NORMATIVA DE SEGURIDAD

Consell Valencià
de Col.legis Veterinaris

DOCUMENTO			
	Tipo	**Grupo**	**Nombre**
Identificación del documento	Documento	Articulado Medidas de Seguridad	Normativa de Seguridad

REGISTRO DE CAMBIOS		
Elaborado	**Revisado por**	**Aprobado por**
Auren	Comité de Seguridad	Responsable de Seguridad

VERSIÓN	FECHA	MOTIVO CAMBIO
1	13/01/2025	Versión inicial

Tabla de contenido

1. INTRODUCCIÓN

El **Consell Valencià de Col·legis Veterinaris** (en adelante, CVCV) ha implantado una serie de medidas técnicas y organizativas encaminadas a garantizar la seguridad de los sistemas y de la información contenida en los mismos. Todo ello en aras de evitar su alteración, pérdida, tratamiento o acceso no autorizado.

La protección a la información referida en el apartado anterior ya sea de carácter personal o de otra índole, comprende tanto la de CVCV (signos distintivos, estrategia de negocio, desarrollo de software, licencias, etc.) como aquella perteneciente a otras instituciones o Administraciones Públicas cedidas por éstas a CVCV para el ejercicio de su actividad profesional.

La implantación de estas medidas tiene los siguientes objetivos fundamentales:

1. Cumplimiento de la normativa de protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (de aquí en adelante, LOPDGDD) y REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (de aquí en adelante, RGPD).
2. CVCV tendrá en cuenta otras normativas como el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia o la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico; así como otras recogidas en el Código de Derecho de la Ciberseguridad cuando así se requiera y le sean de aplicación. También serán de consideración y objeto de estudio las Guías de la Agencia Española de Protección de Datos y los Dictámenes del Grupo de Trabajo del Artículo 29.
3. Cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
4. Cumplimiento de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, por la que se deroga en dos fases la Ley 11/2007, de 22 de junio, de acceso de los ciudadanos a los servicios públicos, y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
5. Mejorar el servicio de la Administración Pública.

La relación y contenido de normas y medidas de seguridad implantadas por CVCV tienen su soporte legal en el cumplimiento del Esquema Nacional de Seguridad y en la normativa vigente en materia de protección de datos.

Todas estas normas son de aplicación tanto para el personal de la plantilla de CVCV como para toda persona perteneciente a otra Organización cuyo trabajo se desarrolle sobre los ordenadores, sistemas de comunicación, redes y/o instalaciones de CVCV.

En ese sentido este documento cumple una doble función identificando la obligación del usuario / persona trabajadora e informar del resto de medidas existentes.

2. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Las obligaciones derivadas de las medidas de seguridad afectan a todo el personal que tratan con el Sistema de Información son:

1. Responsabilizarse del puesto de trabajo que tienen asignado y garantizar que la información que muestran no pueda ser visible por personas no autorizadas. Esto implica que debe adoptarse una política de puesto de trabajo despejado de papeles y de soportes de almacenamiento extraíbles junto con una política de pantalla limpia para los recursos de procesamiento de la información.
2. En el caso de las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.
3. Cuando abandonen su puesto de trabajo, bien temporalmente o bien al finalizar su turno de trabajo, deben dejarlo en un estado que impida la visualización de los datos protegidos, utilizando un protector de pantalla o desconectándose de la aplicación y la red.
4. En el caso de las impresoras deben asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos que contiene, deberán retirar los documentos conforme vayan siendo impresos.
5. Se debe mantener inalterable la relación y configuración de aplicaciones consideradas corporativas (ofimática, antivirus, cliente de correo, etc.) de los puestos de trabajo y sólo podrá ser cambiada bajo la autorización del Responsable de Seguridad o de los administradores autorizados.
6. Deben mantener actualizado el antivirus de su puesto de trabajo. La versión actual de antivirus permite actualizaciones automáticas y desatendidas gestionadas desde el área de Sistemas.
7. Responsabilizarse de la confidencialidad de sus contraseñas y, en caso de que sean conocidas fortuita o fraudulentamente por otras personas, debe comunicarse y registrarse como incidencia de seguridad y proceder a su cambio.
8. Modificar las contraseñas la primera vez que acceden a la red Microsoft y a la Aplicación.
9. Notificar las incidencias de seguridad según se establece en el procedimiento que regula la Notificación y Gestión de Incidencias de Seguridad. El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta por parte de ese usuario. El Procedimiento de Notificación y Gestión de Incidencias de Sistemas y Seguridad está descrito en el presente documento.
10. Se debe evitar almacenar datos afectados por la normativa vigente en materia de protección de datos en ordenadores personales o en cualquier soporte informático sin autorización expresa, y siempre mediante el uso de medidas de seguridad adecuadas.
11. El usuario deberá ser responsable del Software que instale en su ordenador para el ejercicio normal de su trabajo, evitando la instalación de aplicaciones que puedan resultar perniciosas para el correcto funcionamiento del mismo.

