COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
PROTECCIÓN EN EL PUESTO DE TRABAJO (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

La gestión de la información empresarial se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivos tecnológicos como de forma más tradicional (papel, teléfono...). De ahí la importancia de que el empleado se conciencie y se responsabilice del cumplimiento de ciertas normas para la seguridad en, y desde, su puesto.

Por una parte, el empleado debe conocer los riesgos no tecnológicos, por ejemplo:

- información en papel al alcance de personas no autorizadas;
- la falta de confidencialidad de los medios de comunicación tradicionales;
- el peligro de robo o extravío de los dispositivos extraíbles (pendrives, discos duros externos, etc.);
- el acceso físico de terceras personas a las zonas de trabajo (repartidores, personal de limpieza, etc.).

Por otra parte, desde en muchos puestos de trabajo se tiene acceso a ordenadores, dispositivos móviles y portátiles con conexión a la red de la empresa y al exterior (internet). Son pues una «puerta de entrada» a la empresa y a sus recursos de información. Es esencial que el empleado tenga conciencia de lo que esto implica a fin de evitar incidentes que puedan iniciarse en su puesto de trabajo, acentuados por desconocimiento o por falta de preparación:

- accesos no autorizados a los ordenadores y desde ellos a aplicativos de la empresa;
- infecciones por malware;
- robo y fuga de datos en formato digital;
- ataques de ingeniería social, es decir, engaños para manipular a la víctima para obtener
- información (credenciales, información confidencial...) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso, etc.).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, debe implantarse una política de protección del puesto de trabajo. A continuación, se facilita una serie de obligaciones y buenas prácticas en materia de seguridad que aplican a su puesto de trabajo, con el objetivo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.01.A]	DESTRUCCIÓN AVANZADA DE DOCUMENTACIÓN
La información confidencial obsoleta o que ya no sea útil debe ser destruida de forma segura teniendo en cuenta el método apropiado para cada soporte de almacenamiento	
	La información obsoleta se destruirá de forma segura según la Política de borrado seguro y gestión de soportes. En particular: • *mediante destructoras de papel al servicio de los empleados;* • *contratando un servicio externo de destrucción segura, notificando a los empleados de su existencia y obligación de uso;* • *dando a conocer los riesgos asociados a la utilización de papeleras para documentos sensibles (datos personales, información financiera, etc.).*

[SEG.01.B]	BLOQUEO PROGRAMADO DE SESIÓN
Se debe programar el bloqueo automático de sesión en los equipos al no detectarse actividad del usuario durante un corto periodo de tiempo (Máximo 15 minutos)	
	El personal informático programará un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo. Adicionalmente se puede contemplar llevar a cabo la programación del apagado general de equipos una vez terminada la actividad empresarial.

[SEG.01.C]	SISTEMA OPERATIVO ACTUALIZADO
Se deben mantener actualizados los sistemas operativos de los equipos informáticos. En caso necesario, solicitar ayuda del personal técnico	
	El personal responsable de los sistemas aplicará la Política de actualizaciones de software revisando los equipos periódicamente para garantizar su actualización o activando las actualizaciones automáticas.

[SEG.01.D]	ANTIVIRUS ACTUALIZADO Y ACTIVO
Se ha de mantener el antivirus actualizado y activo en todos los equipos informáticos	
	El personal responsable de los sistemas aplicará la Política antimalware que incluya la instalación y actualización de herramientas antimalware en todos los equipos y sistemas, y su revisión periódica de manera que se garantice la protección antimalware.

[SEG.01.E]	USO DE MEDIOS DE ALMACENAMIENTO
La información debe ser almacenada en dispositivos autorizados y de forma segura. Por ejemplo, los dispositivos externos como pendrives o discos duros externos, deben ser encriptados	
	Para que el empleado haga un uso correcto de los dispositivos de almacenamiento disponibles, debe conocer y aplicar la normativa corporativa relativa al almacenamiento local en el equipo de trabajo, almacenamiento en la red corporativa, en la nube y en los dispositivos extraíbles.

[SEG.01.F]	PROHIBICIÓN DE ALTERACIÓN
No está permitido alterar la configuración del equipo o instalar aplicaciones no autorizadas. Siempre debe solicitarse al personal informático la instalación de software específico o el cambio de configuración del equipo si es necesario para el desempeño del trabajo	
	Es un riesgo que el empleado cambie la configuración del equipo o instale las aplicaciones que considere necesarias. Esta modificación podría tener consecuencias de infección de equipos y por lo tanto de pérdida de información. Si el empleado requiere una configuración o software específico para el desempeño de su trabajo, deberá solicitarlo formalmente al equipo informático.

[SEG.01.G]	POLÍTICA DE MESAS LIMPIAS
La mesa de trabajo debe encontrarse siempre despejada y sin documentación confidencial ni dispositivos extraíbles al alcance de otras personas	
	Conocemos como política de mesas limpias la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. El cumplimiento de esta política conlleva: • *mantener el puesto de trabajo limpio y ordenado;* • *guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral;* • *no apuntar usuarios ni contraseñas en post-it o similares.*

[SEG.01.H]	CUSTODIA DE DOCUMENTACIÓN SENSIBLE
Se debe recoger inmediatamente aquellos documentos enviados a imprimir y guardar la información una vez escaneada, especialmente si se trata de información sensible	
	Para evitar que la información acabe en manos no deseadas el usuario debe: • *recoger inmediatamente aquellos documentos enviados a imprimir;* • *guardar la documentación una vez escaneada;* • *utilizar los mecanismos de impresión segura si los hubiera.*

[SEG.01.I]	NO REVELAR INFORMACIÓN A USUARIOS NO DEBIDAMENTE IDENTIFICADOS
Se debe identificar previa y correctamente el destinatario de los datos, teniendo en cuenta los peligros de la ingeniería social y la información que no se debe desvelar	
	La información es uno de los activos empresariales más cotizados. Por este motivo es posible que alguien intente obtener parte de esta información (contraseñas de usuario, información de cuentas bancarias, etc.) engañando a un empleado. Esta práctica se conoce como ingeniería social. *Los delincuentes se hacen pasar por algún responsable, persona o empresa conocida para que el empleado se confíe y facilite la información que le solicitan empleando para ello una llamada telefónica, el correo electrónico, las redes sociales o mensajes del tipo SMS o Whatsapp.*

[SEG.01.J]	OBLIGACIÓN DE CONFIDENCIALIDAD
El usuario de datos debe aceptar y cumplir la política de confidencialidad que firmó al incorporarse al puesto de trabajo	
	El empleado debe aceptar un compromiso de confidencialidad relativo a cualquier información a la que tenga acceso durante su participación laboral en la empresa. La obligación de confidencialidad tendrá validez todo el tiempo que se haya exigido en el contrato laboral. La información debe protegerse aun cuando el empleado ya no forma parte de la empresa.

[SEG.01.K]	CUSTODIA Y USO DE CONTRASEÑAS ROBUSTAS
No se deben publicar ni compartir las claves. Tampoco deben anotarse en documentos, agendas ni en cualquier otro tipo de soporte. Y deben ser dificilmente descrifrables.	
	El usuario debe seguir la Política de Contraseñas: • *las credenciales (usuario y contraseña) son confidenciales y no pueden ser publicadas ni compartidas;* • *no deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte;* • *las contraseñas deben ser robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.);* • *se deben cambiar periódicamente.*

[SEG.01.L]	CAMBIO PERIÓDICO DE CONTRASEÑAS
Se deben cambiar las contraseñas al menos cada 6 meses.	
	Para garantizar la confidencialidad de nuestras contraseñas estas deben ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo elegido.

