REGLAMENTO SOBRE UTILIZACION DE LOS RECURSOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

ÍNDICE

1.- Disposiciones generales.

2.- Objeto.

3.- Definición de Tecnologías de la Información y de la Comunicación. (TIC).

4.- Principio de confidencialidad.

5.- Derecho de información de la política organización/comunidad educativa de TIC al personal de la organización/comunidad educativa.

6.- Deber de formación en política organización/comunidad educativa de TIC

7.- Dirección y control de la actividad laboral.

7.1.- Alcance.

7.2.- Vigilancia y control de los recursos tecnológicos y medios productivos corporativos.

7.3.- Principios que deben regir la actividad de vigilancia y control.

7.4.- Control del correo electrónico.

7.5.- Control del acceso a Internet.

7.6.- Expectativa de uso privativo de medios productivos corporativos.

7.7.- Monitorización del correo electrónico y servicios de acceso a Internet.

1.- **Disposiciones generales**.

En fecha **9 de Junio de 2022** se aprobó el Código de Conducta que establece como uno de los principios de actuación el ***«Uso adecuado de las herramientas informáticas»***.

La absoluta relevancia que ha tenido la irrupción de las nuevas tecnologías en el desarrollo de la actividad y comunicación de la organización/comunidad educativa, conlleva la necesidad de adoptar las medidas adecuadas para su correcta utilización, todo ello en aras a garantizar la protección de todos los bienes jurídicos que están en juego.

2.- **Objeto**.

El objeto del presente Reglamento es definir de forma clara, cuál debe ser el uso que debe darse a las TIC (Tecnologías de Información y Comunicación) corporativas. Este protocolo se encuentra en sincronización con las condiciones generales de cesión de

portátiles que tiene incorporada la organización a los docentes, en especial en cuanto al uso privado de los mismos.

3.- **Definición de Tecnologías de la Información y la Comunicación** (TIC).

Las Tecnologías de la Información y la Comunicación (TIC) son el conjunto de herramientas, aplicaciones e instrumentos desarrollados para gestionar información y enviarla de un lugar a otro. Incluyen las tecnologías para almacenar información y recuperarla después, así como para enviarla de un sitio a otro, y/o procesar tal información.

De ese modo, las **TIC** conforman el conjunto de recursos necesarios para tratar información a través de ordenadores, dispositivos electrónicos, aplicaciones informáticas y redes sociales, necesarias todas ellas para almacenarla, convertirla, administrarla y transmitirla, permitiendo un mejor acceso y clasificación de la información para el desarrollo de su actividad organización/comunidad educativa.

4.- **Principio de confidencialidad**.

La confidencialidad de las comunicaciones constituye un derecho fundamental reconocido en la Constitución Española, que debe guiar el modo de recibir y proporcionar la información. Por tanto, todos los miembros de la organización/comunidad educativa deberán mantener el más estricto secreto profesional y guardar confidencialmente toda la información que manejan en el curso de su labor profesional.

La organización/comunidad educativa y los trabajadores integrarán en su desarrollo profesional y personal la protección de la totalidad de los datos de los que tengan conocimiento por su relación laboral con COL.LEGI MARE DE DÉU DEL CARME, procurando su gestión adecuada y responsable.

Dentro del ámbito del principio de la confidencialidad, nos referiremos a tres ámbitos:

- Los establecidos por la **Ley de Protección de Datos**.
    - Se garantizará que los datos que pudieran recoger, obtener, o conocer, por su trabajo, y a través de cualquier canal -web, redes sociales, blog, oficinas del cliente, etc…- , no podrán transferirse a terceros bajo ningún concepto, ni se emplearán para uso personal.
- Los que determine la **estrategia de la organización/comunidad educativa**: la información que debe ser conocida únicamente por determinados grupos de personas, para maximizar la posibilidad de éxito de las decisiones tomadas.

- Se establecerán dentro de la estructura de la organización/comunidad educativa, los administradores de sistema, que se renovarán de forma anual y que serán los únicos con acceso a ese sistema. Cualquier autorización de administrador a otros miembros de la organización/comunidad educativa, deberá documentarse por escrito, indicándose el objeto del acceso y su duración.

