa, tanto cableadas, como inalámbricas, desde dispositivos que el departamento técnico no pueda controlar. El uso de estos dispositivos debe ser siempre mediante redes personales, como por ejemplo 3G.

El usuario nunca debe ejecutar programas, archivos u otro tipo de aplicaciones que haya obtenido mediante medios personales, ya sea a través de dispositivos de almacenamiento externos, como mediante el correo personal, chats u otros métodos de mensajería.

Una vez realizado el acceso a los dispositivos y redes empresariales, nunca deben usarse dispositivos de almacenamiento no autorizados por el departamento técnico, y siempre se realizará con dispositivos empresariales, nunca personales, ya sean pendrive, discos duros o cualquier otro dispositivo de almacenamiento.

El usuario es responsable directo de la pérdida de la información que se produzca en los dispositivos puestos a su alcance por parte de la empresa. El departamento técnico sólo garantiza la realización de las copias de seguridad de los medios de red que pone al usuario para el almacenamiento de todos los datos empresariales que deban ser salvaguardados. Es por ello aconsejable, que tras finalizar la jornada laboral, todo usuario que disponga de nueva información de importancia empresarial, pase esa información a las unidades de red, no dejándola en su perfil de usuario, como en el escritorio del equipo o en los documentos locales del usuario.

12. Uso de acceso a Internet

Debido a la necesidad de optimizar los recursos disponibles en la empresa y para obtener mayor información con la que poder ejercer nuestra actividad profesional, la utilización del acceso a Internet debe responder a fines estrictamente profesionales. Únicamente podrán acceder a Internet los usuarios que dispongan de cuentas de acceso a estos efectos. Las cuentas de acceso son personales e intransferibles y cada usuario deberá autenticarse únicamente con la cuenta de usuario que le haya sido asignada.

Siempre que sea posible, se preferirá el acceso a sitios de Internet que cuenten con medidas de seguridad adicionales, como por ejemplo el cifrado de la información

mediante protocolos de seguridad como SSL, siendo el caso de las páginas web que comienzan por https, en vez de http.

Se recomienda evitar las descargas de información que no proceda de fuentes confiables, conocidas y seguras. Nunca deben descargarse ningún tipo de archivo ejecutable, es decir con extensiones .exe, .bat, .com, .rar, .zip, etc., ya que estos son los mayores contenedores de virus. En muchas ocasiones, estas extensiones van ocultas, teniendo que marcar la opción de mostrar extensiones de archivos en nuestros equipos.

Un claro ejemplo es el archivo imagen.JPG.exe. Este es un archivo ejecutable capaz de contener un virus informático. La extensión real del archivo es .exe (programa ejecutable), pero si no disponemos de la opción de visualizar extensiones de archivo, veremos tan solo como nombre imagen.JPG, pensando que es una imagen, incluso con el icono característico de los archivos de imagen JPG.

Aunque no se limite técnicamente la capacidad de descarga de archivos de audio y vídeo, los usuarios deberán tener en consideración que la descarga de estos archivos, y la de otros contenidos similares, puede ir en detrimento del correcto funcionamiento de los recursos informáticos, y por ello limitarán la descarga y la reproducción de dichos archivos al ámbito estrictamente profesional. Además estos deberán ser descargados, en caso necesario, de fuentes conocidas y fiables. En ningún caso se usarán redes P2P que no dispongan de garantía alguna de seguridad, como Emule, BitTorrent, etc.

No está permitido el acceso a páginas web cuyo contenido pueda resultar ofensivo, atentar contra la dignidad humana, dispongan de contenidos ilegales, eróticos y/o pornográficos, de temática hacker y cualquier otro que consideremos de grave riesgo para la seguridad de nuestro equipo.

Queda prohibida para los usuarios la descarga de programas y aplicaciones necesarias para la realización de las tareas profesionales. Estas deben ser responsabilidad del departamento técnico, quien se encargará de descargar las aplicaciones de fuentes validadas e instalar correctamente la aplicación en los equipos de los usuarios. Esta es parte de la función de los técnicos informáticos, no de otros usuarios.