[SEG.01.M]	OBLIGACIÓN DE BLOQUEO DE SESIÓN Y APAGADO DE EQUIPO
Es obligatorio bloquear la sesión al ausentarse del puesto de trabajo y apagar el equipo al finalizar la jornada laboral.	
	Para evitar el acceso indebido o por personal no autorizado al equipo del puesto de trabajo: • *el empleado deberá bloquearlo cada vez que se ausente de su puesto;* • *el empleado apagará su equipo al finalizar la jornada laboral.*

[SEG.01.N]	NOTIFICACIÓN DE INCIDENTES
Es obligatorio notificar cualquier incidencia de seguridad (virus, pérdida de información o de dispositivos, etc.)	
	El empleado debe advertir de cualquier incidente relacionado con su puesto de trabajo: • *alertas de virus/malware generadas por el antivirus;* • *llamadas sospechosas recibidas pidiendo información sensible;* • *correos electrónicos que contengan virus;* • *pérdida de dispositivos móviles (portátiles, smartphones o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);* • *borrado accidental de información;* • *alteración accidental de datos o registros en las aplicaciones con información crítica;* • *comportamientos anómalos de los sistemas de información;* • *hallazgo de información en ubicaciones no designadas para ello;* • *evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes…);* • *evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros;* • *cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
USO DEL CORREO ELECTRÓNICO (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

El correo electrónico es una herramienta de comunicación imprescindible para el funcionamiento de una empresa. Sus beneficios son evidentes: accesibilidad, rapidez, posibilidad de enviar documentos adjuntos, etc., aunque cuando se creó, no se hizo pensando en sus aplicaciones actuales ni en la seguridad.

Como toda herramienta de comunicación corporativa es necesario definir su uso correcto y seguro, ya que, además de abusos y errores no intencionados en su uso que puedan causar perjuicio en la empresa, el correo electrónico se ha convertido en uno de los medios que utilizan los ciberdelincuentes para llevar a cabo sus ataques.

Los empleados pueden enviar documentos confidenciales a quien no deberían por error, desvelar, sin querer, la dirección del correo electrónico (que es un dato personal) de clientes o usuarios, o utilizar su correo corporativo para usos no permitidos.

También es habitual que a los buzones corporativos llegue spam, correos de phishing que intentan robar credenciales o correos que suplantan entidades o personas. En estos casos utilizan técnicas de ingeniería social para conseguir sus fines maliciosos, por ejemplo: infectarnos, robar credenciales o que les demos datos confidenciales. En un correo malicioso tanto el remitente como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañar al receptor del mensaje. Para evitar caer en la trampa de los ciberdelincuentes debemos además de utilizar medios tecnológicos (antivirus, antimalware, antispam, etc.), concienciar a nuestros empleados para que sepan distinguir estos mensajes.

Para evitar los riesgos que conlleva el uso del correo corporativo debemos concienciar a nuestros empleados para que hagan un uso seguro del mismo e informarles de las normas que regulan las condiciones y circunstancias en las que puede utilizarse, así como las posibles sanciones y acciones a tomar en caso de detectarse un mal uso.

El objetivo es establecer unas normas de uso permitido y seguro del correo electrónico corporativo que sirva para impedir errores, incidentes y usos ilícitos, y para evitar ataques por esta vía.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.02.A]	ANTIMALWARE Y ANTISPAM
Tanto el servidor como el servidor de correos debe disponer de aplicaciones antimalware y antispam instaladas y activadas	
	Debes instalar aplicaciones antimalware y activar los filtros antispam tanto en el servidor como en el cliente de correo según la Política Antimalware. Estos filtros permitirán que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada evitando así su posible apertura.

[SEG.02.B]	CIFRADO Y FIRMA DIGITAL
Se debe utilizar tecnología de cifrado y firma digital que se puede usar con el correo electrónico para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.	
	Se debe instalar una tecnología de cifrado y firma digital para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.

[SEG.02.C]	DESACTIVAR ELEMENTOS NO SEGUROS
Se debe desactivar el formato HTML, la ejecución de macros y la descarga de imágenes para una protección adicional de las cuentas de correo electrónico.	
	El formato HTML permite utilizar colores, negritas, enlaces, etc. También permite incluir un lenguaje de programación denominado JavaScript. Este lenguaje puede ser usado con fines ilícitos, por ejemplo, para verificar que nuestra cuenta de correo es válida o para redirigirnos a un sitio web malicioso. Por ello es más seguro tenerlo desactivado. Como seguridad complementaria también se deberían deshabilitar las macros y las descargas de imágenes.

[SEG.02.D]	OFUSCAR LA DIRECCIÓN DE CORREO ELECTRÓNICO
No se deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación.	
	No se deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación. De lo contrario esas cuentas pueden ser captadas para incluirlas en listas de envío de spam. Técnicas que puedes utilizar: • *crea una imagen con la dirección de correo que quieras publicar y utiliza la imagen en lugar de introducir el correo como texto;* • *reemplazar '@' y '.' por texto; de esta forma, nombre@miempresa.com se sustituiría por nombrearrobamiempresapuntocom.*

[SEG.02.E]	USO APROPIADO DEL CORREO CORPORATIVO
Nunca se debe usar el correo corporativo con fines personales y el contenido cumple las reglas marcadas por la empresa, es decir, asuntos extrictamente profesionales.	
	El empleado conoce y acepta la normativa relativa al uso del correo corporativo.

[SEG.02.F]	CONTRASEÑA SEGURA
Se debe usar una contraseña segura para acceder al correo.	
	Todas las cuentas deben utilizar contraseñas de acceso de acuerdo con la Política de contraseñas, se recomienda: • *usar una contraseña segura para evitar accesos no autorizados;* • *utilizar doble factor de autenticación para las cuentas críticas;* • *si se accede al correo a través desde una interfaz web nunca se marcará la opción de recordar contraseña.*

[SEG.02.G]	CORREOS SOSPECHOSOS
Se debe sospechar de la autenticidad el correo cuando el mensaje: Presenta cambios de aspecto, contiene una "llamada a la acción" que urge, invita o solicita hacer algo no habitual o solicita credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).	
	Los empleados deben aprender a identificar correos fraudulentos y sospechar cuando: • *el cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente;* • *el mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual;* • *se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.)*

[SEG.02.H]	IDENTIFICACIÓN DEL REMITENTE
Se debe identificar a los remitentes antes de abrir un correo electrónico. Si se sospecha que ha sido suplantado, se debe contactar con el remitente por otro medio para confirmarlo.	
	El empleado no abrirá un correo sin identificar el remitente. Si el remitente no es un contacto conocido habrá que prestar especial atención ya que puede tratarse de un nuevo cliente o de un correo malicioso. *Si el remitente es un contacto conocido pero por otros motivos (cuerpo del mensaje, archivos adjuntos, enlaces...) sospechas que se ha podido suplantar su identidad, debes contactar con éste por otro medio para confirmar su identidad.*

[SEG.02.I]	ANÁLISIS DE ADJUNTOS
Se debe analizar cuidadosamente los adjuntos de correos de remitentes desconocidos antes de abrirlos. Si se sospecha de su autenticidad, no se debe descargar ni abrir.	
	Al recibir un mensaje con un adjunto, este se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y no apercibirnos. La descarga de adjuntos maliciosos podría infectar nuestros equipos con algún tipo de malware. Tener el antivirus activo y actualizado puede ayudarnos a identificar los archivos maliciosos. Estas son algunas medidas para identificar un adjunto malicioso: • *tiene un nombre que nos incita a descargarlo, por ser habitual o porque creemos que tiene un contenido atractivo;* • *el icono no corresponde con el tipo de archivo (su extensión), se suelen ocultar ficheros ejecutables bajo iconos de aplicaciones como Word, PDF, Excel, etc.;* • *tiene una extensión familiar, pero en realidad está seguida de muchos espacios para que no veamos la extensión real (ejecutable) en nuestro explorador de ficheros, por ejemplo: listadoanual.pdf .exe;* • *nos pide habilitar opciones deshabilitadas por defecto como el uso de macros;* • *no reconoces la extensión del adjunto y puede que se trate de un archivo ejecutable (hay muchas extensiones con las que no estamos familiarizados);* • *es o encubre un archivo JavaScript (archivos con extensión .js).*

[SEG.02.J]	INSPECCIÓN DE ENLACES
Se deben examinar atentamente los enlaces incluidos en los correos antes de acceder a ellos.	