- **Acuerdos de confidencialidad** con terceros (clientes, proveedores, asesores, etc…).

La confidencialidad es un elemento transversal a tener en cuenta en las comunicaciones de la totalidad de los miembros de la organización/comunidad educativa.

El acceso a las comunicaciones de los miembros de la organización/comunidad educativa se realizará bajo la más estricta legalidad constitucionalidad, protegiendo la intimidad, el honor y la propia imagen de éstos.

En el marco del principio de confidencialidad se establece la obligación, para todos los miembros de la organización/comunidad educativa, de no confeccionar copias o duplicados de la información confidencial a la que pudiera tener acceso cada uno de ellos.

La recepción de información confidencial se pondrá en conocimiento de la organización/comunidad educativa a través de los mecanismos previstos en la organización/comunidad educativa, con celeridad e inmediatez.

5.- **Derecho de información de la política organización/comunidad educativa al personal de la organización/comunidad educativa**.

La organización/comunidad educativa deberá informar de las normas de utilización de las TIC, de un modo claro, transparente y constante, como forma de implantar una conciencia transversal en su uso, y con la finalidad de generar una cultura acorde con las constantes exigencias en este ámbito.

La organización/comunidad educativa desarrollará la formación necesaria que minimice los posibles riesgos en el uso de dichas herramientas.

En esta política que, queda definida en el presente Reglamento, se fijará para los miembros de la organización/comunidad educativa un deber de formación, así como la posibilidad por parte del empleador, de la dirección y control de la actividad laboral, de la que se determinará de forma expresa el modo y alcance para evitar una merma en la privacidad del trabajador.

6.- **Deber de formación en política organización/comunidad educativa de las TIC'S**.

La organización/comunidad educativa se compromete a desarrollar una formación adecuada, ajustada y reiterada de las TICS a los miembros de la organización/comunidad educativa.

Para ello, se establecerá en las plataformas internas existentes para todos los empleados con COL.LEGI MARE DE DÉU DEL CARME, el recordatorio del Documento de Seguridad y sus sistemas de acceso.

7.- **Dirección y control de la actividad laboral.**

7.1.- ***Alcance***.

Es cada vez más evidente la revolución tecnológica que ha llevado a la utilización de las nuevas tecnologías para la mayor parte del desarrollo de la vida social, familiar, y también por supuesto, del entorno laboral, lo que conlleva la posibilidad y/o necesidad de que los trabajadores cuenten con herramientas informáticas para el desarrollo de su trabajo habitual.

Pero la privacidad del trabajador "*ha de conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la organización/comunidad educativa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores*"[1].

Se establece en el presente reglamento como se llevará a cabo dicha vigilancia y control para verificar el cumplimiento, por parte del trabajador, de sus obligaciones y deberes laborales, salvaguardando, en su adopción, los derechos de aquéllos.

7.2.- ***Vigilancia y control de los medios productivos corporativos***.

Los medios productivos de la organización/comunidad educativa corresponden a la organización/comunidad educativa y, en ningún caso, pueden considerarse propiedad de sus empleados.

La organización/comunidad educativa podrá adoptar las medidas que considere más oportunas para la vigilancia y control del cumplimiento, por parte del trabajador, de sus obligaciones y deberes labores, tal como señala el particular de la Sentencia del Tribunal Supremo -Sala de lo Social- de 26 de septiembre de 2007:

[1] Grupo de Trabajo "Artículo 29": grupo consultivo independiente encargado de estudiar cuestiones relativas a la aplicación de las medidas nacionales adoptadas en virtud de la Directiva 679/16.

"Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución el contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. ***Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el organización/comunidad educativa "como propietario o por otro título" y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen***. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el organización/comunidad educativa puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del organización/comunidad educativa, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes organización/comunidad educativa del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la espera personal del trabajador".

7.3.- ***Principios que deben regir dicha actividad de vigilancia y control***.