No se utilizarán navegadores o programas, ya sean de correo electrónico o de otro tipo, distintos a los instalados a tal efecto por el departamento técnico. No se utilizarán versiones diferentes, ni se modificará la configuración en los aspectos relacionados con la seguridad. Ante cualquier duda, debe consultarse con el departamento técnico.

Los usuarios deberán observar, antes del uso profesional de cualquier información o documento obtenido de Internet, si el uso de dicha información está restringido por las leyes que protegen la propiedad intelectual o industrial. En particular, en lo relativo a programas informáticos descargados de Internet.

13. Uso y mantenimiento de programas informáticos

No se permite la instalación de “software” o programas en los ordenadores. Si fuera necesaria su instalación para disponer de un correcto desarrollo de la actividad laboral, deberá solicitarse al responsable correspondiente para que lo gestione. Este tipo de aplicaciones deben ser siempre descargadas de fuentes validadas, siendo uno de los mayores peligros potenciales para la seguridad informática, mediante todo tipo de código o programas ocultos maliciosos, especialmente el spyware y el malware.

Los procesos de instalación y de uso de programas no gratuitos, deben tener en cuenta el número de licencias de instalación y/o utilización del que dispone la empresa. No será posible hacer uso de ningún programa del que previamente no se haya adquirido la licencia correspondiente, constituyendo un delito que el usuario final deberá asumir en caso de incumplimiento.

Las tareas de instalación de aplicaciones o programas informáticos, deben siempre ser realizadas por el departamento técnico, quien podrá con conocimiento previo, ejecutar las medidas de seguridad oportunas y realizar una monitorización adecuada.

Los usuarios deben evitar el uso, instalación o distribución de programas que no hayan sido aprobados para su utilización dentro de los sistemas empresariales, puesto que puede ser fuente de ataques e incidentes en la seguridad de la red, así como provocar el incumplimiento de las leyes que ejercen las licencias del producto.

14. Control de incidencias

Todos los usuarios deben informar al departamento técnico de los incidentes que puedan tener impacto, directo o indirecto, en la seguridad de los activos de la empresa. Deben comunicarse todos los detalles observados que hayan llevado al usuario a sospecha, prestando asimismo la colaboración que pueda ser precisa al departamento de técnico para la resolución de dicha incidencia.

En caso de que un usuario cometa un error que comprometa la seguridad de los dispositivos o información empresariales, este debe avisar urgentemente al departamento técnico para que éste pueda solventarlo lo antes posible, minimizando en la medida de lo posible el efecto de dicha acción.

Debido a la naturaleza dinámica y cambiante de los requisitos que han de satisfacer y las nuevas amenazas y vulnerabilidades, las aplicaciones informáticas han de mantenerse siempre actualizadas, para lo cual resulta imprescindible la colaboración de todos y cada uno de los usuarios. En el marco de esta colaboración, los usuarios comunicarán a su respectivo departamento técnico cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que hubieran podido observar, así como cualquier mejora que se estime adecuada.

Always On Systems Hispania S.L

La función de mantener actualizados los sistemas y aplicaciones corporativas es responsabilidad directa del departamento técnico, quien debe contar con la infraestructura y medios necesarios para dicha tarea, siempre una vez validadas previamente dichas actualizaciones. Al ser esto un coste que muchas entidades empresariales no pueden o quieren asumir por desconocimiento, la participación de los usuarios se hace imprescindible en muchas ocasiones, por lo que actualizaciones de gran riesgo, como la de los sistemas antivirus y del sistema operativo de los usuarios, dependen de estos directamente, al no disponer el departamento técnico de costosas soluciones centralizadas.

Cuando una incidencia y/o deficiencia pudiera causar un elevado impacto en el funcionamiento del servicio, los usuarios, de acuerdo siempre con el departamento técnico, podrán adoptar las medidas de urgencia que se estimen oportunas. El detalle de los hechos acontecidos y de las medidas adoptadas se deberá poner en conocimiento de quien corresponda a fin de que éste tome las decisiones oportunas y se haga cargo de las responsabilidades en caso de ser necesarias.