	Al recibir un mensaje con un enlace, antes de hacer clic el receptor debe:
	• *revisar la URL, sitúate sobre el texto del enlace, para visualizar la dirección antes de hacer clic en él;*
	• *identificar enlaces sospechosos que se parecen a enlaces legítimos fijándonos en que:*
	  • *pueden tener letras o caracteres de más o de menos y pasarnos desapercibidas;*
	  • *podrían estar utilizando homógrafos, es decir caracteres que se parecen entres sí en determinadas tipografías (1 y l, O y 0).*

[SEG.02.K]	NO RESPONDER AL SPAM (CORREO BASURA)
Nunca se debe responder al corro basura. Se debe agregar a la lista de spam y eliminarlo.	
	Cuando recibimos correo no deseado no respondemos al mismo. De lo contrario confirmaremos que la cuenta está activa y seremos foco de futuros ataques. Agrégalo a tu lista de spam y elimínalo. Tampoco lo reenviaremos en caso de cadenas de mensajes.

[SEG.02.L]	UTILIZAR LA COPIA OCULTA (BCC O CCO)
Se debe utilizar la copia oculta cuando se envía correos a múltiples direcciones.	
	Cuando se envíen mensajes a múltiples destinatarios, envíatelo a ti mismo y utiliza la opción de copia oculta, (CCO o BCO en la mayoría de los clientes de correo) en lugar de la copia normal CC. La copia oculta impide que los destinatarios vean a quién más ha sido enviado. De esta forma evitaremos que cualquiera pueda hacerse con unas cuantas direcciones de correo válidas a las que enviar spam o mensajes fraudulentos. Recuerda que el correo electrónico es un dato personal de nuestros clientes y usuarios, que no debemos utilizar para otros fines distintos de aquellos para los que fue solicitado. No debemos divulgarlo o comunicarlo a terceros sin su consentimiento.

[SEG.02.M]	REENVÍO DE CORREOS
En caso de necesitar el reenvío de algún correo corporativo a una cuenta personal, debe solicitar autorización previa a la dirección de la empresa.	
	Se informará de la prohibición del reenvío de correos corporativos a cuentas personales salvo casos excepcionales que deben ser autorizados por la dirección.

[SEG.02.N]	EVITAR REDES PÚBLICAS
No debe consultarse el correo corporativo si se está conectado a redes públicas como wifis de hoteles, restaurantes o aeropuertos.	
	Evitar utilizar el correo electrónico desde conexiones públicas (la wifi de una cafetería, el ordenador de un hotel, etc.) de acuerdo con la Política de uso de wifis y conexiones externas ya que nuestro tráfico de datos puede ser interceptado por cualquier usuario de esta red. Como alternativa, es preferible utilizar redes de telefonía móvil como el 3G o 4G.

[SEG.02.O]	NORMATIVA DE USO DE CORREO ELECTRÓNICO
Debe existir una normativa referente al uso del correo electrónico a disposición del empleado.	
	La empresa dispondrá de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporase a su puesto de trabajo. Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con la empresa. El contenido del correo deberá cumplir con la normativa y su uso inadecuado podrá conllevar sanciones. El correo corporativo puede ser supervisado por la dirección de la empresa incluyendo una cláusula en la normativa que firma el empleado.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
CONTRASEÑAS (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

El tratamiento diario de la información de la empresa requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la pareja de credenciales: usuario y contraseña. Por la seguridad de los servicios y sistemas en los que existen cuentas de usuarios, tenemos que garantizar la que las credenciales de autenticación se generan, actualizan y revocan de forma óptima y segura.

Existen distintos mecanismos de gestión de identidades y control de accesos. Algunos están implementados en los sistemas operativos habituales, otros están disponibles a través de servicios online, como pueden ser el social login, la federación de identidades, los servicios de intermediarios de seguridad de acceso a la nube o CSAB, etc. En cualquier caso, debemos establecer un procedimiento claro para habilitar y revocar las credenciales y permisos de acceso a los distintos servicios y aplicaciones: correo electrónico, servidor de ficheros, gestor de contenidos web, CRM, ERP, etc.

En el control de accesos el nombre de usuario nos identifica y la contraseña nos autentica (con ella se comprueba que somos quienes decimos ser). Todo sistema de autenticación de usuarios se basa en la utilización de uno, o varios, de los siguientes factores:

- algo que sabes: contraseñas, preguntas personales, etc.
- algo que eres: huellas digitales, iris o retina, voz, etc.
- algo que tienes: tokens criptográficos, tarjeta de coordenadas, etc.

Como la contraseña es el más utilizado de estos factores, la gestión de las contraseñas es uno de los aspectos más importantes para asegurar nuestros sistemas de información. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos y servicios de nuestra empresa.

Dentro de la gestión de contraseñas se incluye el deber de difundir y hacer cumplir unas buenas prácticas: actualizarlas periódicamente, garantizar su fortaleza (dificultad para adivinarla o craquearla), no utilizar contraseñas por defecto o cómo custodiarlas.

El objetivo es establecer, difundir y verificar el cumplimiento de buenas prácticas en el uso de contraseñas.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.03.A]	GESTIÓN DE CONTRASEÑAS
Se debe definir un sistema de gestión de contraseñas avanzado que contemple todos los aspectos relativos a su ciclo de vida. Solicita más información a tu responsable.	

	La gestión de contraseñas es uno de los aspectos más delicados para asegurar el acceso a nuestros sistemas. Se ocupa de:
	• *Identificar los distintos equipos, servicios y aplicativos para los que es necesario activar credenciales de acceso.*
	• *Definir la manera con la que se generarán las claves, así como su formato.*
	• *Distribuir las claves generadas a los usuarios correspondientes, teniendo en cuenta:*
	  • *si esta distribución ha de ser cifrada y con qué método;*
	  • *cómo se activarán las claves.*
	• *Almacenar las claves en repositorios seguros, considerando la necesidad de realizar copias de respaldo.*
	• *Determinar quién puede acceder a estos repositorios y cómo.*
	• *Establecer el periodo de validez para cada tipo de clave.*
	• *Revocar las claves, ya sea por baja de un empleado, por considerar que una clave está comprometida por robo, etc. Además, se determinará la manera con la que las claves serán eliminadas.*
	• *Registrar:*
	  • *motivo por el que se genera una clave;*
	  • *fecha de creación;*
	  • *responsable de la custodia;*
	  • *periodo de validez;*
	  • *posibles observaciones, incidentes, etc.*

[SEG.03.B]	HERRAMIENTAS PARA GARANTIZAR LA SEGURIDAD DE LAS CONTRASEÑAS
Debes ayudarte de técnicas y herramientas informáticas para garantizar la seguridad de las contraseñas. Solicita más información a tu responsable.	

	Para garantizar que nuestras contraseñas se generan y usan de forma robusta, podemos ayudarnos de diversas herramientas como LDAP, Active Directory o servicios externos que obligan al cumplimiento de ciertos requisitos. En todos los casos se contemplarán los aspectos más relevantes como:
	• *periodos de validez para las contraseñas;*
	• *posibilidad de reutilización de contraseñas ya usadas;*
	• *formato de la contraseña:*
	  • *longitud mínima;*
	  • *tipos de caracteres que deben incluir;*
	  • *cumplimiento de reglas semánticas.*
	• *posibilidad de elección y modificación de la contraseña por parte del usuario;*
	• *almacenamiento de las claves:*
	  • *tamaño del histórico de claves a almacenar para cada usuario;*
	  • *método de encriptación de las claves.*
	• *número de intentos de autenticación permitidos.*

[SEG.03.C]	NO UTILIZAR LAS CONTRASEÑAS POR DEFECTO
Se deben cambiar las contraseñas que vienen incluidas por defecto para el acceso a aplicaciones, equipos y sistemas.	
	Debemos cambiar las claves por defecto, las que traen los equipos y sistemas al adquirirlos, por otras elegidas por nosotros mismos. Con esta medida evitamos el acceso no permitido, que sería posible si dejamos la contraseña por defecto por ser estas conocidas o que pueden encontrarse fácilmente en internet. Esto es especialmente importante para el acceso a la configuración de ciertos dispositivos como routers, switches, etc.

