Propiedad y uso de los ordenadores personales

La Empresa facilita a los trabajadores el equipamiento informático (conexión a servicios, ordenadores y red de comunicaciones) necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Este equipamiento es propiedad de la Empresa y no está destinado a un uso personal. El usuario se compromete a utilizar los recursos informáticos de la Empresa exclusivamente para usos relacionados con su actividad laboral.

La información ubicada en la red de la Empresa es propiedad de la Empresa. Sólo aquellos servidores de información expresamente autorizados podrán ser conectados a la red de comunicaciones de la Empresa.

La dirección de sistemas será el responsable de definir la configuración básica hardware y software de los puestos de trabajo y administrar los accesos a la red corporativa. Cualquier necesidad de modificación del puesto será solicitada por la persona responsable de la dirección o unidad que lo solicita.

Los trabajadores deben cumplir las siguientes medidas de seguridad establecidas por la Empresa para el uso de los ordenadores personales:

- *No está permitido alterar la configuración física de los equipos ni conectar otros dispositivos a iniciativa del usuario, así como variar su ubicación.*
- *No está permitido alterar la configuración software de los equipos, desinstalar o instalar programas o cualquier otro tipo de software distinto a la configuración lógica predefinida.*
- *No está permitida la conexión de ordenadores no autorizados (fijos o portátiles) a la red corporativa.*
- *La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad de las unidades de informática. Cada usuario será responsable de la integridad y copia de seguridad de la información almacenada en el ordenador y medios de almacenamiento que tenga asignados.*
- *Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otra distinta del servicio al que está destinada.*

- *El usuario deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario deberá comunicarlo al servicio de Informática para que tome las medidas oportunas.*

- *En ningún caso se podrá acceder a los recursos informáticos y telemáticos con las siguientes finalidades:*

  - *Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.*

  - *Difundir contenidos contrarios a los principios enunciados en los Estatutos de la Empresa.*

  - *Dañar los sistemas físicos y lógicos de la Empresa, de sus proveedores o de terceras personas.*

  - *Introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar los datos anteriormente citados.*

  - *Usar cuentas de usuario sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta.*

  - *Usar la red u ordenadores de la Empresa para conseguir acceso no autorizado a cualquier ordenador.*

  - *Realizar con conocimiento de causa cualquier acto que interfiera en el correcto funcionamiento de los ordenadores, terminales, periféricos, red de comunicaciones, etc.*

  - *Instalar o ejecutar en cualquier punto de la red informática programas o ficheros que deterioren o incrementen en exceso la carga en cualquier punto de la misma, hasta el límite de llegar a perjudicar a otros Trabajadores o al rendimiento de la propia red. Esto incluye cualquier tipo de ensayo, experimento o actividad que incluso pudiendo ser considerada legítima perjudique el buen funcionamiento de la red.*

  - *Instalar o ejecutar en cualquier punto de la red informática programas o ficheros que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye los sniffer, scanner de puerto, etc.*

  - *Intentar sobrepasar protecciones de datos o sistemas de seguridad informática.*

- *Violar la privacidad de los datos y el trabajo de otros Trabajadores.*

- *La conexión a la red de comunicaciones de un nuevo equipo informático tiene que ser autorizada por el STIC quien proporcionará a dicho equipo una dirección IP. Queda prohibido el uso de IPs no proporcionadas por el STIC o el intercambio de ellas.*

- *La Empresa, a través del STIC, gestionará los rangos de direcciones IP que le han sido asignados en base a criterios técnicos, de ahorro y eficacia.*

- *Los ordenadores portátiles tienen la misma consideración de puestos de trabajo y se rigen por estas mismas normas. El uso al que están destinados y la posibilidad de que estos equipos se utilicen fuera del entorno de seguridad de la red corporativa de la Empresa hace necesarios procedimientos de seguridad específicos en relación con la actualización de los sistemas antivirus y del software instalado.*

- *Los equipos portátiles, así como los dispositivos o soportes informáticos, única y exclusivamente están puestos a disposición con la finalidad de permitir el desempeño de las funciones y tareas laborales encomendadas, estando prohibido el uso para otras finalidades de carácter personal.*

