MANUAL DE BUENAS PRÁCTICAS EN SEGURIDAD Y CONFIDENCIALIDAD DE BARBERAN, S.A.

Castelldefels, julio de 2016

Apreciado colaborador,

La reciente Reforma del Código Penal, operada a través de la Ley Orgánica 1/2015, de 30 de marzo, en vigor desde el pasado 1 de julio de 2015, posibilita la imputación de las empresas, tanto por las acciones cometidas por sus administradores como por sus empleados, si la empresa no ha implantado las medidas adecuadas para prevenirlos.
En concreto, el Código Penal establece la obligación de supervisión de la empresa respecto a la actuación de sus empleados.

Del mismo modo, la vigente normativa de protección de datos establece asimismo una obligación de supervisión y diligencia de la empresa en el tratamiento que se efectúa en su seno de datos personales de clientes y de empleados.

En este contexto de cumplimiento normativo, adjuntamos las Normas relacionadas con la seguridad y confidencialidad de la información de la empresa a la que puedes acceder como empleado de BARBERAN, S.A., así como normas relacionadas.

Tales normas tienen como objetivo garantizar la seguridad de la información contenida en los ficheros de clientes, y redes sociales de BARBERAN, así como clarificar aspectos relativos al uso de la información, etc y cumplir la normativa vigente en materia de protección de datos.

Atentamente,

_____

Director General.

1. Normas de acceso físico al local

Las entradas y salidas de la empresa deben efectuarse siempre por la entrada del personal.

2. Norma general relativa a la confidencialidad y uso de información y material.

Cualquier información, archivos, material y medios de cualquier tipo en general que se pongan a disposición de Usted como trabajador de BARBERAN son propiedad de ésta y deben destinarse a su exclusivo uso profesional en el marco de la prestación de servicios, debiendo preservar el colaborador/a la confidencialidad de la información, sin que pueda en ningún caso suministrarse a terceras personas.

3. Uso de los equipos informáticos

Los ordenadores, las redes de comunicación y el acceso a Internet proporcionado por BARBERAN son sólo para fines profesionales de la empresa. Deben adoptarse todas las precauciones con el fin de preservar los equipos.

El uso privado de Internet no está permitido. Respecto al correo electrónico, BARBERAN permitirá el uso privado del sistema de correo interno en una medida razonable (por ejemplo, para el intercambio de mensajes cortos), siempre y cuando no perturbe las operaciones del negocio.

No se permiten las cadenas de mensajes, la compra-venta, anuncios privados, etc. Se señala explícitamente que la confidencialidad de los datos privados no está garantizada.

Los empleados de BARBERAN deben ser conscientes de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable de los equipos para reducir este riesgo. El usuario será responsable de toda la información contenida en dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.

Si desaparecieren soportes magnéticos o material o documentación relacionada con los PCs, deberá comunicarse inmediatamente al responsable de seguridad del centro. Igualmente si se localiza algún soporte magnético extraviado (lápices magnéticos USB, etc) deberá entregarse inmediatamente al responsable de seguridad del centro, sin acceder a su contenido.

El empleo de dispositivos de memoria USB o SD en ordenadores fijos conectados a la red de la empresa no está permitido, con carácter general, salvo autorización previa y expresa del responsable de seguridad. Si el ordenador está fuera de la red o es un portátil, se aplicarán las medidas de seguridad correspondientes.

4. Recursos y datos protegidos

Los puestos de trabajo estarán bajo la responsabilidad de un usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.
Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
El usuario que tenga a su cargo la custodia de documentos con datos protegidos deberá tomar las precauciones necesarias para que esta información no pueda ser accesible por otras personas no autorizadas, debiendo archivar esta documentación en el dispositivo de almacenamiento protegido mediante cierre y destinado a tal efecto, inmediatamente después de finalizado su tratamiento.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos del correspondiente fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
Todos los datos y las aplicaciones elaborados por los empleados o colaboradores o suministrados por la compañía son activos que pertenecen a BARBERAN.

