PROTOCOLO DE USO DE LAS TIC

ACTIVOS MULTIGESTION S.L.U.

G&M
CONSULTORES Y ABOGADOS

INDICE: PROTOCOLO DE USO DE LAS TIC.

PROTOCOLO DE USO DE LAS TIC

1. INTRODUCCIÓN.

El objetivo del presente documento es establecer las normas de uso y directrices generales que garanticen el adecuado uso de las tecnologías de la información y las comunicaciones, así como establecer los sistemas de control y las consecuencias que el incumplimiento de la misma tiene para los empleados.

La implantación de este Protocolo nos permitirá prevenir prácticas abusivas que puedan poner en riesgo la seguridad de los sistemas informáticos, asegurando en todo momento el cumplimiento de la legalidad, eficacia y eficiencia, además de asegurar que cualquier utilización de datos, ficheros, imágenes, bases de datos, etc. que contengan datos personales es adecuada a la normativa en materia de protección de datos.

Este Protocolo será comunicado a todos los empleados a quienes afecte.

2. ÁMBITO DE APLICACIÓN.

1. La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la empresa, incluyendo el personal de proveedores externos cuando sean usuarios de las TIC de la empresa.
2. En este sentido se entiende por usuario toda persona física que tenga autorizado el acceso a las tecnologías de la información y comunicaciones de la empresa, con independencia de la vinculación que tengan con la misma.

3. UTILIZACIÓN DE LOS EQUIPOS INFORMÁTICOS.

1. La empresa pone a disposición de los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional.
2. En consecuencia, los datos, dispositivos, programas y servicios informáticos que la empresa pone a disposición de los usuarios están destinados al desarrollo de las funciones laborales encomendadas, es decir, para fines profesionales.

Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido, es decir, NO está permitido el uso personal de tales recursos.

3. En general, el PC es el recurso informático que permite el acceso de los usuarios a los sistemas de información y servicios informáticos de la empresa, constituyendo un elemento muy importante en la cadena de seguridad, razón por que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.
4. Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados por la empresa para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los sistemas de información.

3.1. Normas Generales.

1. Existirá un inventario actualizado de los equipos informáticos. La persona designada para mantener el inventario actualizado y gestionar el mismo es xxxxxxx. Francisco Javier Hernández Núñez
2. A cada nuevo usuario que se incorpore a la organización y así lo precise, la empresa, le facilitarán un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales.
3. Cada nuevo usuario será incorporado a la Ficha de empleado, que incluirá lo siguiente:
    - ✓ Nombre, Apellidos y NIF.
    - ✓ Ubicación en la empresa y área a la que se incorpora.
    - ✓ Teléfono y dirección de correo electrónico.
    - ✓ Servicios a los que requiere acceso en base a su cargo.
    - ✓ Aplicaciones y perfiles.
4. Los ordenadores personales deberán utilizarse únicamente para fines profesionales y no para fines personales.

5. Únicamente el personal autorizado por la empresa podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de la compañía.
6. Cuando se precise instalar dispositivos no provistos por la empresa deberá solicitarse autorización previa al Administrador.
7. Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa y por escrito de la empresa. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
8. Salvo autorización expresa de la empresa, los usuarios no tendrán privilegio de administración sobre los equipos.
9. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
10. Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Informática, que tomará las oportunas medidas correctoras y dará traslado de la incidencia tanto al Director de la empresa.
11. Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados.
12. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
13. Los usuarios deberán notificar al Responsable de Informática, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

14. Cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto, accediendo a ellos con contraseñas individualizadas.
15. El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta al Responsable de Informática de tales circunstancias.
16. El usuario debe ser consciente 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 los equipos para reducir este riesgo.
17. El usuario será responsable de toda la información extraída fuera de la organización a través de 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.
18. El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al Responsable de Informática al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados.

3.2. Usos expresamente prohibidos.

Están terminantemente prohibidos los siguientes comportamientos:

1. Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.). Salvo que ésta se realice con fines laborales y a través del software VPN que da acceso al servidor.
2. Utilización de cualquier tipo de software dañino.
3. Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
4. Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la empresa, sin la previa autorización del Administrador.
5. Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por el Director General o el Director Financiero.

6. Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias y penales descritas en nuestro Código de Conducta y en nuestro Compliance Penal.

3.3. Normas Específicas para el almacenamiento de la información.

1. Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.
2. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa de la de la Empresa.

3.4. Normas Específicas para equipos portátiles, móviles, tabletas.

1. Los equipos portátiles y móviles serán asignados por la empresa.
2. Existirá un inventario actualizado de los equipos portátiles y móviles. El Departamento ~~Informático~~ Administración será el encargado de gestionar dicho inventario.
3. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable de informática. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
4. La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Responsable de Informática para la adopción de las medidas que correspondan y a efectos de baja en el inventario.