15. Control de virus informáticos y demás software malicioso

Un virus es un programa de ordenador que produce acciones nocivas en los sistemas de la información y en el sistema en general.

La inclusión de un virus informático se puede producir por la ejecución de un programa contaminado o la utilización de un fichero infectado, incluyendo el uso de dispositivos externos de almacenamiento, correos electrónicos, páginas web infectadas con códigos maliciosos, etc.

Todos los puestos de la empresa deben disponer de mecanismos adecuados para el control de software malicioso y han de permanecer activados y actualizados. No está permitida la desactivación de dichos mecanismos y aplicaciones.

No obstante, para reducir el riesgo de propagar una infección en la red, deberá procederse con la máxima cautela antes de ejecutar un archivo procedente de cualquier fuente, incluso aquellas fuentes consideradas de confianza, dado que pueden haber sido suplantadas. En ningún caso se abrirá un archivo, mail, página web u otro cualquiera, que nuestros sistemas de seguridad, principalmente antivirus, nos indique que tiene un potencial peligro, ya sea alto o bajo, aunque este sea de una fuente conocida. En estos casos debe avisarse de inmediato al departamento técnico para que tomen las medidas oportunas.

Ante la sospecha de una infección por virus, se deberá comunicar la incidencia al departamento de técnico de inmediato, ya que este puede dispersarse por toda la red empresarial.

Always On Systems Hispania S.L

16. Uso de impresión

El uso de los dispositivos de impresión de la empresa, queda restringido exclusivamente para la impresión de documentación empresarial

Todo documento enviado a impresión, es responsabilidad directa del usuario, debiendo estar pendiente de dicha impresión y retirarlo lo antes posible, además de custodiar los datos contenidos que estén en proceso.

Todo documento que permanezca al finalizar la jornada laboral, debe ser inmediatamente destruido, con los medios necesarios para garantizar la recomposición de los datos contenidos.

En caso de mal funcionamiento de los sistemas de impresión, el usuario debe informar al departamento técnico para que paralice el proceso de impresión.

17. Uso del servicio de correo electrónico

El correo electrónico, únicamente se utilizará por aquellos usuarios a los que se les haya previsto de una cuenta de correos para uso el profesional que van a desempeñar, quedando totalmente prohibido el uso de cuentas personales en todos los dispositivos empresariales.

Debido a la necesidad de monitorización y auditoría del departamento técnico para mantener un nivel en la seguridad informática, debe prohibirse la utilización del correo electrónico para todas las actividades personales, en especial aquellas con contenidos de privacidad del usuario u otras personas.

Debe prohibirse el uso del correo electrónico para la difusión masiva de archivos no profesionales que pueda poner en peligro el sistema informático empresarial ya sean felicitaciones, mensajes en cadena, y en especial aquellos que impliquen el envío de archivos de gran tamaño capaces de colapsar y ralentizar la red.

Cuando se reenvíen correos electrónicos que fueron dirigidos a varios destinatarios, se evitará incluir las direcciones de los destinatarios del mensaje original en el cuerpo del mensaje redirigido, borrando esta información antes de enviarlo.

Con carácter general, debe evitarse el envío de datos de carácter personal mediante correo electrónico. En caso de ser necesario tal envío, los datos deberán ser cifrados mediante el uso de aplicaciones de cifrado o certificados digitales que debe proporcionar la empresa.

Al recibir un nuevo mensaje de correo electrónico, antes de abrirlo se deberán analizar las cabeceras, intentando detectar si es un mensaje de procedencia dudosa o desconocida para descartar de inmediato. En caso de dudas razonables, se deberán borrar sin abrir los mensajes, o ante dudas, consultar con el soporte técnico, ya que podrían contener virus que afectasen a la información de toda la empresa.

Para evitar el correo masivo no solicitado (spam), como regla general sólo se debe dar nuestra dirección de correo electrónico a personas conocidas o que permitan ampliar y desarrollar nuestra actividad laboral. No se debe introducir la dirección de correo electrónico de la empresa en foros o páginas Web no corporativas o innecesarias para el uso de nuestra actividad profesional. Cuando se reciban correos electrónicos desconocidos o no solicitados no se deben contestar, ya que al hacerlo se reconfirma la existencia de la dirección de correo, siendo un nuevo foco de ataque.