7.3.1.- Necesidad: El empleador, antes de proceder a la actividad de vigilancia y control, deberá comprobar si resulta absolutamente necesaria para un objetivo específico.

Por tanto, esa medida, tendrá carácter excepcional. Algunas conductas que pueden justificar el control del correo electrónico de un trabajador para obtener información o prueba de determinados actos sería:

- Investigación de actuación presuntamente delictiva de un trabajador, que obligara al empleador a defender sus intereses, siendo así que además podría ser declarado responsable civil subsidiario de los actos de dicho trabajador.
- Apertura de correo electrónico de un trabajador cuando sea necesario (por encontrarse de baja por enfermedad o de vacaciones) y no se haya podido derivar la correspondencia de aquel a otros empleados (vía funciones de respuesta o desviación automática).
- Detección de virus maliciosos que requieran conocer el origen de aquel y poder garantizar la seguridad del sistema.

7.3.2.- Finalidad: Los datos deberán recogerse para un fin determinado y legítimo, y tales datos no podrán ser tratados posteriormente con otros objetivos.

Se considerará un fin legítimo, por ejemplo, el evitar la fuga de información confidencial a un competidor.

7.3.3.- Transparencia: El empleador comunicará a todos los empleados la política de vigilancia y control de los correos e informará de manera completa sobre las circunstancias que pueden justificar tal medida, el alcance y su aplicación, que deberá incluir necesariamente:

- Política de utilización de correo electrónico e Internet por parte de los empleados, así como en qué medida puede ser utilizada para fines privados o personales.
- Cuando exista autorización para uso de correo electrónico para fines personales o privados, la vigilancia y control sobre ellos será muy limitada (ej. cuando se trate de detectar entrada de virus y sea necesario para garantizar la seguridad del sistema).

7.3.4.- Proporcionalidad: Se excluye el control general de los mensajes electrónicos y de la utilización de Internet por todo el personal, salvo cuando ello fuere necesario para garantizar la seguridad del sistema.

La tecnología actual ofrece programas que permiten evaluar la utilización del correo electrónico por parte de cada uno de los empleados, informando del número de mensajes enviados y recibidos, así como de los datos o documentos que se adjuntan.

Por otra parte, la tecnología también ofrece sistemas de bloqueo adecuados para evitar el uso abusivo de Internet, más allá del autorizado por el empleador.

7.4.- ***Control del correo electrónico***.

Se fijará dicho control siempre bajo los principios indicados en el apartado anterior, de modo que, cuando resulte necesario, el acceso al correo electrónico se realizará bajo programas informáticos de búsqueda ciega dirigida y no indiscriminada.

Dicha revisión se realizará en presencia del miembro de la organización/comunidad educativa a cuyo correo electrónico se vaya a acceder, o bien de su representante sindical. A tal efecto se levantará la correspondiente acta en el que se identifique a las personas que intervengan, con indicación precisa del objeto de dicho acceso y de su resultado.

Se autorizará por todos los miembros de la organización/comunidad educativa, la posibilidad de acceso y realización de actuaciones informáticas de copia -mediante volcado- del correo profesional -corporativo-.

A tal efecto, se dará a conocer a todos los trabajadores el **Anexo 1** del presente Reglamento relativo a **Políticas de utilización de las TIC.**

7.5.- ***Control del acceso a Internet.***

Se permite un uso razonable del Internet para fines personales y privados de forma excepcional.

Dentro del límite de lo que es razonablemente posible, la política de la organización/comunidad educativa respecto a Internet se basará más en la prevención que en la detección. En tal sentido, se dará prioridad a la utilización de herramientas técnicas dirigidas a limitar el acceso a determinadas páginas o descargas de determinados contenidos -por ejemplo, mediante el bloqueo a algunas páginas webs o instalando advertencias automáticas-.

Se facilitará información rápida al trabajador cuando se detecte la utilización sospechosa de Internet a fin de minimizar los problemas, no solo de un uso abusivo, sino también respecto a posibles riesgos en la seguridad de la red. En este sentido, la comprobación del tiempo empleado o la elaboración de una lista de las webs más visitadas, puede bastar para confirmar la actuación correcta, o incorrecta, del trabajador.