Sin autorización, no deben ser modificados, transmitidos, almacenados en soportes de datos o eliminados.

5. Obligaciones en cuanto al tratamiento de datos personales. Confidencialidad.

Para el desarrollo de sus funciones puede tener acceso a los datos de carácter personal de los clientes contenidos en el Ficheros de Clientes de BARBERAN, por lo que deberá cumplir las presentes normas de confidencialidad:

5.1.- No revelar la contraseña que se le asigne a ninguna persona, al ser su utilización personal e intransferible.

5.2.- Realizar las anotaciones que sean necesarias en el Fichero únicamente para el cumplimiento de sus funciones y en el marco de los servicios solicitados por el Cliente de BARBERAN.

5.3.- No revelar a persona alguna ajena a BARBERAN ningún tipo de información referente a los datos personales de los clientes a que haya tenido acceso en el desempeño de sus funciones.

5.4.- Utilizar la información referida en el párrafo anterior únicamente en la forma que exige el desempeño de sus funciones en la Empresa y no disponer de ella de ninguna otra forma o con otra finalidad.

5.5- No utilizar en forma alguna cualquier información que hubiese podido obtener prevaliéndose de su condición de empleado o colaborador de BARBERAN que no sea necesario para el cumplimiento de sus funciones en la Empresa.

5.6.- No se realizarán anotaciones sobre los ficheros de datos ni se anotarán informáticamente calificaciones personales de ningún tipo que puedan dar lugar a discriminaciones o sean atentatorias contra la dignidad, el honor o la propia imagen.

5.7.- Cumplir los compromisos anteriores después de extinguida, por cualquier causa, la relación laboral que le une a BARBERAN.

6. Configuración de puestos de trabajo

Los puestos de trabajo tendrán una configuración fija en sus aplicaciones, sistemas operativos que solo podrá ser cambiada bajo la autorización del Responsable de Seguridad, por Administradores autorizados O POR DELEGACIÓN DEL RESPONSABLE DE SEGURIDAD.

7. Contraseñas

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo al Responsable de Seguridad quien se encargará de registrarlo como incidencia y proceder a gestionar su cambio.

Queda terminantemente prohibido revelar las contraseñas y códigos PIN que autorizan a los empleados o colaboradores a acceder a un sistema. No se revelarán ni al personal de BARBERAN, ni a terceros. Ni los códigos PIN ni las contraseñas deben en ningún caso ser anotados, dejados en el lugar de trabajo o almacenadas en cualquier soporte de datos. Las autorizaciones de acceso VPN a la red de la empresa (tarjeta de identificación, tarjetas inteligentes, etc) se entregarán sólo a personas autorizadas oficialmente por BARBERAN.
Todos los ordenadores tendrán configurada la protección de pantalla para que se active tras unos minutos sin uso. Para retornar al sistema será necesario volver a introducir la clave de usuario.

8. Ficheros temporales

Respecto a los ficheros temporales, se informa debidamente al usuario de que una vez concluida la finalidad que motivó la creación del fichero, éste debe ser cancelado.

Queda absolutamente prohibido en el PC de los usuarios tener ficheros con datos personales de los ficheros tratados.

Cada usuario es responsable de la confidencialidad y custodia de los datos personales contenidos en soporte papel mientras se encuentran fuera de su lugar de archivo por ser necesario para la realización de alguna tarea.

Cuando se imprime en soporte papel documentos que contengan datos de carácter personal, una vez cumplida la misión que motivó su creación, estos serán destruidos.

9. Incidencias

Todas las incidencias que afecten o puedan afectar a la seguridad de los datos (incidencias que afecten a la identificación y autenticación de los usuarios, incidencias que afecten a los derechos de acceso a los datos, incidencias que afecten a la gestión de soportes, incidencias que afecten a las copias de seguridad y procesos de recuperación, incidencias que afecten al acceso no controlado de datos confidenciales, etc) deberán comunicarse al Responsable de seguridad utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente.

Para que quede constancia de la comunicación, el usuario, además, lo comunicará por escrito. En este sentido, cualquier usuario que tenga conocimiento de una incidencia es responsable de su inmediata comunicación al Responsable de seguridad.