5. Los equipos portátiles y móviles deberán utilizarse únicamente para fines profesionales y autorizados, especialmente cuando se usen fuera de las instalaciones de la Compañía.
6. Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la empresa o no autorizadas para ello.
7. Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá al Responsable de informática llevar a cabo estas modificaciones.
8. Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá al responsable de informática, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

3.5. Normas Específicas para memorias externas y pen drive.

1. En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por la empresa, que serán conformes a las normas de seguridad de la organización.

   Estas memorias USB serán de uso exclusivo en los puestos de usuario de la empresa, no debiendo ser usados fuera de éstos. Siempre con información cifrada o con claves de acceso a la memoria USB.
2. Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento.
3. La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del Responsable de Informática, de forma inmediata, quien dará conocimiento de ello al Director General o al Director Financiero.

3.6. Copias de Seguridad.

1. Mantener copias de seguridad es una cautela esencial de protección de la información.
2. Los datos generados por el usuario en el desempeño de sus competencias profesionales no pueden ser almacenados en el disco duro local, ni en modo local en el escritorio del PC.
3. De forma periódica, se realizarán dos copias de seguridad, réplicas del equipo y backup de la información. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.
4. La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse al Responsable de Informática.

3.7. Eliminación de soportes informáticos.

1. Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información.

   En este sentido, el usuario deberá:

   - Asegurarse del contenido de cualquier soporte antes de su eliminación.
   - Cuando contenga información sensible, confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por la empresa.
2. Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por el Responsable de Informática, previa petición del responsable de departamento. Esta petición deberá dirigirse a través de la apertura de una incidencia al Responsable de Informática, que será responsable de la destrucción o almacenamiento de los medios informáticos obsoletos

3.8. Impresoras en red, fotocopiadoras y faxes.

1. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la

autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la empresa y, en su consecuencia, estén debidamente inventariados.

2. Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.
3. No olvidar recuperar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable de Informática.
4. Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización precisa.

3.9. Digitalización de documentos.

1. Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.
2. Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable de Informática.

3.10. Cuidado y protección de la documentación impresa.

1. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso

a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.

2. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de la empresa, de forma que no sea recuperable la información que pudieran contener.
3. Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.
4. Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

3.11. Pizarras y Flipcharts.

1. Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiaran adecuadamente las pizarras y Flipcharts de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

3.12. Protección de la propiedad intelectual.

1. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de la compañía sin la correspondiente licencia de uso.
2. Los programas informáticos propiedad de la empresa o licenciados a la misma están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa del Director General o del Director Financiero.
3. Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización del Director General o del Director Financiero.
4.

3.13. Protección de la dignidad de las personas

1. Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

4. USO EFICIENTE DE EQUIPOS Y RECURSOS INFORMÁTICOS

1. Dentro de las medidas de austeridad y reducción del gasto de la empresa se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios.
   - ❖ Apagar el PC (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
   - ❖ Imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color.
   - ❖ Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.

5. INSTALACIÓN DE SOFTWARE.

1. Únicamente el personal de soporte técnico autorizado por el Responsable de Informática podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.
2. No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.
3. Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la empresa de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

4. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el personal de soporte técnico, especialmente aquellas relacionadas con la seguridad.

6. ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS.

1. Los datos gestionados por la empresa y tratados por cualquier Sistema de Información de la compañía deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

2. Para acceder a los recursos informáticos es necesario tener asignada previamente una cuenta de usuario y estar dado de alta en los servidores de dominio. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

3. Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por el Responsable de Informática en caso de mala utilización, previa autorización del Director General o del Director Financiero.

4. Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

5. Cuando un usuario deje de atender un equipo durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar las salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de

terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 5 minutos.

7. IDENTIFICACIÓN Y AUTENTICACIÓN.

1. Los usuarios dispondrán de un código de usuario (user-id) y una contraseña (password), para el acceso a los Sistemas de Información de la empresa y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

2. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso, ni mantenerlas por escrito a la vista o al alcance de terceros.

3. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

4. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Director General o al Director Financiero la correspondiente incidencia de seguridad.

8. ACCESO A INTERNET.

1. El acceso a internet por los usuarios se realizará únicamente empleando los medios y a través de la red establecida a estos efectos por la empresa.
2. Las conexiones a internet realizadas tendrán una finalidad profesional. En este sentido, cada usuario autorizado empleará dichas conexiones exclusivamente para el ejercicio de las tareas y actividades que correspondan a las funciones de su puesto de trabajo.