El correo electrónico es indudablemente uno de los canales de propagación e infección de malware más utilizados por atacantes debido a su facilidad de difusión, por lo que es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de este medio.

Queda totalmente prohibido participar de forma directa en el reenvío de cadenas de mensajes. Estas no son nunca reales y se usan para almacenar correos electrónicos válidos para el uso de spam o ataques.

El envío o reenvío de correos electrónicos a personal externo de la empresa, debe ir siempre con los destinatarios en copia oculta (campo CCO) para proteger la identidad e intimidad de los receptores.

En las plataformas o páginas web que soliciten autenticación o registro, nunca debe usarse el correo electrónico de la empresa en la medida de las posibilidades. Si esto fuese necesario, jamás se usará junto a ese mail, una contraseña usada en el ámbito empresarial, ya sea la de acceso a la red, aplicaciones corporativas o mucho menos la del propio correo.

Queda terminantemente prohibido el envío de información interna de la compañía (documentos, correos electrónicos, etc...) a correos del ámbito personal para evitar la fuga de información.

18. Uso de dispositivos móviles

Queda prohibido el uso de dispositivos móviles personales para la realización de cualquier tarea empresarial.

Nunca se podrá descargar aplicación alguna en los dispositivos móviles empresariales sin la autorización correspondiente del departamento técnico.

La extracción de los dispositivos móviles del ámbito empresarial, debe contar con el permiso por escrito de la dirección y además informar al departamento técnico, quien tomará las medidas oportunas para garantizar la seguridad de los datos contenidos en caso de pérdida o robo.

La instalación, configuración, modificación o eliminación de software aplicativo sobre los dispositivos móviles es responsabilidad exclusiva del departamento técnico.

En todo dispositivo móvil empresarial, deben usarse redes de comunicación autorizadas por el departamento técnico, ya sean las empresariales o las de la propia compañía telefónica. Nunca nos conectaremos mediante redes inalámbricas abiertas, o que dispongan de una seguridad no controlada por la empresa.

Se considera competencia directa de los usuarios, la realización de las copias de seguridad de los dispositivos móviles una vez hagan uso de él. Los medios utilizados para tal función, así como el destino de la salvaguarda de los datos, deben estar acreditados por el departamento técnico. En caso de no disponer de tales medios, acudir al departamento técnico.

El usuario que pierda por cualquier motivo un dispositivo móvil empresarial o con contenidos personales de la empresa, deberá notificar de inmediato al departamento técnico, quien verá si es pertinente realizar la denuncia correspondiente, o en caso de disponer de tecnología de gestión de movilidad, bloquear el dispositivo móvil, e incluso eliminar la información si contiene un grave riesgo para la empresa o información de alto grado de carácter personal.

Todas las comunicaciones de datos realizadas desde dispositivos móviles que se encuentren fuera de las instalaciones empresariales, deben ir encriptadas mediante certificados digitales de confianza.

No se permite la conexión de los dispositivos móviles empresariales con otros dispositivos no autorizados, ya sean ordenadores personales o incluso de almacenamientos. Por lo tanto también queda restringido el uso de tarjetas de memoria externas personales o no autorizadas por la empresa y analizadas previamente por las aplicaciones de antivirus empresariales.

19. Otros soportes de información

Los usuarios deben ser conscientes en todo momento que la información a proteger no sólo abarca la incluida en los diferentes soportes informáticos, también se deberá prestar especial atención a la información en papel, teniendo mucho cuidado en no dejar documentos en impresoras o en áreas no controladas y de acceso a otro tipo de personal

e incluso externo. La información de carácter personal, nunca deberá permanecer a la vista de terceros no autorizados y fuera de control, ya que esto incumplirá con las leyes de protección de datos, generando graves sanciones económicas.