3. PROPIEDAD Y USO DE LOS ORDENADORES PERSONALES

CVCV facilita a los usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Este equipamiento es propiedad de CVCV y por tanto no está destinado a un uso personal. Como consecuencia de esto, CVCV se reserva el derecho de revisar, sin previo aviso, los equipos, el uso de Internet y el teléfono corporativo que esté haciendo uso cada usuario, en caso de que existieren indicios de que se está llevando a cabo una utilización indebida. De esta forma el usuario queda informado de que el resultado de los controles efectuados puede ser utilizado para llevar a cabo, en su caso, las actuaciones disciplinarias previstas por la normativa vigente.

El área de Sistemas del Dpto. de Informática o el proveedor TI que preste estos servicios, 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 usuarios deben cumplir las siguientes medidas de seguridad 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 del área de Sistemas.
- 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 área de Sistemas para que tome las medidas oportunas.
- Los ordenadores portátiles Tablets o Smartphones, 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 CVCV 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 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 CVCV 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:
    - Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red de CVCV.
    - Intentar modificar o acceder al registro de accesos.
    - Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros
    - 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 este Organismo, o bien para la realización de actos que pudieran ser considerados ilícitos.
- Queda prohibido terminantemente la apropiación de archivos o ficheros titularidad de CVCV 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 este Organismo en ordenador propio, 'pendrives' o a cualquier otro soporte informático, salvo que solicite autorización al Responsable de Seguridad, con la finalidad de que disponga de información sobre ese soporte. Los datos contenidos en este tipo de soportes deben ser suprimidos 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 archivos permanezcan en el equipo o soporte informático externo, 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 este Organismo y dispuesto a razón única de las funciones o tareas desempeñadas en CVCV. 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.

4. NORMAS DE USO DE DISPOSITIVOS MÓVILES

A continuación, se detallan una serie de normas a seguir por los usuarios que bien tienen asignado un dispositivo móvil (Smartphone, Tablet o portátil) o utilicen uno de itinerancia (préstamo con registro firmado):

- El usuario prestará especial atención al dispositivo en dependencias de libre acceso, como aeropuertos, estaciones, hoteles, etc.
- La asignación o préstamo del mismo tiene como finalidad que el usuario desempeñe actividades profesionales vinculadas a CVCV.
- El dispositivo deberá tener obligatoriamente activada la protección por contraseña o huella dactilar si lo permite.
- En el caso de que el usuario se ausente temporalmente, dejará el terminal bloqueado (sesión de usuario Windows o código en Smartphone/Tablet). Si el tiempo de ausencia es mayor, en cuanto al portátil, deberá dejarlo apagado y en lugar seguro.
- Se debe evitar almacenar datos de carácter personal. Si esto fuera estrictamente necesario, se solicitará al Responsable de Seguridad para que se proceda al cifrado de la unidad que vaya a contener dichos datos.

4.1. Procedimiento de actuación en caso de pérdida o robo

Ante el caso de pérdida o robo, se debe avisar inmediatamente al Responsable de Seguridad para que ordene al operador de comunicaciones el bloqueo del terminal si procede, y registrar una incidencia, tal y como se describe en el apartado 10 de este documento.

5. USO DE LA RED CORPORATIVA

La red corporativa es un recurso compartido y limitado.

Los usuarios deben cumplir las siguientes medidas de seguridad para el uso de la red corporativa:

- La utilización de Internet por parte de los usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, 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. En este sentido se prohíbe el uso de Internet para fines no relacionados con las funciones encomendadas en cada puesto. **CVCV** podrá controlar el uso de acceso a Internet proporcionado.
- Se prohíbe el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.
- La normativa completa sobre el uso de Internet puede consultarse en el apartado “normas de uso de Internet” dentro del presente documento.
- 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. **CVCV** se reserva el derecho de que el Responsable de Seguridad o el Responsable del Sistema pueda revisar y controlar el uso correcto del correo electrónico corporativo.
- Los envíos masivos de información, así como lo correos que se destinen a gran número de usuarios serán solo los estrictamente necesarios, para evitar que 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.
- La normativa completa sobre el uso del correo electrónico se detalla en el apartado “normas de uso del correo electrónico” descrito en el presente documento.

