**Política de buenos usos a protección de datos**

1. **Objetivo, alcance y ámbito de aplicación.**

La presente política de buenos usos se ha realizado con el objetivo de mantener un buen nivel de protección sobre la información y/o datos de carácter personal de COMEVA, con el fin de evitar un posible abuso por parte de aquellos proveedores, Colegiado, y/o terceros, que accedan a la misma utilizando los recursos facilitados por la propia organización. Es por ello que, con esta política, se pretende garantizar la seguridad, rendimiento, fiabilidad y privacidad de las comunicaciones, así como de la información y datos de carácter personal almacenados en los recursos propiedad de **COMEVA** y puestos, en su caso, a disposición de terceros.

Los proveedores, Colegiado, y/o terceros, únicamente podrán hacer uso de los recursos a los que **COMEVA** facilite acceso, en cumplimiento de lo aquí dispuesto, en cumplimiento de lo dispuesto en el Contrato Principal que regule la relación entre ambas partes y en cumplimiento de lo dispuesto en el contrato con acceso a datos personales o de cesión de datos firmado entre las partes; no pudiendo bajo ningún concepto utilizar los datos personales, o en su caso, recursos, sistemas y medios de comunicación que, **COMEVA**, ponga a su disposición para cuestiones ajenas al Contrato Principal.

En concreto, el acceso a la plataforma web de **COMEVA** y/o en su caso, el otorgamiento de un correo electrónico corporativo es propiedad de **COMEVA** y no deberán ser considerados como elementos de comunicación personal.

Este documento será de aplicación a proveedores, Colegiado, y/o cualquier otro tercero que tengan acceso a los recursos tecnológicos propiedad de **COMEVA**. Dicho acceso incluye todos los sistemas de información propiedad de la organización, en su caso, equipos informáticos (PC`s, dispositivos móviles, servidores), infraestructura de comunicaciones, conexión a redes internas o externas, terminales, software, hardware, soportes de información, servicios telemáticos, infraestructura de redes, accesos a Internet y todos los recursos a los que tenga acceso el proveedor, Colegiado, y/o tercero para cumplir con el Contrato Principal.

El uso inapropiado, abusivo o que exceda de los hábitos tolerados en el uso de los servicios de comunicación y de los medios tecnológicos, será sancionado con la eliminación del acceso a los recursos y, en su caso, con la rescisión del Contrato Principal por incumplimiento de las Condiciones derivadas del mismo.

**COMEVA** podrá realizar las revisiones y controles necesarias tanto en equipos como enherramientas facilitadas a proveedores, Colegiado, y/o terceros en aras a comprobar el cumplimiento del Contrato Principal y lo aquí dispuesto, siempre sin atentar ni dañar la dignidad o intimidad del usuario y, siendo las finalidades no exhaustivas de dicho control, las siguientes:

* Protección del sistema y red informática y de los equipos que lo conforman, a fin de mantener la integridad y seguridad de los sistemas y de la información.
* Garantizar la continuidad del trabajo en el caso de que el proveedor, Colegiado, y/o tercero cese la relación contractual con **COMEVA.**
* Prevención de responsabilidad frente a terceros.
* Comprobar el cumplimiento de las obligaciones contractuales con el proveedor, Colegiado, y/o tercero.
* Comprobar la existencia o no del uso abusivo de los medios tecnológicos facilitados al proveedor, Colegiado, y/o tercero por parte de **COMEVA**.

En conclusión, los contenidos, informaciones y ficheros almacenados en los equipos y/o recursos informáticos facilitados por **COMEVA** al proveedor, Colegiado, y/o tercero, incluida la información temporal, podrán ser accedidos por **COMEVA** o por los responsables designados por ellos al efecto.

1. **Obligaciones y deberes de los proveedores, Colegiado, es y/o terceros.**

Los proveedores, Colegiado, es y/o terceros que tengan acceso a los recursos y sistemas de información de **COMEVA** para cumplir con el Contrato Principal, se comprometen a respetar su integridad, quedando prohibido llevar a cabo o facilitar a cualquier tercero la ejecución de:

* Dar acceso a la plataforma web o a cualquier otro recurso de **COMEVA** a terceros sin seguir el procedimiento de solicitud de permisos establecido por **COMEVA**, y, por tanto, sin obtener previamente autorización.
* Hacer modificaciones de privilegios o permisos sin autorización del administrador de sistemas.
* Ocasionar daños físicos o lógicos, por mal uso o negligencia de los equipos informáticos, aplicaciones, herramientas informáticas, soportes de información y todo dispositivo o medio tecnológico.
* Desarrollar llar o usar programas maliciosos o acceder a recursos restringidos por el administrador de sistemas.
* No guardar con la debida diligencia las claves, contraseñas, nombres de usuario o cuales-quiera otros identificadores que pudieran facilitarse al proveedor, Colegiado, y/o tercero para utilizar cualquiera de las herramientas, o para acceder a los equipos o sistemas de **COMEVA**. En ningún caso se facilitará esta información a terceros.
* Acceder sin autorización a las comunicaciones que circulan por la red, así como su manipulación, destrucción/borrado y/o apropiación indebida.
* Extraer información de **COMEVA** en cualquier tipo de soporte sin la debida autorización de **COMEVA**.
* El borrado masivo y malintencionado de documentos, datos y/o cualquier información de interés para **COMEVA**. Para borrar documentos, datos y/o cualquier información de la plataforma web, se deberá obtener permiso del Responsable de Seguridad o del Administrador de sistemas.
* Guardar documentos ofimáticos o de interés para **COMEVA** fuera de las ubicaciones indicadas por los Responsables de Seguridad y/o Administradores del Sistema.
* Transmitir, tratar o crear material que infrinja el 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, o lo dispuesto en la ley de Propiedad Intelectual.
* Facilitar acceso a los recursos y/o instalaciones de **COMEVA**, a personas no autoriza-das.
* Malgastar recursos de red de forma premeditada como son envío de correos electrónicos masivos en nombre de **COMEVA** o de cualquier otra forma, descarga de grandes ar-chivos, uso de programas de intercambio de archivos, etc.
* Corromper o destruir datos de otros usuarios o violar su privacidad de forma intencionada.
* Introducir de forma deliberada un virus o cualquier otro software malicioso.
* Revelar las contraseñas y medios de acceso a los recursos de **COMEVA** a terceros no autorizados.
* Utilizar los activos tecnológicos de **COMEVA** para lucro personal y más allá de lo es-tablecido en el Contrato Principal.
* Crear, utilizar y/o transmitir material ofensivo y/u obsceno.
* No verificar la correcta actualización de las herramientas antivirus y otros sistemas de pro-tección adoptados por la Organización.
* Las anteriores restricciones y prohibiciones regirán tanto para los accesos de los recursos informáticos de **COMEVA**, pese a que estén conectados a través de VPN u otros me-dios.
1. **Accesos a los equipos.**
	1. **Acceso de los usuarios.**

El acceso a los sistemas de información, tales como la plataforma web de **COMEVA,** está controlado y autorizado por el administrador de sistemas y por el Responsable de Seguridad, quedando estrictamente prohibido para el proveedor, Colegiado, y/o tercero, intentar acceder a aquellos sistemas o recursos sobre los que no tenga autorización expresa y fehaciente por parte del Responsable de Seguridad.

Además, el proveedor, Colegiado, y/o tercero, deberá respetar los derechos de terceros en caso de que tengan acceso compartido, comprometiéndose a no acceder a la información privada de otros usuarios sin previa autorización. Igualmente se comprometen a no compartir ficheros o documentos de cualquier tipo con otros usuarios sin implementar las medidas necesarias que garanticen la seguridad de la información y de los sistemas informáticos.

Toda suplantación de identidad será sancionada de acuerdo con la normativa vigente que resulte de aplicación.

Los proveedores, Colegiado, y/o terceros, accederán a los sistemas informáticos de **COMEVA** con un nombre de usuario y contraseña que son personales e intransferibles, comprometiéndose a tratarla con la máxima confidencialidad, y siendo los únicos responsables del buen uso de la misma. El titular autorizado será responsable único y directo de todo lo ejecutado en el sistema bajo su nombre de usuario y contraseña, quedando prohibido el intento para obtener el acceso de contraseñas de otros usuarios.

Queda prohibido divulgar por cualquier medio las claves de acceso a cualquiera de los servicios que se facilite al proveedor, Colegiado, y/o tercero. Todos los nombres de usuario, contraseñas, claves de acceso y demás identificadores facilitados a los usuarios tendrán el carácter de confidencial, resultando personales e intransferibles.

Los usuarios se comprometen a dar aviso al Administrador de Sistemas y/o al Responsable de Seguridad de **COMEVA** y de manera inmediata, de cualquier incidencia, anomalía o punto débil en la seguridad, detectada en los accesos que haga a los sistemas de información.