[SEG.03.D]	DOBLE FACTOR PARA SERVICIOS CRÍTICOS
Se deben incorporar sistemas de autenticación multifactor en los accesos a servicios con información muy sensible.	
	Es recomendable implantar un sistema de autenticación de doble en el acceso a servicios que contengan información especialmente sensible o crítica. Se pueden considerar además de la contraseña otro factor como: • *huella digital;* • *tokens criptográficos hardware;* • *sistemas OTP (One Time Password);* • *tarjetas de coordenadas.*

[SEG.03.E]	NO COMPARTIR LAS CONTRASEÑAS CON NADIE
Las contraseñas son unipersonales, por lo que deben mantenerse en secreto y evitar compartirlas. Si se sospecha que se ha violado la integridad de una contraseña, se debe cambiar inmediatamente.	
	Si compartimos nuestras contraseñas están dejarán de ser secretas y por tanto perderán su utilidad. Debemos asegurarnos de lo siguiente: • *no debemos compartirlas con nadie;* • *no debemos apuntarlas en papeles o post-it;* • *no debemos escribir nuestras contraseñas en correos electrónicos ni en formularios web cuyo origen no sea confiable.*

[SEG.03.F]	LAS CONTRASEÑAS DEBEN SER ROBUSTAS
Se deben generar las contraseñas teniendo en cuenta su fortaleza.	

	Para que nuestras contraseñas sean fuertes, difíciles de adivinar o calcular, debemos cumplir las siguientes directrices:
	• *deben contener al menos ocho caracteres;*
	• *deben combinar caracteres de distinto tipo (mayúsculas, minúsculas, números y símbolos);*
	• *no deben contener los siguientes tipos de palabras:*
	  • *palabras sencillas en cualquier idioma (palabras de diccionarios);*
	  • *nombres propios, fechas, lugares o datos de carácter personal;*
	  • *palabras que estén formadas por caracteres próximos en el teclado;*
	  • *palabras excesivamente cortas.*
	• *tampoco utilizaremos claves formadas únicamente por elementos o palabras que puedan se públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento);*
	• *se establecerán contraseñas más fuertes para el acceso a aquellos servicios o aplicaciones más críticas;*
	• *se tendrá en cuenta lo expuesto en los puntos anteriores también en el caso de utilizar contraseñas de tipo passphrase (contraseña larga formada por una secuencia de palabras).*

[SEG.03.G]	NO UTILIZAR LA MISMA CONTRASEÑA PARA SERVICIOS DIFERENTES
Debes asegurarte de elegir distintas contraseñas para cada uno de los servicios que se utiliza.	
	Nunca debemos utilizar la misma contraseña para diferentes servicios. Tampoco utilizaremos las mismas contraseñas para uso profesional y doméstico. De esta forma evitaremos tener que cambiar todas nuestras contraseñas en el caso de que solo una haya sido comprometida.

[SEG.03.H]	CAMBIO PERIÓDICO DE CONTRASEÑAS
Se deben modificar las contraseñas periódicamente, como mínimo cada 6 meses.	
	Para garantizar la confidencialidad de nuestras contraseñas estas deben ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso. No deben utilizarse contraseñas que hayan sido usadas con anterioridad. Pueden utilizarse sistemas que fuercen al cambio de contraseña en el plazo elegido.

[SEG.03.I]	NO HACER USO DEL RECORDATORIO DE CONTRASEÑAS
No debe utilizarse nunca las opciones de recordatorio de contraseñas de los navegadores y aplicaciones.	
	No es recomendable el utilizar las funcionalidades de recordatorio de contraseñas, ya que pueden facilitar el acceso a personal no autorizado. Esto es especialmente frecuente en el uso de navegadores web.

[SEG.03.J]	UTILIZAR GESTORES DE CONTRASEÑAS
Debe usarse gestores de contraseñas seguros para poder recordarlas, tales como KeePass, LastPass, Enpass, etc. Solicita más información a tu responsable.	
	Debemos considerar el uso de gestores de contraseñas en aquellos casos en los que tengamos que recordar un gran número de ellas para acceder a muchos servicios. En estos casos es muy recomendable elegir un gestor cuyo control quede bajo nuestra supervisión, que cifre las credenciales e implantar doble factor de autenticación para acceder al mismo.

[SEG.03.K]	PRECAUCIÓN AL USAR TÉCNICAS DE AUTENTICACIÓN EXTERNAS
Existen métodos de autenticación externa que pueden facilitar el registro y/o el acceso a otros servicios. Estos sistemas deben de usarse con precaución.	
	Los avances en el mundo digital posibilitan la elección de mecanismos de autenticación descentralizados que permiten el uso de contraseñas únicas para acceder a varios servicios. En ciertos casos la empresa puede plantearse el uso de alguna de estas técnicas, teniendo siempre en cuenta el riesgo que supone permitir que terceros gestionen nuestras credenciales: • ***Social-login.*** *Se basa en la utilización de identidades ya creadas en redes sociales (como Facebook, Linkedin, Google o Twitter) para registrarnos automáticamente en otros servicios.* • ***Autenticación federada.*** *Permite disponer de un único punto de autenticación para acceder a servicios de distintas compañías. Puede ser de utilidad para empresas muy integradas con proveedores y partners.* • ***Single-sign-on.*** *Se trata de un mecanismo que permite a un usuario autenticado en un servicio el acceso automático a otras muchas aplicaciones y servicios.* • ***Autenticación condicionada al dispositivo.*** *Nos permiten la autenticación a través de alguna característica del dispositivo previamente registrada en el servidor de autenticación.* • ***CSAB (Cloud Access Security Brokers).*** *Especialmente pensado para empresas que hacen uso de servicios cloud.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

REDES WIFI Y REDES EXTERNAS (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Es habitual tener que acceder a los datos de la empresa cuando estamos fuera del lugar de trabajo (viajes, reuniones, teletrabajo, etc.). En ocasiones no podemos hacer uso de las redes o conexiones 4G/5G, lo que nos obliga a conectarnos a redes domésticas o a redes públicas (hoteles, cafeterías, aeropuertos, etc.) que en la mayoría de los casos podrían no ser seguras.

Es prudente asumir que, por defecto, las redes inalámbricas que utilizan los trabajadores fuera del entorno empresarial, no disponen de las medidas de seguridad necesarias para la protección de los datos y las comunicaciones corporativas. A menudo, la información confidencial de nuestra empresa se transmite a través de redes inalámbricas cuya seguridad no está bajo nuestro control, por lo que debemos asegurarnos de que los datos viajan convenientemente protegidos antes de hacer uso de estas redes.

La empresa debe establecer las condiciones y circunstancias en las que se permite el acceso remoto a los servicios corporativos. Es decir, determinar quién puede acceder a qué, cómo y cuándo. Esta tarea implica disponer de los medios necesarios para llevarla a cabo y ofrecer la correspondiente formación a los trabajadores para que conozcan cómo conectarse de forma segura y cómo mantener sus equipos seguros cuando viajan o se conectan desde el exterior.

Una de las herramientas de seguridad que podemos implantar para realizar accesos remotos corporativos desde el exterior de la empresa, es la utilización de una Red Privada Virtual o VPN. Utilizaremos una VPN cuando necesitemos acceder a información confidencial de manera remota, y la red que estemos utilizando no ofrezca las suficientes garantías de seguridad. Estas son las ventajas de utilizar una VPN:

- toda la información se transmite de manera segura gracias al cifrado de datos y de conexión;
- confidencialidad e integridad de la información: al ir cifrada, la información no puede ser leída, modificada o alterada durante la transmisión;
- la información solo se trasmite entre dispositivos autorizados y configurados para este fin;
- restricción de acceso: a través de usuario y contraseña necesitando una previa autorización;
- fácil ampliación del número de usuarios.