3. Nunca se accederá a direcciones de internet que tengan un contenido ofensivo o atentatorio de la dignidad humana. A estos efectos, la empresa podrá restringir el acceso a determinados servidores de contenidos en internet.
4. La empresa podrá controlar los accesos a internet, procediendo a monitorizar las direcciones de acceso y el tiempo de conexión de los usuarios a internet, así como la limitación de su uso en razón de las funciones que ejerza, por motivos de seguridad o rendimiento de la red.
5. Las transferencias de datos desde o a internet se realizarán exclusivamente cuando lo exija el ejercicio de las funciones del puesto de trabajo. En todo caso, los usuarios deberán tener en cuenta, antes de utilizar la información proveniente de la red, si dicho uso es conforme a las normas que protegen la propiedad intelectual e industrial.
6. Se considerará Uso Abusivo, y por tanto queda terminantemente prohibida la realización de cualquiera de las siguientes conductas:
   - ❖ Publicación o envío de información no solicitada.
   - ❖ Publicación o envío de información sensible, confidencial, protegida o propiedad de la empresa, a personas, físicas o jurídicas, entes públicos o privados, no autorizados.
   - ❖ Uso de internet para propósitos que puedan influir negativamente en la imagen de la empresa, de sus representantes o de los organismos con los que se mantiene relación.
   - ❖ Acceso a otras redes, con el propósito de violar su integridad o seguridad.
   - ❖ Acceso a contenidos no relacionados con los cometidos profesionales tales como:
     - Acceder, recuperar o visualizar textos o gráficos que excedan los límites de la ética.
     - Almacenar en el equipo informático, tableta, terminal móvil, servidores o similar, propiedad de la empresa, archivos personales.
     - La transferencia de archivos y/o ficheros no relativa a las actividades profesionales del usuario (por ejemplo: juegos, música, fotos, videos, películas, etc.).
     - Realizar cualquier actividad de promoción de intereses personales.

9.USO DEL CORREO ELECTRÓNICO CORPORATIVO.

1. La empresa suministrará a cada usuario una dirección individual de correo electrónico, procediéndole a instalar y configurar una cuenta de correo. El acceso a dicha cuenta de correo se efectuará mediante una clave personal.
2. Se prohíbe el uso en al ámbito de la empresa de otras cuentas de correo electrónico distintas a las facilitadas por la empresa.
3. El uso del correo electrónico facilitado por la empresa es estrictamente profesional, pudiendo ser utilizado única y exclusivamente para el ejercicio de las funciones correspondientes al puesto de trabajo que desempeñe el usuario.
4. Los usuarios tienen terminantemente prohibido el acceso a cuentas de correo electrónico que no le hayan sido asignadas. Para que un usuario distinto pueda acceder a una cuenta de correo será preciso que el titular de la misma lo autorice por escrito, salvo los supuestos de cuentas de correo asociadas a puestos singulares.
5. Está terminantemente prohibido interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otros usuarios.
6. Queda prohibido el uso abusivo del correo electrónico, utilizando mensajes con contenidos ofensivos o atentatorios a la dignidad humana. Así mismo queda prohibido el envío deliberado de cualquier clase de programa o virus que pueda causar perjuicios en los sistemas de información de la empresa o a terceros.
7. Está terminantemente prohibido el uso del correo electrónico para el envío de publicidad, salvo que exista consentimiento expreso previo, así mismo queda prohibido el uso abusivo del sistema de listas de correos para el envío de mensajes de forma masiva o piramidal.
8. Una vez finalizada la relación entre el usuario y la empresa se interrumpirá el acceso a la cuenta de correo electrónico del usuario.

10. USO DE REDES SOCIALES.

1. Está prohibido el uso de redes sociales personales (Facebook, twitter, Instagram, etc.) en el ámbito laboral.
2. Nunca se ofrecerá información que pueda ser confidencial perteneciente a la empresa, a través de redes sociales.

11. CONTROL EMPRESARIAL.

1. La Dirección de la empresa se reserva el derecho de comprobar, si la utilización de las herramientas informáticas puestas a disposición del usuario, se realiza conforme a lo establecido en el presente protocolo.
2. De conformidad con la facultad de la empresa inherente a su poder de dirección, se utilizarán las medidas que se consideren adecuadas para garantizar el cumplimiento del presente Protocolo, pudiendo instalar sistemas en el servidor central que permitan conocer las páginas de internet visitadas, el tiempo de conexión a internet, el número de correos recibidos y enviados, las direcciones y el asunto de los mismos.

12. INCUMPLIMIENTO DEL PROTOCOLO.

1. TODOS LOS USUARIOS DE LA EMPRESA ESTÁN OBLIGADOS A CUMPLIR LO PRESCRITO EN LA PRESENTE NORMATIVA. A cuyo efecto, la empresa garantizará la divulgación y conocimiento de la misma, valiéndose para ello de cuantos medios informativos estén a su alcance.

2. En caso de infracción de la presente normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan, según la legislación laboral, y en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados al usuario.