En caso de que el proveedor, Colegiado, y/o tercero, requiera diversos usuarios para cumplir con el Contrato Principal, deberá comunicarlo previamente a **COMEVA**, para que, en caso de ser necesario, se faciliten tales usuarios de manera que siempre quede constancia de la persona/usuario que accede a los sistemas de información de **COMEVA** y de qué hace durante tales accesos.

1. **Protección de la información.**
	1. **Puesto de trabajo despejado.**
2. **Bloqueo del puesto de trabajo.**

En caso de que el proveedor, Colegiado, tercero y/o usuario de éstos autorizado, tenga que ausentarse de su puesto de trabajo, deberá bloquear la sesión de forma que ningún otro usuario o tercero pueda acceder al equipo.

Automáticamente se bloqueará la sesión tras un período de inactividad y para desbloquearlo se necesitará iniciar sesión nuevamente mediante usuario y contraseña.

1. **Destrucción y borrado de información.**

Los documentos en papel y soportes electrónicos (CD, pendrive, discos duros, etc.), no se desecharán si los mismos contienen datos de carácter personal. Para su destrucción se deberán seguir procedimientos de borrado y/o destrucción seguros y, en su caso, proceder a la certificación de dicha destrucción.

**5. Asignación de claves y políticas de contraseñas.**

1. **Procedimientos de asignación de contraseñas.**

Cada usuario con acceso autorizado a los sistemas de información de COMEVA, dispondrá de un nombre de usuario personalizado y de una contraseña para autenticarse en los sistemas de información. La comunicación del nombre de usuario y contraseña será proporcionada por el Responsable de Seguridad, garantizando su confidencialidad y secreto y, facilitando al usuario la posibilidad de modificar posteriormente dicho nombre de usuario y contraseña.

Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

Por otro lado, y cuando el mismo ordenador o dispositivo sea utilizado por el proveedor, colaborador, y/o tercero para el tratamiento de datos personales y para fines de uso personal, deberá disponerse de varios perfiles o usuarios distintos para cada una de las finalidades; debiendo mantenerse separados los usos profesional y personal del ordenador.

1. **Gestión de incidencias.**

Cualquier incidencia o vulnerabilidad detectada por el proveedor, Colegiado, y/o tercero, en la utilización de los recursos y medios tecnológicos de **COMEVA**, deberá ser notificada a la mayor brevedad al Responsable de Seguridad, que será el encargado de registrar la incidencia y hacer el debido seguimiento.

En caso de que el proveedor, Colegiado, y/o tercero, no comunique una incidencia detectada sobre cualquier recurso y/o medio tecnológico que **COMEVA** hubiera puesto a su disposición, será responsables de las consecuencias que se produzcan por la no comunicación al Responsable de Seguridad.

1. **Seguridad, confidencialidad y protección de datos personales.**

Toda la información contenida en los equipos informáticos, correo electrónico, en su caso, o cualquier otro sistema de información puesto a disposición de proveedores, Colegiado, mediadores y/o terceros, son de carácter privado y confidencial y, propiedad de **COMEVA**.

Es por ello que, a continuación, se indican una serie de medidas técnicas (mínimas y no exhaustivas) que deberán aplicar los proveedores, Colegiado y/o terceros, para garantizar la salvaguarda de los datos de carácter personal de **COMEVA** a la que tengan acceso con objeto del Contrato Principal, y que complementarán, en su caso, lo dispuesto en el Contrato de encargado del Tratamiento firmado entre las partes:

− ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenado-res utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.

− MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

− CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

− CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

− COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

En caso de que los proveedores, Colegiado, y/o terceros, obtengan datos de carácter personal sin la debida autorización, los traten y/o cedan a terceros, vulnerando la privacidad y confidencialidad de los datos, serán sancionados por infringir la normativa vigente, pudiendo ser sancionados incluso con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 %, tal como dispone el actual Reglamento Europeo de Protección de Datos, y con la rescisión y finalización del Contrato Principal, y el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

Es por ello por lo que, con la firma de esta Política, los proveedores, Colegiado y/o terceros, se comprometen ahora e incluso una vez finalizada la relación contractual, a guardar secreto de la información a la que tengan acceso como consecuencia de la prestación y cumplimiento del Contrato Principal, y a respetar la privacidad y confidencialidad de los datos e información a la que accedan, comprometiéndose a no ceder a terceros, los datos e información a los que tengan acceso en cumplimiento del Contrato Principal