Debe evitarse el copiado de datos de los sistemas empresariales a cualquier tipo de soporte, como discos compactos, llaves USB, papel, etc., sin la autorización pertinente por escrito y el establecimiento de las medidas de seguridad que procedan.

Nunca un usuario, deberá sacar dispositivos o información de la empresa fuera de la red corporativa, así como datos de carácter personal de otras personas sin previa autorización del departamento técnico, quien deberá previamente garantizar la salvaguarda de dicha información mediante protocolos de encriptación.

20. Uso de certificados digitales y cuidado de claves criptográficas

El avance de los algoritmos criptográficos y de sus aplicaciones, está permitiendo el uso de medios telemáticos para la realización de tareas que tradicionalmente se asociaba a procedimientos manuales, pues estos permiten establecer garantías respecto a la autenticación de la identidad de los usuarios, generando una confidencialidad en las comunicaciones, la integridad de la información, y la depuración de responsabilidades.

Para el uso de tales algoritmos de seguridad, se provee a los usuarios de claves criptográficas, cuya autenticidad e integridad son garantizadas por un tercero de confianza (entidad certificadora), mediante la generación de certificados digitales que acreditan la autenticidad de que quien dice ser, lo es realmente, además de generar unas comunicaciones encriptadas, y por lo tanto más seguras.

En los casos en los que la organización proporcione un certificado digital a los usuarios, deberán observarse las siguientes pautas:

Los usuarios deberán hacerse responsables de salvaguardar sus claves privadas y de cualquier elemento necesario para su acceso, ya sean tarjetas criptográficas, programas específicos, códigos PIN, etc.

Los usuarios comunicarán a la correspondiente entidad prestadora de servicios de certificación y/o registro cualquier compromiso de su clave privada, o de los elementos o códigos utilizados para su acceso, a la mayor brevedad posible, para que se puedan cambiar o tomar las medidas oportunas. Igualmente deberá comunicarse cualquier hecho que pueda hacer sospechar el compromiso de las mismas.

Los usuarios comunicarán a la correspondiente entidad prestadora de servicios de certificación y/o registro cualquier variación de los datos aportados para la obtención del certificado.

Los usuarios deberán respetar las garantías y requisitos suscritos por la entidad empresarial y por la correspondiente Entidad Prestadora de Servicios de Certificación, así como la correspondiente Declaración de Prácticas de Certificación de la Autoridad de Certificación relevante, con respecto a la provisión de servicios técnicos, administrativos y de seguridad necesarios para garantizar la validez de las transmisiones electrónicas emitidas y recibidas.

Una vez finalizada la colaboración laboral del usuario con la empresa, este certificado debe ser inmediatamente eliminado, ya que su uso posterior es considerado como un delito de suplantación de identidad grave.

21. Actualizaciones

Las empresas creadoras de software o programas, ya sean antivirus, sistemas operativos como Windows, y muchas otras, recomiendan que se mantengan actualizados sus productos. Un punto muy importante es que el origen de las actualizaciones sea un sitio de confianza, al poder ser el creador de dichas aplicaciones.

En cuanto a actualizar todo lo que nos ofrecen, esto no es totalmente correcto. En el caso de los antivirus y otras aplicaciones de seguridad es indudable la importancia de mantener los sistemas actualizados.

No ocurre lo mismo en los sistemas operativos y otro tipo de aplicaciones. En muchas ocasiones vemos que la actualización de todos sus parches es realmente perjudicial, tanto para la seguridad de la información, como para el correcto funcionamiento del equipo informático.

Las actualizaciones deben ser administradas por el departamento técnico, quien debe ver la necesidad real de cada actualización e instalarla una vez realizadas las pruebas correspondientes en un sistema de pre-producción o no real para el correcto funcionamiento empresarial.

Un claro ejemplo son las actualizaciones de los sistemas Windows. Cada segundo martes de cada mes, saca un paquete de actualizaciones. Muchas de ellas son paquetes que cubren vulnerabilidades o agujeros de seguridad que deben ser remediadas de manera inmediata, pero en otras ocasiones nos encontramos que también nos introducen actualizaciones de aplicaciones internas del sistema que no usamos, e incluso en ocasiones generan malfuncionamiento en el rendimiento de nuestro equipo o aplicaciones que realmente son necesarios para la productividad laboral. Es por ello que las actualizaciones deben ser administradas por un especialista en la materia.