6. NORMAS DE USO DE INTERNET

Con carácter general, los usuarios del **CVCV** disponen de acceso a Internet como herramienta de productividad y conocimiento, así como de mejora de los sistemas de trabajo y búsqueda de información. Esta herramienta es propiedad de la entidad, la cual se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes. Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

- Seguridad: debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- Volumen del tráfico externo de datos: garantizando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de **CVCV**.
- Volumen del tráfico interno de datos: como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- Ética: es ineludible el compromiso que **CVCV** debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

Con el despliegue de las TIC y, en particular, con el desarrollo de Internet como herramienta de comunicación global, se han extendido igualmente las amenazas que pueden poner en peligro los sistemas de información de las organizaciones.

En este sentido, se incluye un conjunto de normas y medidas de seguridad que tienen como objetivo reducir los riesgos derivados por el uso de Internet:

- Utilizar Internet para fines profesionales. Se trata de una herramienta más de las utilizadas por los usuarios de **CVCV**, por lo que debe usarse de manera responsable. Por tanto, el servicio de Internet no debe de ser usado para fines personales, quedando estrictamente prohibido el uso de redes *peer-to-peer* (P2P) tipo emule, edonkey, kazaa, bitcomet, bittorrent, soulseek o de descarga de música, videos, juegos, software, visitar paginas para adultos y/o de sexo explícito, ya que este tipo de prácticas tienen el riesgo de contener virus, spyware y otro tipo de aplicaciones, que pueden reducir el rendimiento de las aplicaciones y el servicio de Internet.
- No descargar código o programas no confiables. Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas. Tales actividades deben ser acometidas, de manera exclusiva, por el área de Informática.
- Cuidar la información que se publica en Internet. No se debe proporcionar información sobre **CVCV** en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta. En este sentido, está prohibido difundir sin autorización cualquier tipo de información no pública sobre el funcionamiento interno de **CVCV**, sus recursos, estructura, etc.
- El usuario debe minimizar el tráfico de red innecesario que pueda interferir en la capacidad de otros usuarios de utilizar de forma eficaz los recursos de red. Se debe tener en consideración que la descarga de archivos de audio o vídeo puede ir en detrimento del rendimiento de los recursos informáticos y, por ello, se debe limitar su descarga y reproducción.

- Asegurar la autenticidad de la página visitada. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones (ataque conocido como *phishing*). Cuando la página web se encuentre autenticada mediante certificado digital, el usuario verificará su autenticidad.
- Comprobar la seguridad de la conexión. En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar su cifrado. Una manera de asegurar la confidencialidad es comprobar que se utiliza protocolo HTTPS en la comunicación en vez del protocolo estándar http (examinando la barra de direcciones). También debería aparecer un icono representando un candado en la barra del navegador. A través de dicho candado se puede obtener información sobre el certificado digital de identidad del sitio web visitado.
- Cerrar las sesiones al terminar la conexión. Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información, ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador. Esto puede hacer que otros usuarios tengan acceso a las cuentas de los usuarios que no hubieren cerrado correctamente las sesiones. La mayoría de los sitios web disponen de una opción de "cierre de sesión", "desconexión", "*logout*" o similar que conviene utilizar.
- Mantener actualizado el navegador y las herramientas de seguridad. Es imprescindible actualizar las herramientas de acceso a Internet (navegadores) y de seguridad (antivirus, cortafuegos, etc.) a las últimas versiones estables, siempre de conformidad con lo indicado y aprobado por el área de Informática. Puesto que el código dañino se genera incesantemente, es muy importante actualizar las firmas de virus con la mayor frecuencia posible. Los sistemas deben estar configurados para realizar esta tarea de forma automática. Asimismo, es muy importante informar sobre cualquier problema que se detecte en este proceso.
- Utilizar los niveles de seguridad del navegador. Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.
- Eliminar la información privada. Los navegadores almacenan información privada durante su utilización, tal como el historial de navegación, cookies aceptadas, contraseñas, etc.; información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.
- No instalar complementos desconocidos. Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador del usuario un complemento (*plug-in*, *add-on*, etc.) para poder acceder al contenido. Es muy recomendable analizar primero la conveniencia de instalar tal complemento y hacerlo, en cualquier caso, siempre desde la página del distribuidor o proveedor oficial del mismo.
- El acceso y uso de Internet no podrá ser utilizado con fines comerciales o lucrativos en beneficio del usuario. Asimismo, queda prohibida cualquier actividad que infrinja o no haga un

uso apropiado de los derechos de propiedad intelectual de un tercero, como copyright, marcas registradas, secretos comerciales, piratería de software, patentes, etc.