Si tales comprobaciones generales revelaran una posible utilización abusiva de Internet, el empleador podría entonces valorar la posibilidad de proceder a determinados controles en la zona de riesgo.

En todo caso, se informará al trabajador de los hechos conocidos mediante estas herramientas, a fin de que pueda refutar la utilización abusiva alegada por el empleador.

En tal sentido, se informará claramente a los trabajadores en qué condiciones se autoriza la utilización de Internet con fines privados, con indicación expresa de los elementos que no se puedan descargar, copiar o visualizar.

Se indicará también en el **Anexo 1**, los sistemas instalados para impedir el acceso a determinados sitios o detectar una posible utilización abusiva, así como si éste se llevará a cabo de manera individualizada o por departamentos, y si el contenido de las webs consultadas será visualizado o registrado por el empleador en determinados casos.

7.6.- ***Expectativa de uso privativo de medios productivos corporativos***.

La organización/comunidad educativa permite y autoriza cierta tolerancia del uso de medios corporativos mediante las TICS para uso personal y privado de los trabajadores, siempre que tengan relación directa con el funcionamiento de la organización/comunidad educativa. (Mensajes sindicales…).

En el caso de utilización para fines exclusivamente privados, este se llevará a cabo a través de cuenta de correo privada (WEB)- No será posible utilizar el correo electrónico corporativo.

7.7.- ***Monitorización del correo electrónico y servicios de acceso a internet***.

Se establece en este Reglamento la posibilidad de monitorización por parte de la organización/comunidad educativa del correo electrónicos corporativo y servicios de acceso a Internet de los empleados, en los términos establecidos en esta el **Anexo 1** de este documento.

ANEXO 1.- Política y normas de utilización y control de las tecnologías de la información y comunicaciones (TIC) en el COL.LEGI MARE DE DÉU DEL CARME

1.- **OBJETIVO**.

El objetivo de la presente Política es establecer las líneas de actuación a tener en cuenta a fin de garantizar el uso responsable y adecuado de las tecnologías de la información y las comunicaciones (en adelante TIC) de la organización/comunidad educativa COL.LEGI MARE DE DÉU DEL CARME, así como establecer los sistemas de control y las consecuencias que el incumplimiento de dicha política pueda acarrear a sus empleados.

Esta política estará integrada en el Código Ético y Convenio Colectivo, si lo hubiere, aprobados en su día para COL.LEGI MARE DE DÉU DEL CARME, así como con la normativa en materia de protección de datos personales, a la que también se hace referencia en este documento.

Esta política se ha comunicado a los representantes de los trabajadores y será luego comunicada a todos los empleados.

2.- **POLÍTICA DE USO Y CONTROL DE LAS TIC**.

2.1- **POLITICA DE USO DE LAS TIC**

COL.LEGI MARE DE DÉU DEL CARME, es una organización/comunidad educativa concienciada con la importancia que reviste la protección de datos personales y la seguridad de los sistemas de información. Por ello, quiere poner todos los medios necesarios para lograr un máximo nivel de seguridad, así como dar estricto cumplimiento a la legalidad vigente. En consecuencia, pone de manifiesto que:

a) Los empleados que utilicen los equipos y recursos informáticos puestos a su disposición por COL.LEGI MARE DE DÉU DEL CARME, son responsables de su conservación, así como de su utilización de acuerdo con la Ley y con las reglas establecidas en este protocolo. Dichos recursos y equipos son propiedad de COL.LEGI MARE DE DÉU DEL CARME, y solo se permite su utilización para desarrollar las tareas establecidas en el ámbito laboral.

b) La organización/comunidad educativa únicamente admite la utilización de las TICS y herramientas informáticas para uso personal y privado, de forma excepcional y cuando ello fuera estrictamente necesario.