- *Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por la Empresa, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. De este modo, está prohibido, entre otros: i) emplear identificadores y contraseñas de otros trabajadores para acceder al sistema y a la red de la empresa ii) Intentar modificar o acceder al registro de accesos. iii) Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros y iv) En general, el empleo de la red corporativa, sistemas, equipos informáticos y cualquier medio puesto al alcance del usuario, vulnerando el derecho de terceros, los propios de la empresa, o bien para la realización de actos que pudieran ser considerados ilícitos.*

- *Queda prohibido terminantemente la apropiación de archivos o ficheros titularidad de la Empresa, para uso particular y/o de terceros. Es por esto que, en este sentido, se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de la empresa en ordenador propio, pen drives o a cualquier otro soporte informático. En caso de que así fuera menester, deben ser eliminados una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. Asimismo, durante el periodo de tiempo que los ficheros o archivos permanezcan en el*

equipo o soporte informático de su propiedad, deberá restringir el acceso y uso de la información que obra en los mismos.

- *En relación con lo anterior, deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de la empresa y dispuesto a razón única de las funciones o tareas desempeñadas en la Empresa.*

- *Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.*

- *La Empresa podrá suspender el uso de estos recursos a aquellos trabajadores que contravengan la presente normativa y en los casos en los que cualquier circunstancia sobrevenida lo aconseje.*

- *Si el posible trastorno causado a otros trabajadores o al servicio, por un trabajador, se entiende que no afecta de forma inmediata al buen funcionamiento del servicio, se le notificará su mal proceder mediante correo electrónico u ordinario. Si por el contrario, se entendiera que el trastorno producido altera el buen funcionamiento del servicio, el STIC tendrá la facultad de tomar las medidas necesarias para restaurar de forma inmediata el correcto servicio. Entre otras medidas de aplicar, se contemplan las siguientes: desconectar/deshabilitar las cuentas en los servidores, e inhabilitar el acceso a la red del ordenador o grupo de ordenadores que están generando el mal funcionamiento.*

Uso de la Red Corporativa

La red corporativa es un recurso compartido y limitado. Este recurso sirve no sólo para el acceso de los trabajadores internos de la Empresa a la intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

Los trabajadores deben cumplir las siguientes medidas de seguridad establecidas por la Empresa para el uso de la red corporativa:

- *Las acciones que intencionadamente rompan, retarden, pongan en peligro o accedan al trabajo de otros trabajadores, sin autorización específica, están prohibidas, son éticamente reprobables y serán perseguidas con las normas internas, y judicialmente si fuera preciso.*

- *La utilización de Internet por parte de los trabajadores autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como personal de la Empresa, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado.*

- *Queda prohibido cualquier uso comercial y/o privado no autorizado de los recursos informáticos de la Empresa.*

- *El propietario de una cuenta es el único responsable de su uso. Cuando se detecte una actividad prohibida, la Empresa responsabilizará al propietario de la misma.*

- *Está prohibido el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.*

- *Se considera el correo electrónico como un instrumento básico de trabajo. El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones.*

- *Los envíos masivos de información así como lo correos que se destinen a gran número de trabajadores serán solo los estrictamente necesarios que no puedan provocar un colapso del sistema de correo.*

- *No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia.*

Acceso a aplicaciones y servicios

Gran parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde ordenadores personales a aplicaciones que residen en servidores conectados a la red corporativa.

Los trabajadores deben cumplir las siguientes medidas de seguridad establecidas por la Empresa para el uso de aplicaciones y servicios corporativos:

- *Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante usuario y contraseña, u otro mecanismo) y previamente autorizado por el responsable correspondiente.*

- *La custodia de la contraseña es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona.*

- *Las contraseñas no deben anotarse, deben recordarse.*

- *Las contraseñas deben cambiarse periódicamente. Los trabajadores disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.*

- *Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable correspondiente.*

- *Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones establecidas, y apagar los equipos al finalizar la jornada laboral. Excepto en los casos en que el equipo deba permanecer encendido.*

Acceso y tratamiento de datos de carácter personal, a nivel informático y en papel.