- Se prohíben todas aquellas actividades que tengan por misión fines ilícitos, de acceso no autorizado, de robo, bloqueo o daño de información, sobrecarga o deterioro de los servicios, sistemas, redes, y de los equipos con o sin ocultación de su identidad, evitando las medidas de seguridad si las llevara implementadas, vulnerando las condiciones de uso de los mismos o sus derechos reconocidos y/o amparados por la legislación.
- **CVCV se reserva el derecho de monitorizar y comprobar**, de forma aleatoria, cualquier sesión de **acceso a Internet** iniciada por un usuario de la red corporativa, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a **CVCV** como responsable civil subsidiario.

7. ACCESOS REMOTOS

Para acceder a servicios protegidos de la red interna, así como para atravesar los filtros especiales impuestos a algunas de ellas, se dispone de varios servidores de túneles VPN.

8. NORMAS DE USO DEL CORREO ELECTRÓNICO

8.1. Normas de uso

El correo electrónico (e-mail) es un servicio de red para permitir a los usuarios de **CVCV** enviar y recibir mensajes. Junto con los mensajes también pueden ser enviados ficheros adjuntos. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

Es importante entender que el servicio de correo o SMTP, fue desarrollado en la década de 1980 utilizando codificación ASCII de 7 bit para el envío de mensajes de texto. Posteriormente se fueron añadiendo nuevas funcionalidades tales como la posibilidad de enviar ficheros anexados. Esto ha provocado que para poder enviar ficheros binarios sobre código ASCII de 7 bit, se necesite un protocolo de codificación llamado MIME que puede aumentar en promedio entre un 20-40% el tamaño de los ficheros anexos. Es decir, un anexo de 10MB, se podría convertir en 14MB de tráfico. Los servidores de correo, en función de sus políticas, imponen siempre una limitación en el tamaño de los mensajes adjuntos, por lo que un mensaje podría ser rechazado por exceso de tamaño.

En este sentido, se incluye un conjunto de normas que tienen como objetivo reducir el riesgo en el uso del correo electrónico:

- La utilización del sistema de correo electrónico puesto a disposición del usuario se encuentra limitada exclusivamente a actividades profesionales, no permitiéndose su utilización para fines diferentes a los que se desprenden del cargo ocupado por cada empleado. Gran parte de los mensajes de correo electrónico no deseados que lleguen a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo. Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de ataque.
- Utilizar el servicio de correo electrónico corporativo como medio de comunicación, quedando prohibida la instalación y uso de cualquier otra aplicación de correo electrónico, así como de una versión diferente de la aplicación homologada que no haya sido autorizada e instalada por el personal técnico autorizado.
- Utilizar contraseñas seguras. Para limitar la posibilidad de un acceso no autorizado a las cuentas de correo electrónico, es muy importante utilizar contraseñas robustas.
- Se entiende que una contraseña es robusta cuando posee, al menos, 8 caracteres (compuestos por letras mayúsculas y minúsculas, dígitos y signos especiales), evitando que la contraseña obtenida sea una palabra de un diccionario, una fecha o, de alguna manera, esté relacionada con el usuario (NIF, nombres propios y apellidos, nombres de mascotas, nombres de ciudades o países, nombres de personajes famosos, deportistas, etc.). Para evitar la problemática derivada de la necesaria memorización de las contraseñas, un mecanismo muy útil puede ser seleccionar un carácter de cada palabra de una frase conocida y fácilmente memorizable.
- No ceder el uso de las cuentas de correo. Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales -para los que deberá solicitarse y obtenerse la correspondiente autorización-, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información

confidencial. Además de ello, es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios.