El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del fichero por parte de ese usuario.

10. Soportes y documentos

BARBERAN aplica como política de soportes la de generar los mínimos necesarios, tenerlos adecuadamente controlados y borrar explícitamente dichos soportes una vez dejan de ser necesarios.

Los soportes electrónicos que contengan datos de los ficheros, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, proceso que los ha originado y fecha de creación.

Aquellos medios electrónicos que sean reutilizables, y que hayan contenido copias de datos de los ficheros, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Los soportes y documentos que contengan datos deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del fichero.

No podrá extraerse de la empresa ningún soporte, salvo autorización previa y por escrito del Responsable de seguridad del centro.

No pueden realizarse copias de datos que consten en el ordenador, propiedad de la empresa y destinado a uso profesional, en soportes externos.

Los soportes magnéticos (lápices magnéticos USB, etc) que se utilicen excepcionalmente, en su caso, deben ser exclusivamente los facilitados por BARBERAN y no deben salir del lugar de trabajo, salvo autorización previa y expresa del responsable de seguridad.

En consecuencia, no pueden utilizarse PCs ni soportes magnéticos de BARBERAN fuera de la empresa, por motivos profesionales, salvo en caso de la autorización previa por parte del responsable de seguridad del centro.

Si desaparecieren soportes magnéticos o material o documentación relacionada con los PCs, deberá comunicarse inmediatamente al responsable de seguridad del centro.

En ningún caso de introducirán soportes no autorizados. No pueden realizarse copias de datos que consten en el ordenador, propiedad de la empresa y destinado a uso profesional, en soportes externos.

Cuando se imprime en soporte papel documentos que contengan datos de carácter personal, una vez utilizados y cuando se vayan a desechar, deberán ser destruidos utilizando las máquinas destructoras.

11. Tareas de Administración y software.

Sin un permiso explícito, los empleados o colaboradores no realizarán tareas propias de un administrador de red y no instalarán o utilizarán programas de software (analizadores de red) con los que se puedan determinar palabras clave, contraseñas o códigos PIN.

Como protección contra: "virus", "Caballos de Troya" (para espionaje y denegación de servicio de los programas), averías de los sistemas y para el cumplimiento de los derechos de licencia y propiedad, los empleados o colaboradores no están autorizados a instalar software en su PC o portátil, incluso si el software se proporciona por un proveedor reconocido. Los datos y archivos de datos desarrollados por terceros deben ser chequeados en busca de virus antes de ser incluidos en el sistema por parte de las personas con derecho a hacerlo.

Los empleados o colaboradores con equipos portátiles no tienen autorización para instalar software ajeno al licenciado y autorizado por la empresa. No se admite su uso como contenedor de datos privados ni aplicaciones personales. El empleo de periféricos USB o SD está prohibido, con carácter general, salvo autorización previa y expresa del responsable de seguridad. Por ser especialmente sensibles, estos equipos sólo podrán ser configurados por personal de la empresa.

12. Copias de seguridad

Con el fin de preservar el contenido de los ficheros de la empresa, se realizan automáticamente copias de seguridad de las informaciones que contienen los PC con carácter periódico.

Es obligatorio permitir el sistema de back-up de todos los ficheros

13. Protección Antivirus

Todos los PC's tienen instalado un software Antivirus actualizado. Está prohibido desconectar dicho antivirus. En caso de detectarse algún virus, debe retirarse inmediatamente el soporte, no volver a introducirlo, e informar al Departamento de Informática.
No deben utilizarse soportes que previamente se hayan introducido en equipos ajenos a la empresa.

14. Acceso desde el exterior

Desde el exterior, las conexiones de comunicación con la empresa sólo pueden ser establecidas a través de sistemas de acceso especiales, solicitados y proporcionados con suficiente antelación al empleado o colaborador por el Responsable del centro y que garanticen la seguridad y la identidad.