Las anteriores instrucciones serán de aplicación en la observancia del cumplimiento de una normativa de especial importancia, la protección de datos de carácter personal [Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal]. Dado que está Ley trata de salvaguardar un derecho fundamental, mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el Usuario, que accede y trata información de carácter personal en el desempeño de las funciones y tareas, deberá atender a las siguientes obligaciones

- *Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal, conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la Empresa.*

***Datos de carácter personal** = información alfabética, numérica, gráfica, fotográfica, acústica o de cualquier otro tipo, relativa a un aspecto/s físico, psíquico, fisiológica, cultural, social o económico de la persona, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.*

Acceso y Tratamiento de Ficheros Informáticos

En particular, respecto a la información de carácter personal contenida en ficheros informáticos, deberá cumplir, en consonancia con lo expuesto en anteriores apartados, las siguientes diligencias:

- ***Claves de acceso al sistema informático.-** Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Queda*

prohibido, asimismo, emplear identificadores y contraseñas de otros trabajadores para acceder al sistema informático. En caso de que fuera necesario acceder al sistema, en ausencia de un compañero, se solicitará al Responsable de Seguridad que se habilite el acceso eventual. Una vez finalizada la/s tarea/s que motivaron el acceso, deberá ser comunicado, de nuevo, al Responsable de Seguridad.

- ***Bloqueo o apagado del equipo informático.***- *Bloquear la sesión del usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público.*

- ***Almacenamiento de archivos o ficheros en la red informática.***- *Guardar todos los ficheros de carácter personal empleados por el usuario, en el espacio de la red informática habilitado por la Empresa, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.*

- ***Manipulación de los archivos o ficheros informáticos.***- *Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros. Los permisos de acceso de los Trabajadores a los diferentes ficheros son concedidos por la Empresa, en concreto por el Responsable de Seguridad. En el caso de que cualquier Usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del citado departamento.*

- ***Generación de ficheros de carácter temporal.***- *Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. Estos ficheros deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática. Si transcurrido un mes el usuario detecta la necesidad de continuar utilizando la información almacenada en el fichero, deberá comunicárselo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.*

- ***No uso del correo electrónico para envíos de información de carácter personal sensible.***- *No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros. De modo que, se pondrá en conocimiento del Responsable de Seguridad para que*

implemente el cifrado, encriptado u otro mecanismo que salvaguarde la integridad y privacidad de la información.

- ***Comunicación de incidencias que afecten a la seguridad de datos de carácter personal.***- *Comunicar al Responsable de Seguridad las incidencias de seguridad de las que tenga conocimiento, que puedan afectar a la seguridad de los datos personales.*

Entre otros, tienen la consideración de incidencia de seguridad que afecta a los ficheros informáticos, los sucesos siguientes:

- *Pérdida de contraseñas de acceso a los Sistemas de Información.*
- *Uso indebido de contraseñas.*
- *Acceso no autorizado de Trabajadores a ficheros excediendo sus perfiles.*
- *Pérdida de soportes informáticos con datos de carácter personal.*
- *Pérdida de datos por mal uso de las aplicaciones.*
- *Ataques a la red.*
- *Infección de los sistemas de información por virus u otros elementos dañinos.*
- *Fallo o caída de los Sistemas de Información, etc.*

Acceso y Tratamiento de Ficheros en Papel

En relación con los ficheros en soporte o documento papel, el usuario deberá cumplir con las siguientes diligencias:

- ***Custodia de llaves de acceso a archivadores o dependencias.***- *Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal.*

- ***Cierre de despachos o dependencias.***- *En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.*

- ***Almacenamiento de soportes o documentos en papel.***- *Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada laboral. Cuando estos soportes o documentos, no se encuentren almacenados, por estar siendo revisados o tramitados,*

será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.

- ***No dejar en fotocopiadoras, faxes o impresoras papeles con datos de carácter personal.***- *Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes.*

- ***Documentos no visibles en los escritorios, mostradores u otro mobiliario.***- *Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.*

- ***Desechado y destrucción de soportes o documentos en papel con datos personales.***- *No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. A estos efectos, deberá ser siempre desechada o destruida mediante las destructoras de papel de las que dispone la Empresa. Se prohíbe terminantemente echar en papeleras, contenedores de cartón o papel, soportes o documentos, donde se contengan datos personales.*

- ***Archivo de soportes o documentos.***- *Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de la Empresa. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información.*