- No emplear el correo electrónico como medio de comunicación para enviar o recibir información confidencial o que contenga datos de carácter personal de nivel alto (datos de salud, ideología, afiliación sindical, religión, creencias, origen racial, vida sexual, violencia de género, fines policiales). Únicamente, y en aquellos casos en los que sea estrictamente necesario, se utilizará este medio, en cuyo caso, se enviará con las medidas de seguridad apropiadas para cada tipo concreto de información mediante la utilización de un software de cifrado, normalmente WinZip con AES 256, previa autorización expresa del responsable de seguridad.
- Cuando se envíen correos electrónicos al exterior con ficheros adjuntos voluminosos, deben comprimirse dichos ficheros antes de ser adjuntados. Con esta medida se consigue reducir el consumo de recursos y acelerar el tiempo de recepción del fichero.
- Cuando se desee compartir un fichero con otro usuario dentro de los sistemas de **CVCV**, deberá evitarse en la medida de lo posible el uso del correo electrónico. En su lugar, deberá depositarse el fichero en un recurso compartido de red y notificar al receptor su localización usando el correo electrónico. De este modo se reduce considerablemente el uso de recursos de correo electrónico.
- Prestar especial cuidado con las respuestas a correos en las que se incluye el envío original y los ficheros adjuntos. El fichero adjunto deberá eliminarse de la respuesta que se dé a un correo electrónico, debido a que resulta redundante y supone un incremento en el consumo de recursos.
- **Evitar abrir archivos adjuntos sospechosos**. Nunca deben ejecutarse los archivos adjuntos recibidos. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el remitente del correo es sospechoso. Gran parte del código malicioso, especialmente el **Ransomware** suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).
- En el caso de se requiera enviar un mensaje de correo electrónico a varios destinatarios, **se utilizará el campo CCO** (copia oculta) para introducir las direcciones de correo de los destinatarios, con excepción de aquellos mensajes en los que necesariamente se requiera la identificación de todos los destinatarios para confirmar que han sido informados.
- Comunicar al área de Sistemas, mediante el registro de la correspondiente incidencia, toda recepción de mensajes de correo electrónico de distribución masiva sin relación con el desempeño de sus funciones, así como virus y correos electrónicos no deseados (*spam*). Esta regla es de especial aplicación al correo publicitario masivo y a las denominadas “cartas encadenadas”. En ningún caso debe responderse a este tipo de envíos.
- Depurar periódicamente el buzón de correo electrónico, eliminando los mensajes innecesarios y transfiriendo aquellos documentos cuyo almacenamiento sea realmente necesario a los recursos individuales que tienen a su disposición en los servidores de ficheros.
- No utilizar el servicio de correo electrónico de **CVCV** en actividades que puedan ser consideradas ilícitas o ilegales, como puede ser: enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario, enviar cualquier comunicación electrónica fraudulenta, enviar mensajes de correo electrónico

usando el nombre o la dirección de terceros, con el fin de engañar al destinatario sobre el remitente de los mismos.

En relación con el acceso remoto (vía web) al correo electrónico, deben adoptarse las siguientes cautelas:

- Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.
- Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
- Desactivar las características de recordar contraseñas para el navegador.
- Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.

Ante una situación excepcional, en los supuestos de ausencia temporal, suspensión de la relación laboral/contractual o extinción de la misma de cualquier persona trabajadora/colaborador, el supervisor o responsable podrá solicitar a la persona responsable del sistema el acceso al buzón de correo de la persona trabajadora/colaborador, con el fin de dar continuidad a los servicios prestados por **CVCV**.

CVCV se reserva el derecho a revisar los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a **CVCV** como responsable civil subsidiario.

8.2. Prevención contra ‘spam’

El término ‘spam’ se define como el envío de correos no solicitados, de forma masiva, a direcciones de correo electrónico, constituyendo uno de los problemas de seguridad más habituales con los que se enfrentan las organizaciones. Tales mensajes pueden contener código dañino que, de penetrar en los sistemas de información, podrían llegar a colonizar una institución y propagarse a través de las redes de comunicaciones.

Además de las medidas técnicas de prevención y eliminación de ‘spam’ ya implantadas en **CVCV**, se detallan a continuación las normas que todo usuario deberá seguir para hacer frente a este problema:

- Con carácter general, sólo se proporcionará la dirección de correo electrónico profesional de **CVCV** a personas de confianza y del entorno profesional.
- Se debe evitar introducir la dirección de correo de **CVCV** en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios y con proveedores de confianza. Muchos ataques de ‘spam’ se sirven de estas direcciones, introducidas en sitios no seguros.