15. Dispositivos portátiles.

No debe acudirse al puesto de trabajo con ordenadores portátiles propios.
En cuanto a los dispositivos móviles, debe hacerse un uso razonable.

No se podrá configurar en los dispositivos portátiles el correo electrónico de la empresa, salvo autorización expresa del responsable del centro.

16. Cámaras de video- vigilancia.

Se informa al empleado o colaborador de la existencia de cámaras de video-vigilancia en los accesos y en diversos extremos del centro, a efectos de vigilancia y control del centro.

17. Uso de correo electrónico

El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad de BARBERAN y no pueden introducirse dispositivos externos en la empresa, propiedad del trabajador, salvo previa y expresa autorización al efecto por el responsable de seguridad.

Respecto al correo electrónico, BARBERAN permitirá el uso privado del sistema de correo interno en una medida razonable (por ejemplo, para el intercambio de mensajes cortos), siempre y cuando no perturbe las operaciones del negocio.

No se permiten las cadenas de mensajes, la compra-venta, anuncios privados, etc. Se señala explícitamente que la confidencialidad de los datos privados no está garantizada.

Cualquier fichero introducido en la red corporativa o en el Terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

BARBERAN se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa, así como el acceso al correo electrónico, siempre de conformidad con el principio de confidencialidad y con absoluto respecto a los derechos de los trabajadores.

La recuperación y transmisión de la información hacia otras cuentas de la empresa de informes ejecutables de fuentes poco fiables o ajenas al propio desarrollo del trabajo (amigos, familia, remitentes desconocidos, ocio en general) está prohibida.

Se ruega a los usuarios la no inclusión en lista de correo o solicitud de información en Internet a menos de que exista una necesidad de trabajo para hacerlo.

Todos los mensajes enviados vía Internet se entenderán creados por nuestra organización. Es importante que dichos mensajes reflejen nuestros mejores niveles de profesionalidad.

El uso de mensajería instantánea y chats están completamente prohibidos, excepto que exista una necesidad de trabajo para hacerlo.

En el caso de vacaciones se podrá acceder al correo electrónico del mismo, para poder continuar la actividad.

A partir del momento en que el colaborador deje de prestar sus servicios a la empresa, podrá accederse a su correo electrónico, al ser éste un medio propiedad de BARBERAN.

No está permitido leer e-mail de otra persona o enviar por e-mail con un nombre falso. Por otra parte, el correo electrónico debe ser conservado y archivado de tal manera que sea accesible siempre que sea necesario (preservación de las pruebas en los procedimientos judiciales; períodos de conservación que se observa legalmente, etc.).

18. Acceso a Internet

El uso del sistema informático de BARBERAN para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de BARBERAN y los cometidos del puesto de trabajo del usuario.

El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.

El acceso a páginas Web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. se limita a aquellos que contengan información relacionada con la actividad de BARBERAN o con los cometidos del puesto de trabajo del usuario.
BARBERAN se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.
Cualquier fichero introducido en la red corporativa o en el Terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

La Empresa se reserva el derecho de facilitar o no el acceso a Internet dependiendo de la necesidad del puesto de trabajo.

El uso de Internet siempre debe tener una finalidad profesional o estar relacionado con las actividades de BARBERAN. En consecuencia, se prohíbe expresamente el uso de Internet para motivos personales.

Las informaciones de la empresa disponibles en Intranet / Red están reservadas a los colaboradores de BARBERAN y no deberán ser comunicadas a terceros.

No puede efectuarse ninguna importación de ficheros vía Internet, excepto si fuera necesaria para fines profesionales.

Para tener un sistema seguro, debe mantenerse la confidencialidad de la contraseña.

Deben efectuarse limpiezas periódicas de los datos acumulados para optimizar los recursos.

Si se detecta algo anormal en el funcionamiento del sistema, se debe indicar al responsable de seguridad del centro.

Podrían instaurarse por parte de la empresa controles sobre el uso de Internet.

Se ruega a los usuarios la no inclusión en lista de correo o solicitud de información en Internet a menos de que exista una necesidad de trabajo para hacerlo.