Las conexiones establecidas utilizando VPN protegen la información que se intercambia, ya que establecen un canal cifrado de comunicación entre nuestro dispositivo y nuestro lugar de trabajo por donde «viajan» nuestros datos de manera segura.

El objetivo es garantizar la seguridad de los datos y comunicaciones corporativos cuando el acceso a los mismos tiene lugar desde fuera de las instalaciones de la empresa mediante la utilización de redes externas no corporativas.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.04.A]	EXISTENCIA DE POLÍTICA DE CONEXIÓN
Debe existir una normativa de conexión a disposición del empleado	
	La dirección debe determinar si la política de seguridad permite la conexión desde redes externas a los recursos de la empresa y establecer las condiciones este tipo de accesos.

[SEG.04.B]	Configuración de la VPN
Para acceder a los sistemas de la empresa desde el exterior, se hacer desde una conexión VPN, con cuenta de usuario con permisos de accesos y únicamente para el software autorizado. Se debe establecer un tiempo de desconexión automática de la VPN tras un periodo de inactividad.	
	Para los accesos permitidos desde el exterior el equipo técnico debe disponer y configurar un servicio VPN: • *crear cuentas de usuario con permisos de acceso personalizados;* • *determinar el software permitido para realizar conexiones VPN;* • *establecer un tiempo para la desconexión automática de la VPN tras un periodo de inactividad.*

[SEG.04.C]	USO DE LA VPN
Se debe conocer cómo conectarse vía VPN y en qué situaciones hacerlo. Solicita más información a tu responsable.	
	Los empleados que tengan autorizado el acceso vía VPN conocerán cómo hacerlo y cuándo está permitido: • *cuando utilicemos redes públicas o no confiables;* • *para acceder a los recursos corporativos como impresoras, documentos, servidores de base de datos, aplicaciones específicas, etc.;* • *cuando necesitemos hacer operaciones confidenciales: acceso a bases de datos, banca online o facturación, que impliquen la transmisión de usuarios, contraseñas, o cualquier otra información confidencial;* • *cuando queramos interconectar redes separadas de forma segura: distintos edificios u oficinas separadas geográficamente, equipos utilizados en teletrabajo con la oficina, etc.;* • *cuando hagamos uso del teletrabajo.*

[SEG.04.D]	ACCESO A REDES WIFI AJENAS
Al conectarse a una red inalámbrica, se debe comprobar que se utiliza el protocolo WPA2. También debe comprobarse si los sitios a los que se accede tienen certificado y utilizan protocolos seguros (https://) si vas a realizar actividades críticas.	
	Al conectarte a una red inalámbrica desconocida, compruebas que utiliza el protocolo WPA2 y revisas el uso vas a hacer de esa red: • *Sólo utiliza **redes WiFi púbicas no seguras** para realizar actividades de bajo riesgo como navegar o leer noticias, pero asegúrate que el canal está cifrado (sitio web con https:// y certificado) si has de iniciar sesión (hacer login) o suscribirte.* • *Sólo utiliza **redes WiFi públicas seguras** (al menos con WPA2) si no tienes otro medio más seguro (redes móviles 4G/5G o una VPN) a tu alcance para realizar actividades de alto riesgo (uso de email, trabajar con documentos online, redes sociales, banca online o compras online) comprobando además que accedes a sitios web legítimos, cifrados (https://) y con certificado.*

[SEG.04.E]	CONFIGURACIÓN DE LA RED WIFI DOMÉSTICA
Antes de utilizar la red WiFi doméstica para asuntos relacionados con la entidad, se debe configurar el protocolo WPA2, cambiar el nombre SSID y las credenciales por defecto.	
	En el caso de usar una wifi doméstica, tendremos que configurarla para: • *activar el protocolo WPA2;* • *cambiar el nombre por defecto del SSID;* • *cambiar las credenciales por defecto;*

[SEG.04.F]	REDES INALÁMBRICAS DE LOS DISPOSITIVOS MÓVILES
Solo se deben abrir las conexiones WiFi y Bluetooth de los dispositivos móviles cuando se van a utilizar y para conectarse a dispositivos confiables.	
	Activar la conexión WiFi, Bluetooth o antena GPS únicamente en los momentos que se vayan a utilizar y con las convenientes medidas de seguridad.

[SEG.04.G]	USO DE DISPOSITIVOS MÓVILES
Se debe revisar las políticas de uso de dispositivos móviles y uso de dispositivos personales en el ámbito corporativo.	
	Si utilizas dispositivos móviles para trabajar fuera de la empresa, se han de tomar las medidas de seguridad indicadas en las Políticas de uso de dispositivos móviles corporativos y en la de uso de dispositivos móviles no corporativos.

[SEG.04.H]	USO DE ORDENADORES NO CORPORATIVOS
Se debe evitar el uso de ordenadores no corporativos. Revisar la seguridad de los dispositivos y tomar precauciones cuando se utilice dispositivos de uso compartido.	
	Si utilizas ordenadores de uso público evita realizar actividades de alto riesgo (uso de email corporativo, trabajar con documentos online, redes sociales, banca online o compras online). Desconfía de la seguridad del equipo y sus conexiones. En cualquier caso, si te vieras en la necesidad de utilizarlos para hacer login en algún servicio corporativo siempre que esté permitido y no puedas hacer uso de una VPN: • *revisa el entorno para evitar la mirada de observadores o de cámaras* • *utiliza el modo de navegación privada del navegador;* • *teclea la URL o dirección web, en lugar de utilizar el buscador;* • *verifica que la página a la que accedes es auténtica, que utiliza protocolo https:// y que tiene certificado y está vigente;* • *evita que el navegador guarde las contraseñas;* • *al finalizar la sesión borra el historial de navegación y las cookies en el navegador;* • *no conectes pendrives ni otros dispositivos externos;* • *revisa que no dejas ningún archivo personal en el equipo.* *Si utilizas ordenadores domésticos:* • *actualiza el software de sistemas operativos y aplicaciones;* • *utiliza un usuario no compartido;* • *instala y activa un antivirus y el cortafuegos del sistema operativo;* • *no instales aplicaciones sin licencia o cuyo origen desconozca*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS(v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

El uso de dispositivos personales (portátiles, smartphones, tablets), propiedad del empleado, en el ámbito corporativo es lo que se conoce como BYOD (Bring Your Own Device). Se trata de una práctica muy frecuente, por lo tanto, se debe prestar una especial atención para que su uso no comprometa la seguridad de la información de la empresa.

Existen ciertos riesgos que debemos conocer antes de permitir el uso de dispositivos personales en el ámbito corporativo:

- La exposición a redes inseguras en el ámbito personal. Este tipo de conexión podría tener como consecuencia que la información corporativa fuera accesible o pudiera ser interceptada por terceras personas no autorizadas.
- La instalación de aplicaciones que solicitan permisos para acceder a partes del dispositivo donde puede haberse almacenado información sensible, e incluso solicitar la activación de la geolocalización.
- La inexistencia de mecanismos de control de acceso a los dispositivos y la ausencia de medidas de seguridad en cuanto al almacenamiento de la información. Si alguien tuviera acceso a nuestro dispositivo no tendría ninguna dificultad a la hora de acceder o extraer información confidencial.
- La carencia de herramientas antivirus y de una normativa de actualizaciones adecuada. Actualizar las aplicaciones y disponer de un antivirus protegen al terminal de posibles ataques y accesos no autorizados.
- La opción (activada) de recordar y usar contraseñas de forma automatizada para acceder a redes, aplicaciones, sitios web, etc. Si alguien tuviera acceso al dispositivo no necesitaría disponer de las credenciales de usuario para acceder a la información.

Una vez establecida la política de seguridad relativa al uso seguro de los dispositivos personales para el trabajo, debe ponerse en conocimiento de los empleados y ser aceptada por los mismos antes de que utilicen sus dispositivos para acceder a aplicaciones o tratar con información de la empresa.