- *Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos.*

- *No podrá acceder o utilizar los archivos pertenecientes a otros Departamentos, que compartan la sala o dependencia habilitada a archivo.*

- ***Traslado de soportes o documentos en papel con datos de carácter personal.***- *En los procesos de traslado de soportes o documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubieren datos de carácter personal.*

- ***Traslado de dependencias.***- *En caso de cambiar de dependencia, en el proceso de traslado de los soportes o documentos en papel, se deberá realizar con el debido orden. Asimismo, se procurara mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal.*

- ***Envío de datos personales sensibles en sobre cerrado.-*** *Si se envían a terceros ajenos a la Empresa, datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte o documento papel, se debe realizar, en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.*

- ***Comunicación de incidencias que afecten a la seguridad de datos de carácter personal-*** *Comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales.*

Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel, los sucesos siguientes:

- *Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal.*
- *Uso indebido de las llaves de acceso.*
- *Acceso no autorizado de Trabajadores a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal.*
- *Pérdida de soportes o documentos en papel, con datos de carácter personal.*
- *Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.*

1. Los empleados/as podrán utilizar el correo electrónico, la dirección e-mail, la red corporativa e internet con libertad y en el sentido más amplio posible, para el desempeño de las actividades de su puesto de trabajo.

2. Siempre que precisen realizar un uso de estos medios que exceda el habitual, envíos masivos o de especial complejidad, utilizarán los cauces adecuados, de acuerdo con su jefe inmediato, para no causar daños en el desarrollo normal de las comunicaciones y en el funcionamiento de la red corporativa.

3. Con carácter general, los empleados/as no podrán utilizar el correo electrónico, la red corporativa, ni internet para fines particulares.

4. Bajo ningún concepto podrán los empleados/as utilizar estos medios para realizar envíos masivos de mensajes, enviar mensajes con anexos de gran tamaño (capacidad), ni realizar cualquier tipo de envío sin relación alguna con el desempeño profesional, que interfiera las

comunicaciones del resto de empleados/as o perturbe el normal funcionamiento de la red corporativa. Igualmente, no está permitido el envío de cadenas de mensajes electrónicos, la falsificación de mensajes de correo electrónico, el envío de mensajes o imágenes de material ofensivo, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc., aquellos que promuevan el acoso sexual, así como la utilización de la red para juegos de azar, sorteos, subastas, descarga de vídeos, audio u otros materiales no relacionados con la actividad profesional.

5. El incumplimiento de estas normas determinará la utilización por la empresa de las restricciones que considere oportuno en la utilización de estos medios y la aplicación de régimen disciplinario, en su caso, sin perjuicio de la exigencia de otras responsabilidades

6. Cuando existan indicios de uso ilícito o abusivo por parte de un empleado/a, la empresa realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoria en el ordenador del empleado o en los sistemas que ofrecen el servicio, que se efectuará en horario laboral y en presencia de algún representante de los trabajadores o de la organización sindical que proceda, en caso de afiliación, si el empleado/a lo desea, con respeto a la dignidad e intimidad del empleado/a.

Cámaras de video vigilancia en el centro de trabajo

Se informa a los trabajadores que el centro de trabajo cuenta con cámaras de video vigilancia, en las áreas de tránsito, para velar por la seguridad de las personas, bienes e instalaciones; así como para la prevención de delitos (robos, hurtos, etc.) y a verificar la comisión de los mismos a través de la visualización y grabado de imágenes.

Recordamos que las imágenes captadas por estas cámaras, instaladas conforme a lo dispuesto en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, pueden ser igualmente utilizadas para el control de la actividad laboral en el centro.

Por tanto, las imágenes captadas y grabadas a través de las mismas pueden ser objeto de tratamiento para verificar la comisión de infracciones laborales por parte de las personas que trabajamos en la empresa y, en su caso, en los procedimientos que se inicien como consecuencia de tales infracciones.

El fichero de las imágenes que se graban con estas cámaras y las obligaciones legales derivadas del mismo, es responsabilidad de la Universidad sede de las instalaciones de esta Empresa. Las imágenes grabadas pueden ser utilizadas a los efectos anteriormente expuestos. En

el supuesto de ser utilizadas como medio prueba, se mantendrán el tiempo que requieran los procedimientos laborales, administrativos y/o penales incoados.