c) El uso de las TICS será controlado tanto por motivos de seguridad como por motivos de control de la actividad laboral. Respecto al sistema de control, se dará prioridad a la utilización de herramientas de prevención y control menos

invasivos y a través de la medición de volumen, tráfico, actividad, extensiones de archivos, etc…

d) Se podrán establecer sistemas de control basados en catas aleatorias pero que no supongan de inicio un control total de la actividad.

e) Se podrán adoptar las medidas legales oportunas frente al incumplimiento de estas políticas y normas y, en general, frente al incumplimiento de la legalidad vigente, del Código Ético o del Convenio Colectivo.

f) Las claves de acceso para acceder a los sistemas y equipos informáticos constan de un "nombre de usuario" y "contraseña" -password-, que son secretos, personales e intransferibles. Por ello se prohíbe su comunicación a otras personas salvo que concurran motivos urgentes y extraordinarios que justifiquen tal comunicación.

2.2. **NORMAS DE USO**

Con carácter general, siempre se procurará trabajar sobre los servidores corporativos. Cuando sea necesario trabajar en modo local, el empleado será responsable de que la información contenida en el equipo -sean o no datos personales- quede guardada debidamente en el servidor habilitado al efecto para evitar su pérdida.

2.2.1.- **USO DEL CORREO ELECTRÓNICO CORPORATIVO:**

a) El correo electrónico corporativo se configura como una herramienta de trabajo. Se prohíbe su uso para fines no relacionados con las funciones laborales encomendadas.

b) El empleo del nombre o apellidos de los empleados junto al dominio de la organización/comunidad educativa, no significa la asignación por la organización/comunidad educativa de un correo personal, sino que tal correo está vinculado al área y puesto de trabajo.

c) Se podrá realizar copia de seguridad de los mails y acceder a su contenido, ante problemas técnicos o de seguridad o bien cuando existan sospechas de incumplimiento de las normas contenidas en este documento.

d) El correo electrónico corporativo no debe usarse como herramienta de difusión de correos masivos.

e) Se prohíbe expresamente realizar envíos de mensajes de forma masiva o en cadena, no autorizados, especialmente aquellos con finalidades comerciales o publicitarias sin el consentimiento del destinatario (correo basura o spam).

f) Dado que el correo electrónico es una de la fuentes más importantes de difusión de virus, se recomienda no abrir mensajes recibidos de remitentes desconocidos,

especialmente si además de desconocidos, tienen el asunto en inglés -a excepción de aquellos cuya lengua docente sea esta- o llevan archivos adjuntos. Se eliminarán los mensajes con anexos susceptibles de ejecución.

g) Se prohíbe cualquier tipo de envío sin relación con la actividad profesional que perturbe el funcionamiento normal de la red.

h) Se prohíbe expresamente el uso no autorizado de correo de otros compañeros así como la falsificación de mensajes de correo electrónico, ya sea sobre su contenido o manipulando las cabeceras para ocultar la identidad del usuario remitente.

2.2.2. **ACCESO A INTERNET.**

a) El acceso a Internet se configura como una herramienta a disposición de los empleados para el cumplimiento de sus tareas y funciones en la organización/comunidad educativa.

b) No se podrán descargar o utilizar programas o softwares que no estén previa y expresamente autorizados por la organización/comunidad educativa. De ser necesarios, se solicitará autorización al Director de Servicios Informáticos.

2.2.3 **DISPOSITIVOS DE ALMACENAMIENTO EXTERNO.**

Los usuarios no utilizarán dispositivos de almacenamiento externo. Cuando de forma excepcional sea necesario, se solicitará autorización para ello al Director de Servicios Informáticos y se adoptaran todas las medidas de seguridad:

- Cuando se autorice su uso, los dispositivos serán siempre facilitados por la organización/comunidad educativa.

- La información contenida en dichos dispositivos se guardará cifrada o con contraseña.