El objetivo es establecer las normas que garanticen la seguridad de la información si se permite el uso de los dispositivos personales en el ámbito corporativo.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.05.A]	NORMAS Y PROCEDIMIENTOS BYOD
Únicamente se permiten el uso de dispositivos no corporativos si disponen de antivirus y sistemas operativos actualizados, tienen configuraciones de seguridad, no tienen instalado software sin licencia y están debidamente encriptados. No obstante, se debe disponer de autorización específica por parte del personal responsable.	
	El empresario elaborará normas y procedimientos específicos que regulen el uso de dispositivos BYOD (listado de dispositivos autorizados, en qué condiciones se permite su uso, cómo se accede a la información, configuraciones de seguridad necesarias para poder utilizarlos, etc.).

[SEG.05.B]	PROHIBICIÓN DE USO DE DISPOSITIVOS MANIPULADOS
Se prohíbe el uso de dispositivos rooteados o a los que se ha realizado jailbreak.	
	Se recomienda prohibir el uso de dispositivos rooteados o a los que se les ha hecho jailbreak ya que permiten la instalación de aplicaciones de repositorios no oficiales.

[SEG.05.C]	CONCIENCIACIÓN DE LOS EMPLEADOS
El personal deberá estar concienciado del posible robo de sus dispositivos móviles	
	Los dispositivos como el teléfono móvil o el portátil son susceptibles de robo. Por ello es importante involucrar a los usuarios en la protección de sus propios dispositivos concienciándolos de la trascendencia de la protección del mismo y de los datos que contiene.

[SEG.05.D]	FORMACIÓN DE LOS EMPLEADOS
El personal deberá de estar formado para un uso seguro de los dispositivos móviles.	
	Proporcionaremos a los empleados formación suficiente para un uso seguro de los dispositivos. Por ejemplo, han de saber: • *configurar los parámetros de seguridad de los dispositivos;* • *actualizar tanto el sistema operativo como las aplicaciones periódicamente (en especial el antivirus);* • *no instalar aplicaciones que exijan permisos que pongan en riesgo la información confidencial (acceso a la agenda, geolocalización, etc.);* • *bloquear los dispositivos con contraseña y activar el bloqueo automático tras un periodo corto de inactividad;* • *no desatender los dispositivos al viajar en transporte público.*

[SEG.05.E]	LÍMITE DE ACCESO A REDES EXTERNAS
Se prohíbe el uso de redes inalámbricas externas no corporativas para el acceso a los sistemas de la entidad mediante equipos no corporativos. Solo se permiten accesos de redes 3G/4G/5G.	
	Los usuarios deben conocer que es preferible optar por la conexión de datos de su móvil 3G/4G/5G cuando las redes inalámbricas disponibles sean desconocidas. Estas redes WiFi deben considerarse inseguras

[SEG.05.F]	LISTA DE APLICACIONES NO PERMITIDAS
Antes de instalar una aplicación en un dispositivo no corporativo para el uso de los datos de la entidad, se debe solicitar autorización al personal responsable.	
	Estableceremos una lista de tipos de aplicaciones que no se podrán instalar en estos dispositivos por el peligro que suponen para la información corporativa. Estas aplicaciones pueden requerir para su instalación acceso a datos confidenciales de la organización (datos de la agenda, geolocalización del terminal, etc.).

[SEG.05.G]	CONTROL DE ALMACENAMIENTO EN LA NUBE DE LOS DATOS CORPORATIVOS
No está permitido el uso de aplicaciones de almacenamiento de datos corporativos en la nube en dispositivos no corporativos.	
	Las aplicaciones personales en los dispositivos móviles para el tratamiento de datos en la nube no son tan seguras como las empresariales por lo que hay que prestar especial atención a este intercambio de archivos. Se puede permitir la consulta de información en la nube, pero se recomienda no actualizarla desde estos dispositivos personales.

[SEG.05.H]	PROCESO DE BORRADO DE LA INFORMACIÓN
Cuando un dispositivo no corporativo deja de usarse para usos corporativos o el empleado que lo usaba abandona la empresa, previamente deben formatearse para evitar la recuperación de datos.	
	Estableceremos el proceso a seguir para entregar/eliminar la información en estos dispositivos cuando el empleado abandona la empresa.

[SEG.05.I]	CONTROL DE ACCESO A LA RED
Sólo está permitido el acceso a la red corporativa con equipos no corporativos mediante el uso de conexiones VPN.	
	El acceso a la red corporativa a través de dispositivos personales debe estar integrado en el sistema de control de accesos (autenticación, doble factor...). De esta forma el empleado debe acreditar su identidad antes de acceder a los servicios de la red corporativa. Para mayor seguridad la empresa puede proporcionar a sus empleados acceso mediante red privada virtual (VPN) que cifra las comunicaciones.

[SEG.05.J]	CONTROL DE USUARIOS Y DISPOSITIVOS
Debes asegurarte que tú y tu dispositivo está registrado en el listado de usuarios y dispositivos autorizados. Solicita información a tu supervisor.	
	Mantendremos un registro de usuarios y dispositivos que tienen acceso a los datos y aplicaciones de la empresa, detallando los privilegios de seguridad asignados para autorizar el acceso tanto a esos usuarios como a los dispositivos. *Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos. Por ejemplo:* • *Implementaremos en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación de usuarios.* • *Impediremos guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas.*

[SEG.05.K]	ENCRIPTADO DE DISPOSITIVOS
El uso de dispositivos no corporativos debe ser cifrado y las carpetas con datos corporativos protegidas con contraseñas.	
	Se deberá de utilizar las opciones de cifrado del dispositivo disponibles. De esta forma, los datos del dispositivo estarán inaccesibles en caso de robo.

[SEG.05.L]	BLOQUEO PROGRAMADO
Se debe configurar el bloqueo automático del dispositivo no corporativo tras un periodo de inactividad.	
	Configuraremos el dispositivo para que se bloquee automáticamente tras un periodo de inactividad. Para ello, haremos uso de la funcionalidad de protecctor de pantalla del sistema operativo. *Los periodos de inactividad deben ser tiempos cortos, normalmente 10 minutos.*

[SEG.05.M]	EXTRAVÍO DE DISPOSITIVOS
Los dispositivos no corporativos deben ser configurados con medidas de seguridad para proteger la información corporativa (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas) en caso de extravío.	
	Ante la posibilidad de pérdida o extravío de este tipo de dispositivos, estableceremos las siguientes medidas: • *Localización mediante GPS, WiFi o la información de la antena de telefonía con la que esté conectado el dispositivo. Una vez marcado como «perdido», el Smartphone empieza a enviar los datos de su ubicación de manera constante a una cuenta previamente configurada (correo, SMS, central de control…).* • *Tener siempre activado el bloqueo de pantalla del terminal. En caso contrario se bloqueará de manera remota.* • *Borrado remoto de datos: esta opción permite que los datos contenidos en el dispositivo se borren de manera remota, impidiendo su utilización por un usuario no legítimo.* • *Vigilar las aplicaciones que se ejecutan. El seguimiento de las llamadas* • *efectuadas y las redes sociales accedidas entre otros, suelen ser datos suficientes para obtener nombres, apellidos y hasta direcciones de un posible delincuente.*

[SEG.05.N]	DESCONEXIÓN WIFI Y BLUETOOTH
Se debe desactivar la búsqueda de redes WiFi y de dispositivos vía Bluetooth cuando no sean necesarios.	
	Se desactivará en el teléfono la búsqueda de redes WiFi y de dispositivos vía Bluetooth cuando no sean necesarios.

[SEG.05.O]	CUMPLIMIENTO DE LA NORMATIVA
El personal de la empresa deberá de comprometerse y cumplir la normativa referente a uso de dispositivos móviles no corporativos	
	Nos aseguraremos que los empleados conocen la normativa corporativa y se comprometen a cumplirla antes de la incorporación de sus dispositivos personales al entorno de trabajo.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

USO DE DISPOSITIVOS MÓVILES CORPORATIVOS (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Hoy en día trabajar fuera de las instalaciones corporativas es posible con el uso de dispositivos móviles (portátiles, tablets y teléfonos móviles) propiedad de la empresa o del empleado.