- Con carácter general, si no se conoce el remitente de un correo, y/o el asunto del mismo es extraño, se recomienda borrar el mensaje (o situarlo en cuarentena hasta disponer de más datos), especialmente si contiene ficheros adjuntos.
- Si el usuario identifica un mensaje como 'spam', deberá:
    - Si lo reconoce como tal por la dirección o el asunto que contiene, borrarlo inmediatamente (sin abrirlo).
    - No responder nunca al mensaje.
    - No acceder a los enlaces o documentos anexos que pudieran contener.

9. ELIMINACIÓN DE METADATOS

9.1. Introducción

Los archivos utilizados para el intercambio de información proporcionan a menudo información complementaria donde pueden aparecer datos como el nombre del autor, dirección de correo, ruta de ubicación del archivo, nombre del dominio etc.…

Estos datos pueden ser explotados por terceros con fines fraudulentos, tales como 'spam' o el progreso de ataques que consigan comprometer los servicios, partiendo de la información interna facilitada. Esta información adicional, que no aparece dentro del propio fichero, recibe el nombre de metadatos.

Se describe a continuación el procedimiento de eliminación de metadatos que deberá ser aplicado a todos aquellos documentos que deban ser enviados a terceros fuera de la organización.

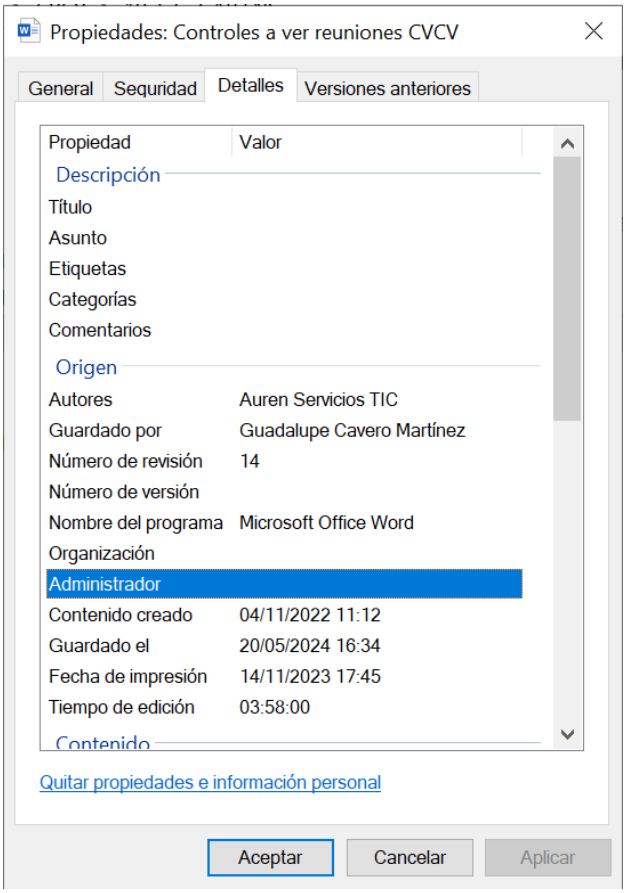
Los tipos de documentos susceptibles de ser 'limpiados' son:

- Archivos PDF
- Archivos Word
- Hojas de Cálculo
- Archivos de Base de Datos (Access)
- Archivos de presentaciones (.ppt)