2.2.4.- **OTRAS CONDUCTAS PROHIBIDAS** (relativas tanto al uso de correo electrónico, Internet y redes sociales).

a) La utilización y tratamiento de datos de carácter personal de terceros sin la autorización necesaria.

b) El envío de mensajes o imágenes con material ofensivo, inadecuado o con contenidos discriminatorios por razón de género, así como aquellos que promuevan el acoso sexual.

c) Utilizar la red para juegos de azar, sorteos, subastas, descargas de vídeos, audio u otros materiales no relacionados con la actividad profesional.

d) Alterar, destruir, inutilizar o dañar de cualquier forma los datos, programas o contenidos electrónicos de COL.LEGI MARE DE DÉU DEL CARME o de terceros.

Dichos actos pueden constituir delito de daños, previstos en el artículo 264.2 del Código Penal.

e) Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la dirección técnica, u otros tipos de materiales protegidos por derechos de propiedad intelectual, cuando no se disponga de autorización.

f) Instalar o ejecutar desde cualquier punto de la red, programas o archivos vía Internet o a través de cualquier otro soporte externos (USB, CD,…) sin autorización expresa del Director de Servicios Informáticos.

g) Instalar o ejecutar desde cualquier punto de la red, programas o archivos que tengan por finalidad, o con los que se intente acceder, descubrir, manipular o destruir, información distinta a la que corresponda al empleado, sea cual sea el medio empleado -detectores, escáneres de puertos, programas de administración remota, …

h) Emplear identificadores y contraseñas de otros usuarios para acceder al sistema. Facilitar a otros empleados el identificador y contraseña personal a otros empleados salvo los casos expresamente previstos y autorizados.

i) Burlar las medidas de seguridad establecidas por el sistema informático, para acceder a contenidos -ficheros o programas- cuyo acceso no le esté permitido.

j) Modificar la configuración de redes, equipos y/o cualquier dispositivo de trabajo.

k) Llevarse los equipos u ordenadores personales a los domicilios particulares, incluso cuando sea para la realización de tareas profesionales, sin contar con la autorización expresa (por escrito) del responsable de Informática.

k) Y, en general, emplear la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del empleado, vulnerando el derecho de terceros, los derechos de la propia organización/comunidad educativa, o realizar cualquier otro acto que pueda considerarse ilícito por el Código Penal.

3.- **PROTECCION DE DATOS**

3.1.- **POLITICA RELATIVA A LA PROTECCION DE DATOS**

A fin de garantizar un tratamiento responsable y adecuado de los datos personales de los propios empleados y de terceros, y dar cumplimiento a la exigencia legal de proteger tanto los ficheros automatizados como los no automatizados, se detallan a continuación las obligaciones generales relativas a la protección de datos cualquier que sea el soporte en que se hallen.

3.2.- **OBLIGACIONES GENERALES Y COMUNES** -FICHEROS AUTOMATIZADOS Y NO AUTOMATIZADOS (PAPEL).

a) Guardar la necesaria reserva respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con COL.LEGI MARE DE DÉU DEL CARME.

b) Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en lugar seguro, cuando estos no estén siendo utilizados y, especialmente, una vez concluida la jornada laboral.

c) Queda prohibido el traslado por cualquier medio -vía correo electrónico mediante remisión de correos electrónicos del ordenador de la organización/comunidad educativa al ordenador personal, mediante copiado en dispositivos de almacenamiento externo -CD, USB,…- de listados, archivos o documentos con datos de carácter personal en los que se guarde información titularidad de COL.LEGI MARE DE DÉU DEL CARME fuera de los locales de sus locales sociales o centros de trabajo, sin autorización del Director de Servicios Informáticos. En el supuesto de resultar necesario dicho traslado o remisión de soporte, archivo o documento, éste se realizará cifrando los datos, o utilizando mecanismos que dificulten el acceso o manipulación por terceros en caso de pérdida o robo. (Utilización de contraseñas para lectura),

d) Los ***ficheros de carácter temporal*** son aquellos que almacenan datos de carácter personal para el cumplimiento de una necesidad determinada o trabajo temporal y cuando su existencia no sea superior a un mes. Estos ficheros deberán ser borrados una vez dejen de ser necesarios y, mientras mantengas su vigencia, deberán cumplir los niveles de seguridad asignados por el Responsable de Seguridad. Si transcurrido un mes, el empleado requiere seguir utilizando la información almacenada en dicho fichero, lo comunicará al Responsable de Seguridad a fin de adoptar las medidas oportunas sobre el particular.