Las tecnologías de movilidad como los ordenadores portátiles permiten al empleado desempeñar su trabajo como si estuviera en las instalaciones de la empresa: acceso al correo, a las aplicaciones corporativas, información confidencial, etc.

Estos dispositivos son más susceptibles de pérdida o robo, por lo que existe un riesgo añadido al acceso de la información corporativa. Por eso es imprescindible tomar algunas medidas de seguridad como establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el equipo siempre actualizado y con el antivirus activo, etc.

Si la empresa permite al empleado utilizar sus propios dispositivos (BYOD o Bring Your Own Device) debe consultar la Política de uso de dispositivos móviles no corporativos para que sea con garantías de seguridad.

El objetivo es establecer una normativa de seguridad, aplicable en los niveles de gestión, técnico y de usuario, para un correcto uso de los dispositivos móviles corporativos.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.06.A]	ASIGNACIÓN DE DISPOSITIVOS
Existe un procedimiento de solicitud y asignación de dispositivos móviles corporativos, por lo que debes asegurarte de utilizarlo.	
	Elaboraremos un procedimiento de solicitud y asignación de los dispositivos móviles corporativos para mantener un inventario activo y registrar las necesidades de los trabajadores.

[SEG.06.B]	REGISTRO DE EQUIPOS
Todos los equipos portátiles asignados deben ser registrados (qué portátil y a quién se le asigna), así como el software y el hardware requerido por el empleado.	
	Es recomendable mantener un registro de los dispositivos móviles asignados (qué dispositivo y a quién se le asigna). También registraremos el uso que se da al dispositivo, así como el software y hardware que son requeridos por el empleado.

[SEG.06.C]	MANTENIMIENTO DE DISPOSITIVOS
Para realizar cambios en el dispositivo (modificación de hardware, instalación de software, cambios en la configuración) deben ser solicitados al personal responsable.	
	El mantenimiento de dispositivos queda restringido al departamento responsable de su mantenimiento. Por tanto, debe prohibirse que el usuario haga cambios en el hardware, instale software o modifique la configuración del equipo sin autorización del departamento competente.

[SEG.06.D]	PROTECCIÓN DE LA BIOS
La BIOS de los equipos portátiles están configurados con contraseñas	
	Los equipos portátiles corporativos tendrán el acceso a la BIOS protegido con contraseña para evitar modificaciones en la configuración por parte del usuario.

[SEG.06.E]	SOFTWARE DE LOCALIZACIÓN
Algunos equipos precisan de software de localización. Solicita información a tu supervisor.	
	En el caso de que se considere necesario instalar o activar algún software de localización se comunicará al usuario del dispositivo antes de realizar la entrega del mismo. El usuario que va a estar geolocalizado debe firmar un documento aceptando esta condición.

[SEG.06.F]	ALMACENAMIENTO DE LA INFORMACIÓN
No se debe almacenar información corporativa que no sea extrictamente necesaria para el desarrollo del trabajo.	
	La información corporativa que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no debe almacenarse en el dispositivo. Si se accede a la información desde varios dispositivos, esta tiene que estar sincronizada para evitar duplicidades y errores en las versiones.

[SEG.06.G]	TRATAMIENTO DE INFORMACIÓN CONFIDENCIAL
Se debe cifrar la información confidencial y eliminarla de forma segura. Solicita apoyo técnico.	
	Toda la información confidencial debe almacenarse cifrada. Antes de la devolución del dispositivo, la información debe ser eliminada de forma segura o solicitar su eliminación al técnico responsable.

[SEG.06.H]	CONEXIÓN A REDES
Solo se debe conectar el portátil a redes conocidas y privadas, y optar por una conexión 3G/4G/5G cuando el resto de las redes disponibles no sean confiables.	
	Las conexiones a redes ajenas a la organización seguirán las normas establecidas en la política de uso corporativo de redes externas.

[SEG.06.I]	NOTIFICACIÓN EN CASO DE INFECCIÓN
Se debe notificar al personal técnico responsable la sospecha de infección por virus u otro software malicioso del equipo.	
	Si se sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal técnico responsable.

[SEG.06.J]	TRANSPORTE Y CUSTODIA
No debes exponer el equipo a altas temperaturas. No se debe descuidar el portátil si se viaja en transporte público, no se debe guardar en el coche ni dejarlo visible o fácilmente accesible. Si se trabaja en lugares donde no se garantiza su custodia, se debe anclar con un candado de seguridad o guardarlo en un armario de seguridad. En caso de robo o pérdida del equipo debe ser notificado al responsable inmediatamente.	
	El equipo no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo. En ningún caso se debe descuidar el portátil si se viaja en transporte público. Tampoco se ha de guardar en el coche ni dejarlo visible o fácilmente accesible. Si se trabaja en lugares donde no se garantiza la custodia del equipo, este debe quedar anclado con un candado de seguridad o guardado en un armario de seguridad. En caso de robo o pérdida del equipo se debe notificar de manera inmediata al personal técnico responsable.

[SEG.06.K]	USO DEL PUESTO DE TRABAJO
Se debe aplicar las normas recogidas en la Política de uso del puesto de trabajo relativas al uso de un equipo informático (obligación de notificar incidentes de seguridad, uso correcto de contraseñas, bloqueo del equipo, etc.)	
	El usuario aplicará las normas recogidas en la Política de uso del puesto de trabajo que sean relativas al uso de un equipo informático (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, etc.).

[SEG.06.L]	RESPONSABILIDADES
El empleado conoce las responsabilidades que conlleva el uso de dispositivos corporativos móviles y aplica las normas de seguridad correspondientes.	
	El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones corporativas. Por tanto, es el trabajador el que debe garantizar la seguridad tanto del equipo como de la información que contiene. Esta normativa será de obligado cumplimiento y podrá ser objeto de acuerdos que se firmen al aceptar el uso de estos dispositivos.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

APLICACIONES PERMITIDAS(v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Las normas de protección de la propiedad intelectual obligan a las empresas a usar en todo momento software legal. El uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales. Además, la instalación y uso de software ilegal en algún dispositivo incrementa los riesgos de infección por malware.

Por otra parte, para evitar fugas de información y garantizar la privacidad de los datos de carácter personal, la empresa debe determinar y controlar qué software está autorizado para el tratamiento de la información dentro de la empresa.

Cualquier incidente de seguridad puede repercutir en la imagen de la compañía.

Para hacer cumplir esta política la empresa debe contar con:

- un listado de software autorizado;
- un repositorio del software autorizado y un registro de licencias;
- las sanciones disciplinarias derivadas del incumplimiento de la política.

Y debe identificar a los responsables para realizar las actualizaciones del software y las auditorías.

El objetivo es controlar que siempre se usa software autorizado en la empresa, y que ha sido adquirido de forma legal.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.07.A]	REGISTRO DE LICENCIAS
Existe un registro actualizado de licencias disponibles del software autorizado.	
	Si queremos saber de qué software dispone la organización conviene tener un registro actualizado de licencias. En dicho registro se almacenará al menos la siguiente información: • *nombre y versión del producto* • *autor* • *fecha de adquisición* • *vigencia de la licencia* • *tipo de licencia* • *número de usuarios permitidos por licencia* • *número de licencias adquiridas por cada software* • *facturas o comprobantes de compra* • *ubicación física del producto*

[SEG.07.B]	COMPETENCIA DE INSTALACIÓN, ACTUALIZACIÓN Y BORRADO
Únicamente el personal técnico está autorizado para encargarse de la instalación, actualización y eliminación de software en los equipos corporativos.	
	Para asegurarnos una configuración óptima en nuestros equipos es aconsejable que únicamente el personal técnico indicado pueda instalar, actualizar y eliminar software. En los casos en los que no se disponga de dicho personal técnico o este sea externo, se debe documentar y notificar la autorización y la operativa para instalar, actualizar, revisar y eliminar software legal de forma autónoma, para ello se deberá utilizar una cuenta de administrador diferente a la del usuario habitual. En ningún caso debe permitirse la instalación ni la actualización de software a través de enlaces de webs o correos cuyo origen no sea completamente seguro. Por último, remarcar que además de ser legal, el software instalado en los equipos debe estar correctamente actualizado.