22. Phishing

La forma más habitual en la que nos encontramos intentos de ataque con phishing, son todos aquellos mails donde aparece un enlace aparentemente correcto en el que nos pide que nos autentiquemos para validarse, normalmente de entidades bancarias.

Ninguna empresa, ya sea un banco, nuestra propia empresa o cualquier otra entidad, nos va a pedir que nos validemos con nuestras credenciales o que se las mandemos. Estas credenciales son datos de carácter personal e intransferible, por lo que jamás las entregaremos y siempre que las usemos tras pulsar un enlace del correo electrónico, veremos que la dirección web mostrada por el navegador, coincide con la que realmente corresponde a la entidad o empresa donde nos autentificaremos.

Este tipo de enlaces suele ir re-direccionado a páginas web clonadas por los atacantes con el objetivo de infectarse con malware o de obtener nuestras credenciales.

23. Ingeniería Social

Cuando pensamos en un hacker o atacante, pensamos en una persona que dispone de grandes conocimientos informáticos y es capaz de acceder a nuestra información empresarial mediante técnicas, comandos y aplicaciones informáticas muy sofisticadas.

Si bien es cierto que este tipo de personas existen, son muchos los que no necesitan saber mucho de informática para acceder a nuestra información. Usted puede obtener información privada de una gran empresa sin mayor conocimiento informático del que ya dispone.

Para ello se usa una técnica llamada Ingeniería Social. Esto consiste en obtener la mayor información posible sobre la víctima en internet, para posteriormente usar el desconocimiento de ciertos usuarios para obtener lo que deseamos.

Estos ataques consisten en hacer pensar a un empleado, que otro miembro de la empresa o incluso el director o gerente, te está solicitando unos datos determinados. Ante la creencia de que el gerente te solicita una tabla con información, un informe concreto, un listado de clientes, un teléfono concreto o cualquier otra información, solemos reaccionar con miedo y responder rápidamente entregando la información que nos pidan.

Conocer la alta jerarquía de una red empresarial es muy sencillo, al igual que ser consciente de los eventos a los que acude. Estas son excusas que muchos utilizan para obtener mayor información sobre la red empresarial y generar miedo en los usuarios para llegar a obtener toda la información deseada, incluso claves de acceso.

No hace falta gran conocimiento de informática para obtener información disponiendo de las claves de acceso que nos la brindan. Es por ello que nunca deberemos entregar nuestras contraseñas a nadie.

Always On Systems Hispania S.L

Los medios más frecuentes usados por este tipo de atacantes, son el correo electrónico y el teléfono, el cual les permite generar una mayor manipulación.

En muchas ocasiones se hacen pasar por técnicos. Debemos tener en cuenta, que los administradores del sistema disponen de acceso a toda la información de la red con sus credenciales, en ningún momento necesitarán las nuestras, y de necesitarlas (cosa que no es real), pueden cambiarnos o averiguar sin problema.

24. Finalización de la vinculación o relación

Los sistemas y servicios de información provistos por la entidad empresarial a los usuarios, son accesibles por éstos exclusivamente mientras se mantenga vigente su relación o vinculación laboral con la misma mediante contrato.

Al término de dicha vinculación o relación, los usuarios dejarán de tener acceso a los sistemas de información de la empresa, y a los datos en ellos contenidos. Igualmente, los usuarios deberán devolver a la entidad empresarial cualesquier soporte del que dispongan y que contengan datos a los que hayan tenido acceso en el marco de su vinculación o relación laboral.

En caso de terminar la relación o vinculación de un usuario con la empresa, o si dicho usuario cambia de puesto o de ubicación, se verá obligado a ceder el control sobre todos los ficheros y documentos relativos a su prestación profesional. Si en los sistemas de información a los que haya tenido acceso hubiera creado ficheros o documentos de carácter no profesional, dichos ficheros o documentos deberán ser eliminados de inmediato.