e) Solo las personas autorizadas en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de accesos de los empleados son concedidos por el Responsable de Seguridad. Si algún empleado requiriera para el desarrollo de su trabajo acceder a ficheros o documentos a cuyo acceso no esté autorizado, lo comunicará al Responsable de Seguridad correspondiente para que le facilite dicho acceso por el tiempo necesario.

f) Comunicar al Responsable de Seguridad, las posibles incidencias de las que pueda tener conocimiento cualquier empleado.

3.3.- **OBLIGACIONES ESPECÍFICAS PARA LOS FICHEROS AUTOMATIZADOS**

a) Cambiar las contraseñas cuando el sistema lo requiera y guardar la oportuna reserva.

b) Cerrar o bloquear las sesiones a la finalización de la jornada laboral o cuando el empleado se ausente temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

c) No copiar información de ficheros o documentos en los que se almacenen datos de carácter personal al ordenador personal, sin autorización expresa del Responsable de Seguridad y sin adoptar las medidas de seguridad y custodia para evitar el acceso por parte de terceros.

d) Archivar los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad, a fin de facilitar la aplicación de las medidas de seguridad que correspondan.

e) Los empleados tienen prohibido terminantemente el envío de información de carácter personal de nivel alto, salvo autorización expresa del Responsable de Seguridad. En todo caso, el envío de esta documentación, solo podrá realizarse previa adopción de los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

3.4. **OBLIGACIONES RESPECTO A LOS FICHEROS NO AUTOMATIZADOS**

a) Mantener debidamente custodiadas las llaves de acceso a la organización/comunidad educativa, despachos y armarios, archivadores o elementos que contengan ficheros no automatizados, con datos de carácter personal. Se deberá comunicar al Responsable de Seguridad, cualquier hecho que pueda haber comprometido esta custodia.

b) Cerrar los despachos al término de la jornada laboral o cuando se ausente temporalmente de aquél, para evitar accesos no autorizados.

c) Establecer procedimientos de copiado o reproducción de documentos a fin de que puedan realizar esas tareas las personas habilitadas por el Responsable de Seguridad.

4.- **INCUMPLIMIENTO**

4.1. **COMUNICACIÓN**

En caso de infracción de las presentes normas COL.LEGI MARE DE DÉU DEL CARME comunicará al empleado, tan pronto tenga conocimiento de los hechos y le sea posible, la infracción cometida y sus consecuencias.

4.2. **CONSECUENCIAS**

La organización/comunidad educativa dispone de diferentes medios frente al incumplimiento de las obligaciones contenidas en el presente documento:

a) Podrá incoar un expediente disciplinario al empleado con las correspondientes sanciones previstas por el Convenio Colectivo o legislación laboral.

b) Si como consecuencia de la actuación del empleado, la organización/comunidad educativa fuera objeto de sanción o responsabilidad, o deba abonar alguna indemnización por daños, de cualquier orden, podrá repetir contra el empleado el importe de la cantidad que hubiera tenido que abonar más, en su caso, los gastos que ello le hubiera ocasionado.

5.- **VIGILANCIA Y CONTROL POR PARTE DE COL.LEGI MARE DE DÉU DEL CARME.**

Las herramientas informáticas son puestas a disposición de los empleados por parte de COL.LEGI MARE DE DÉU DEL CARME, con fines exclusivamente profesionales, por lo que éstas deben ser utilizadas única y exclusivamente con tal finalidad, con las excepciones previstas en el presente Protocolo (si se acuerda posible uso personal y privado).

Por ello, COL.LEGI MARE DE DÉU DEL CARME se reserva el derecho de comprobar, cuando lo estime conveniente, si la utilización que se hace de dichos recursos se ajusta a la finalidad que le es propia, y a lo previsto en el presente Protocolo.