Quedamos a vuestra disposición para cualquier aclaración o ampliación de esta información.

Uso del teléfono móvil en el centro de trabajo

"El uso de los teléfonos móviles particulares u otros dispositivos tales como tabletas, dentro de la empresa (y durante la jornada laboral, a salvo de los tiempos de descanso) está permitido, siempre y cuando se respeten las siguientes pautas de conducta y de utilización de tales dispositivos:

- Los teléfonos móviles deberán mantenerse en modo vibración o con un timbre lo suficientemente bajo como para no perturbar el trabajo de otros compañeros (se permiten las señales lumínicas de aviso de entrada de mensajes, salvo en el caso de puestos donde el uso de móviles esté expresamente prohibido).

- La duración de las llamadas deberá limitarse a dar o recibir avisos o mensajes de corta duración (entendiéndose como tiempo estimado uno o dos minutos).

- En ningún caso se podrán abandonar las instalaciones de la empresa o el centro de trabajo para atender llamadas personales, salvo que, atendiendo a las circunstancias personales de cada supuesto y una vez comunicado al supervisor o superior inmediato jerárquico, el trabajador obtenga el permiso para abandonar el puesto de trabajo por este motivo.

- El empleado deberá desconectar obligatoriamente su teléfono móvil en estos casos: durante la celebración de reuniones, presentaciones o videoconferencias, en visitas de clientes o proveedores y cuando así lo determinen los responsables de prevención de riesgos laborales.

- La infracción o incumplimiento de estas directrices en el uso de los teléfonos móviles dentro del ámbito empresarial y jornada laboral podrá dar lugar a la imposición de las sanciones correspondientes en el orden laboral.

Protección de datos/confidencialidad

La información confidencial relacionada con la Empresa y con el ámbito de trabajo de la misma, así como cualquier otra información confidencial, debe ser protegida. El deber de preservar la protección de datos y la confidencialidad continúa tras la finalización de su relación profesional con La empresa.

Por motivos de seguridad, y también para cumplir con los requerimientos legales, La Empresa puede acceder y observar determinadas actividades del ordenador que utiliza el usuario. Ponemos en conocimiento de nuestros trabajadores que los sistemas y protocolos de seguridad son capaces de grabar cada página de Internet visitada, cada chat, grupo de noticias o e-mails y cada archivo transferido desde la red interna; reservándose la Empresa el derecho de hacerlo en cualquier momento. El empleado no debe esperar tener privacidad en el uso de Internet en el puesto de trabajo. La Empresa puede revisar el sistema y la actividad en Internet y analizar los patrones de uso.

Propiedad de los sistemas relacionados con Internet

Los sistemas relacionados a Internet (incluyendo y no limitado a: equipo informático, software y sistemas operativos, cuentas de correo, página Web, protocolo de transferencia de datos, etc., trabajo en red y sistemas de intranet y software) son propiedad de La Empresa. Se implementan para ser utilizados con propósitos laborales y para servir a los intereses de la Empresa y de los servicios prestados en el curso normal de las operaciones.

La cuenta de correo electrónico asignada a cada trabajador en ningún caso es una cuenta personal, sino corporativa, por lo que, si las circunstancias lo requieren, la empresa puede acceder al contenido de las cuentas de correo o asignarla a otra persona temporal o definitivamente, respetando, en cualquier caso, la información personal que el usuario pudiera haber alojado en la misma (por este motivo no se deberían usar las cuentas de correo corporativas asignadas a cada trabajador para almacenar información personal o realizar gestiones personales, siendo el trabajador el responsable de hacer un uso razonable en este aspecto).

Privacidad de las comunicaciones

Las comunicaciones de los trabajadores en estos sistemas no son privadas. Aunque la administración de la red desea proveer de un razonable nivel de privacidad, los usuarios deben ser conscientes de que los datos que ellos crean en el sistema de la Empresa sigue siendo propiedad de la misma y que normalmente deben ser recuperados o incluso eliminados por el usuario. A parte de las precauciones de seguridad, no hay una forma segura e infalible de prevenir que un usuario no autorizado acceda a archivos almacenados en la red. La información que deba permanecer confidencial, debe y por lo tanto tiene que estar protegida por una clave o contraseña de acceso.