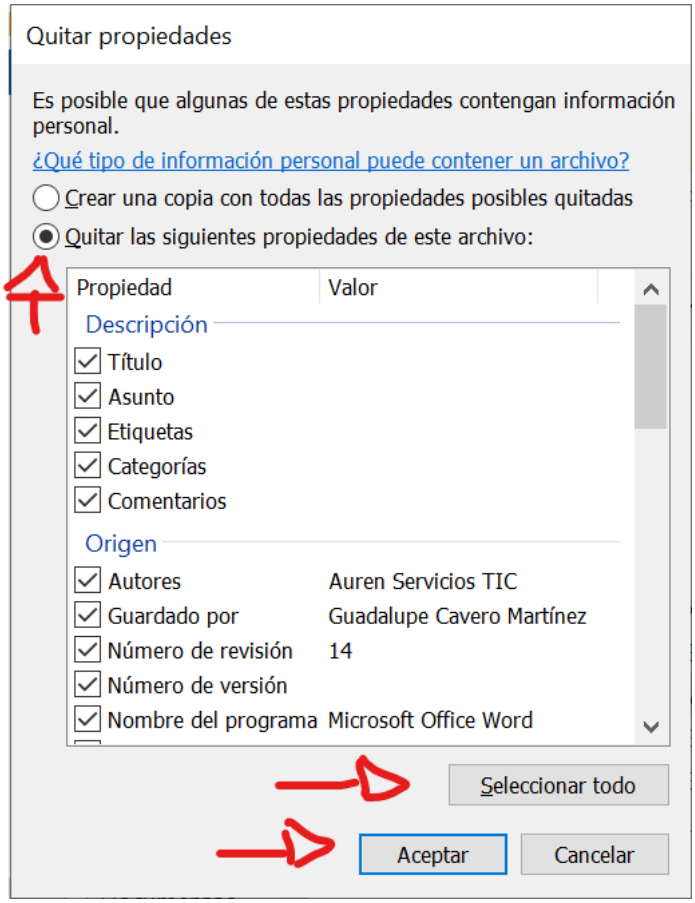
9.2. Procedimiento

Para eliminar los metadatos asociados a los documentos ofimáticos que se envían a terceros, fuera de la red de datos de **CVCV**, se procederá del modo siguiente:

Desde una ventana del administrador de archivos, se pulsa el botón 'propiedades' del archivo a enviar.



Seleccionando la pestaña ‘detalles’, puede observarse la lista de metadatos asociada al documento. Pulsando la opción ‘Quitar propiedades e información personal’, aparece la siguiente ventana:



Seleccionando la opción “Quitar las siguientes propiedades de este archivo”, y luego pulsando sobre los botones “seleccionar todo” y “Aceptar”, habremos eliminado todos los metadatos asociados al archivo.

En caso de necesitar mantener algún tipo de información no comprometedora, es posible seleccionar de forma selectiva aquellas propiedades que se deseen mantener.

10. PROCEDIMIENTO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

Una incidencia se puede definir como cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos. Controlar, analizar y prevenir estas anomalías es crucial para asegurar correctamente el grado de protección deseado en cuanto a confidencialidad, disponibilidad e integridad se refiere.

El procedimiento de **Notificación y Gestión de Incidencias** describe el flujo de comunicación, la operativa y los actores que deben gestionar los aspectos relacionados con las incidencias de seguridad que puedan afectar al Sistema de Información de **CVCV**.

Las incidencias se deberán notificar a través de correo electrónico a mhernandez@auttic.com.

11. ACCESO A APLICACIONES Y SERVICIOS

Tanto el equipamiento informático como todos los recursos facilitados al usuario para la realización de las tareas relacionadas con su puesto de trabajo (tales como teléfonos móviles, aplicaciones, servicios, etc.) son propiedad de **CVCV**, por lo que deberá hacerse un uso diligente de los mismos. En este sentido se le informa de que podrá revisarse la utilización que cada usuario esté haciendo de los teléfonos móviles facilitados para el desempeño de su puesto de trabajo. En caso de que existieran indicios acerca del uso indebido de los mismos, podrá realizarse un control de la facturación, así como de los destinatarios de las llamadas realizadas.

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 usuarios deben cumplir las siguientes medidas de seguridad establecidas por **CVCV** 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 usuarios 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, habilitar el protector de pantalla con bloqueo con contraseña, y apagar los equipos al finalizar la jornada laboral.

Excepto en los casos en que el equipo deba permanecer encendido.

12. ACCESO Y TRATAMIENTO DE DATOS A NIVEL INFORMÁTICO Y EN PAPEL

12.1. Tratamientos Automatizados

En particular, respecto a la información de carácter personal contenida en soportes 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 usuarios** para acceder al sistema informático. En caso de que fuera necesario acceder al sistema, en ausencia de un compañero, se solicitará al área de Sistemas para que se habilite el acceso eventual. Una vez finalizada la/s tarea/s que motivaron el acceso, deberá ser comunicado, de nuevo, al área de Sistemas.
- **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 o comparta oficina con otros usuarios o no cierre la puerta de su despacho.
- **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 **CVCV** 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 usuarios a los diferentes ficheros son concedidos por **CVCV**, en concreto por el área de Sistemas. 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 servicio.
- **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 área de Sistemas, para adoptar las medidas oportunas sobre el mismo. Esto resulta también de aplicación a los documentos que se fotocopien
- **No utilizar el 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 de cifrado recomendados por el área de Sistemas

necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

- **No conservar documentos ofimáticos con datos de salud o sindicales.**- Estas herramientas de uso común no permiten disponer de la medida de seguridad que corresponde a estos datos de nivel alto relativa al mantenimiento de un registro de los accesos realizados por los usuarios (*log*). En estos casos resulta más seguro disponer de esta información únicamente en papel, si no se dispone de una herramienta informática que permita registrar dicha información para cumplir con la normativa. Pudiéndose utilizar únicamente plantillas de documentos ofimáticos, pero sin que los mismos conserven datos personales.
- Con relación a los soportes informáticos que pudieran almacenar información (*pendrives* y discos duros externos USB, CDs, DVDs, disquetes, etc.):
    - La salida de soportes que contengan datos confidenciales o especialmente protegidos fuera de los locales de **CVCV** precisa de autorización previa por parte del Responsable de Seguridad. Una vez comunicada la salida de soportes por parte del usuario, y autorizada por el Responsable de Seguridad, el Responsable de Seguridad o el Jefe del área de Sistemas procederá a anotarla en el registro de entrada y salida de soportes.
    - La entrada de soportes deberá ser comunicada al Responsable de Seguridad con la finalidad de que se anote en el registro de entrada y salida de soportes. Una vez procesado, el soporte recibido deberá ser borrado completamente.
    - Queda terminantemente prohibido el uso de unidades de almacenamiento de la información externas para uso privado como por ejemplo disquetes, pendrives, discos duros externos, CD-R, DVD-R, etc., salvo autorización explícita del Responsable de Seguridad.
    - Queda terminante prohibido facilitar a persona alguna ajena a **CVCV** ningún soporte conteniendo datos a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.
    - En caso de necesitar desechar un soporte con información, se destruirá mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. También deberá procederse al borrado previo de la documentación cuando el soporte vaya a reutilizarse. Para ello, el usuario deberá dirigirse al Responsable de Seguridad o al Jefe del área de Sistemas para su adecuado borrado.
- **Comunicación de incidencias que afecten a la seguridad de datos de carácter personal.-** Comunicar al área de Sistemas las incidencias de seguridad de las que tenga conocimiento, que puedan afectar a la seguridad de los datos personales. Esto resulta también de aplicación a la información en papel.

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 usuarios a ficheros excediendo sus perfiles.
- Pérdida de soportes informáticos o documentos en papel 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.
- Documentos que se hallen en papeleras con datos personales.

12.2. Tratamientos No Automatizados

En relación con los ficheros en soporte o documento papel, el usuario deberá observar las siguientes diligencias indicadas anteriormente con respecto a la confidencialidad de la información, acceso autorizado a la información en atención a las necesidades de su trabajo, gestión de soportes y documentos, trabajo fuera de las instalaciones de **CVCV**. Asimismo, con carácter especial y únicamente de aplicación a los ficheros en papel, el usuario deberá cumplir además 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 de trabajo 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 de trabajo. 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. Asimismo, el archivo de la documentación se realizará siguiendo los criterios establecidos por **CVCV**, para garantizar su correcta conservación.
- **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 destructora de papel u otro medio que disponga **CVCV**. 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 **CVCV**. 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 hubiera 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 procurará 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 **CVCV** 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.
- Mantenimiento de los registros de accesos a la documentación con datos especialmente protegidos -datos sindicales y de salud-, siempre y cuando vayan a ser utilizados por varios usuarios.
- **Comunicación de incidencias que afecten a la seguridad de datos de carácter personal.-** Comunicar al área de Sistemas las incidencias de seguridad 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 tratamientos no automatizados**,** 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 usuarios 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.

13. NORMAS DE CUMPLIMIENTO DE LA LEY DE PROPIEDAD INTELECTUAL

Con el fin de llevar a cabo un cumplimiento del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, todo el personal de **CVCV** se compromete al cumplimiento de las siguientes medidas:

- Queda prohibido que las personas trabajadoras, directivos o representantes de **CVCV**, hagan uso de patentes o marcas registradas sin disponer de las licencias correspondientes.
- Asimismo, tampoco se podrá hacer uso de una patente o marca registrada de un tercero, para finalidades comerciales, sin el consentimiento previo del titular.
- Queda prohibido la utilización de programas tendentes a vulnerar las protecciones de un programa informático, con la finalidad de proceder de forma ilegal a su copia e instalación en los equipos de la empresa. Es por ello que se deberá promover dentro de **CVCV** un uso legítimo de todos aquellos programas utilizados para el desarrollo de las funciones propias de cada uno, a través de la solicitud de la correspondiente licencia.
- Por último, se prohíbe el uso de todo tipo de material (textos, imágenes, etc.), que no sean creación por parte del personal de **CVCV**.