Tipos de control:

- ***Procedimiento de control permanente*** y sin previo aviso al empleado a fin de comprobar, a través de los programas necesarios e imprescindibles, la utilización que se esté haciendo de las herramientas informáticas puestas a disposición de los empleados.
- **Procedimiento de control a través del acceso a los equipos informáticos**. Este podrá llevarse a cabo cuando haya indicios de incumplimientos de las medidas establecidas en dicho protocolo, en función de las circunstancias concurrentes, y de acuerdo con el siguiente procedimiento:
    - Se hará siempre en presencia del empleado al que esté asignado el equipo sometido a revisión y dentro de la jornada de trabajo. Si el empleado se negare a ello, se dejará constancia en acta levantada a tal efecto.
    - La revisión se hará a presencia de, al menos, dos representantes legales de los empleados, siempre que el usuario cuyo equipo se va a examinar lo solicite, salvo que aquéllos se negaren a estar presentes.
    - COL.LEGI MARE DE DÉU DEL CARME designará un representante que podrá contar con el apoyo y asesoramiento de una o varias personas con conocimientos informáticos.

- El empleado afectado tiene obligación de facilitar el acceso a su equipo informático, para lo cual proporcionará las claves necesarias. Si el empleado se negare a ello, se hará constar dicha negativa y, en su caso, se podrán adoptar las medidas técnico-informáticas necesarias para ese acceso al equipo y a los diferentes programas.
- Los archivos y demás documentos que se consideren de interés a efectos de probar el incumplimiento, se imprimirán en papel y se firmarán por todos los presentes, quedando bajo la custodia de la Dirección de COL.LEGI MARE DE DÉU DEL CARME. Si alguno de los presentes se negara a la firma se dejará constancia en el acta. Como alternativa a la impresión, cabrá la realización de dos copias de seguridad, quedando una de ellas depositada en lugar que garantice su custodia e intangibilidad. La otra podrá ser objeto de revisión por parte de COL.LEGI MARE DE DÉU DEL CARME.
- Se levantará acta de todo lo acontecido en la que se indicará:
    a) Nombre, apellidos y DNI de los asistentes y calidad en la que están presentes.
    b) Motivo de la revisión y actuaciones que se llevaran a cabo.
    c) Breve descripción del resultado de las actuaciones.
    d) Posibles incidencias

<u>Reglas para la revisión del correo electrónico</u>:

COL.LEGI MARE DE DÉU DEL CARME podrá establecer los mecanismos necesarios para que el sistema informático pueda detectar el número de correos remitidos y direcciones. En cuanto al contenido se distinguirá entre correos personales y no personales.

Respecto a los correos no personales, COL.LEGI MARE DE DÉU DEL CARME tendrá total libertad de revisión.

Respecto a los correos personales solo podrán ser revisados en los siguientes casos:

- Cuando existan indicios razonables de que se está utilizando para cometer infracciones administrativas o penales.
- Cuando pueda razonablemente presumirse la existencia de acoso y otro tipo de actuación delictiva, mediante correo electrónico, a subordinados, clientes, proveedores, o personas vinculadas a COL.LEGI MARE DE DÉU DEL CARME.

La revisión se llevará a cabo en los términos indicados para el acceso a los equipos informáticos.

ANEXO 2: PROPUESTA A SEGUIR EN EL SISTEMA DE INFORMACION A LOS EMPLEADOS

Se aconseja en primer lugar comunicar dichas normas al Comité de Organización/comunidad educativa.

Una vez comunicada e informados a dichos representantes, se dará a conocer todos los empleados a través del medio que se considere más conveniente:

a) Realizar envío de una circular y comunicar que este Reglamento y Política de Uso de TIC's y Protección de Datos Personales, están disponibles en la Intranet de COL.LEGI MARE DE DÉU DEL CARME.

b) Realizar charlas de formación donde se explique estas normas de uso, comunicando que están a su disposición en la Intranet de LA ORGANIZACIÓN/COMUNIDAD EDUCATIVA para su consulta.