[SEG.07.C]	SANCIONES POR USOS NO AUTORIZADOS
La empresa pudiera establecer una política de sanciones por uso no autorizado de software. Consulta a tu responsable.	
	Es importante documentar y dar a conocer las posibles sanciones disciplinarias por el uso de software ilegal o no autorizado. Además, se notificará la posibilidad de acarrear con responsabilidades civiles y penales según la legislación vigente en cada momento en materia de protección de la propiedad intelectual. Con esta medida conseguimos concienciar a la plantilla sobre las consecuencias de utilizar software ilegal.

[SEG.07.D]	REPOSITORIO DE SOFTWARE
El software autorizado y sus correspondientes credenciales de instalación se encuentran en un repositorio autorizado y no debe mantenerse copias en otras ubicaciones no autorizadas ni descargarse de otros sitios de internet.	
	Para poder instalar el software rápidamente se debe determinar las localizaciones donde estará ubicado, así como sus claves de activación, números de serie, licencias, etc. Además, puede ser conveniente registrar metódicamente quien accede a dichos repositorios.

[SEG.07.E]	AUDITORÍAS DE SOFTWARE INSTALADO
El personal técnico o autorizados realizarán auditorías periódicas para analizar que el software instalado en cada uno de los equipos de los usuarios está autorizado y tiene licencia.	
	La organización debe reservarse el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.

[SEG.07.F]	AUTORIZACIÓN Y LICENCIA DEL SOFTWARE
Se debe utilizar en todos los dispositivos software autorizado y que dispone de las correspondientes licencias de uso.	
	Debemos garantizar en todo momento que los programas instalados en cualquier dispositivo corporativo (se incluyen los dispositivos BYOD) están debidamente autorizados y que disponen de las licencias necesarias. Es aconsejable además que los empleados lean y comprendan los términos y condiciones de uso de dichas licencias De este modo podremos cumplir con la Ley de Propiedad Intelectual.

[SEG.07.G]	POLÍTICA DE COPIAS DE SOFTWARE
No se debe realizar copias del software puesto a disposición del empleado si el debido consentimiento del personal responsable.	
	Para garantizar lo especificado en las licencias de uso no se debe permitir que los empleados realicen copias del software disponible sin el debido consentimiento.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

ALMACENAMIENTO EN LOS EQUIPOS DE TRABAJO (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

En el puesto de trabajo los empleados utilizan como herramienta equipos informáticos: ordenadores, tabletas, teléfonos móviles, etc. También generan y transmiten información necesaria para el desempeño de sus funciones. Esta información a veces se almacena de manera local en los discos duros de estos equipos, por lo que surge la necesidad de disponer de una política que regule cómo hacerlo de forma segura. Igualmente deben regularse en forma de políticas el almacenamiento en dispositivos extraíbles, en la nube y en la red corporativa.

La empresa dispondrá de una Política de clasificación de la información. Junto con esta clasificación se elaborará una normativa para el tratamiento de la información crítica y sensible (según el RGPD), que indicará cuando debe ir cifrada, cuando se ha de controlar el acceso a la misma y otras medidas de seguridad a llevar a cabo como las copias de seguridad o la destrucción de la información.

El objetivo es mantener de modo seguro la información almacenada de forma local, especificando reglas, criterios y procedimientos que deben seguir todos los empleados.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.08.A]	QUE SE PUEDE ALMACENAR EN LOS EQUIPOS DE TRABAJO
Únicamente información extrictamente necesaria para la labor que se esté realizando en el momento.	
	Los empleados deben conocer qué tipo de información se puede almacenar en los equipos locales. Para ello redactaremos una normativa que regule el almacenamiento de información en los equipos locales, indicando la información que no debe almacenarse (documentos personales, archivos de música, fotografías, etc.). *Se debe prestar especial atención a los archivos descargados que posean derechos de autor. Los empleados no almacenarán información que no haya sido aprobada por la organización.*

[SEG.08.B]	DÓNDE GUARDAR LA INFORMACIÓN
Se debe respetar el árbol de directorios de trabajo en el servidor, especialmente para aquellos datos confidenciales y sensibles.	
	La normativa debe detallar dónde guardar la información derivada del trabajo dentro del árbol de directorios del equipo. Esta medida facilita la migración de esta información a servidores.

[SEG.08.C]	CONSERVACIÓN DE LA INFORMACIÓN EN DISCOS LOCALES
El tiempo de conservación de la información de forma local será de 1 semana. Después se transferirá a los servidores o se eliminará.	
	Para evitar problemas de espacio en los discos duros estableceremos un periodo de tiempo de conservación de la información. Transcurrido este tiempo, según la información en cuestión, tendremos que decidir si se transfiere a los servidores empresariales o si se elimina definitivamente.

[SEG.08.D]	PERMANENCIA DE LA INFORMACIÓN EN DISCOS LOCALES TRAS SER TRANSFERIDA A LOS SERVIDORES
El tiempo de permanencia de la información en local una vez transmitida a los servidores corporativos es de 24 horas. Después será eliminada.	
	Si la información ya se ha transferido a los servidores corporativos, tendremos que establecer un periodo de permanencia en local para no almacenar por duplicado la información. Después de este periodo de tiempo establecido, la información se borrará del disco duro del equipo.

[SEG.08.E]	CIFRADO DE LA INFORMACIÓN
Se debe cifrar la información crítica y sensible antes de guardarla localmente.	
	El empleado debe conocer cuándo y cómo utilizar el cifrado de documentación, según la Política de uso de técnicas criptográficas. Esta medida es útil en caso de fuga de información o acceso no autorizado.

[SEG.08.F]	CONOCIMIENTO Y APLICACIÓN DE LA NORMATIVA
El personal conoce y aplica la normativa establecida para el almacenamiento en equipo de trabajo.	
	Los empleados deben conocer y aplicar la normativa relativa al almacenamiento en local en sus equipos de trabajo y otras políticas relacionadas.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
ALMACENAMIENTO EN LA NUBE (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Son muchas las razones para almacenar información corporativa en la nube:

- acceder a la información desde cualquier dispositivo y lugar;
- ahorro de recursos y ahorro económico;
- proporciona directorios compartidos con distintos permisos de acceso;
- y permite el trabajo colaborativo sobre un documento.

Pero antes de su implantación en la empresa también deben valorarse sus aspectos negativos como la dependencia de terceros o la necesidad de conexión a internet para tener acceso a la información.

Para que los empleados hagan un buen uso de los recursos de almacenamiento, la empresa dispondrá de una Política de clasificación de la información donde se debe indicar qué tipo de información puede subirse a la nube. Además, se informará al personal sobre el contenido de la misma.

Junto a esta clasificación se elaborará una normativa interna para el tratamiento de la información crítica y sensible, que indicará cuándo debe ir cifrada y otras medidas de seguridad que le aplicarán como backups o borrado seguro de la información.

El objetivo es establecer en qué casos se permite utilizar el almacenamiento en la nube y mantener de modo seguro la información almacenada en la nube, especificando reglas, criterios y procedimientos que deben seguir todos los empleados que usen estos servicios.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.09.A]	USO DE SERVICIOS DE ALMACENAMIENTO EN CLOUD PÚBLICAS
Únicamente se permite el uso de servicios de almacenamiento en cloud públicas autorizadas por la entidad. Solicita información a tu supervisor.	
	El empresario debe decidir si está permitido el uso de servicios de almacenamiento nube pública. El empleado no podrá utilizar este tipo de repositorios si así lo contempla la normativa de la empresa.

[SEG.09.B]	LISTA DE SERVICIOS CLOUD PERMITIDOS
Solicita a tu responsable la lista de servicios de almacenamiento en cloud que están permitidos y cuáles no.	
	Es práctico elaborar y difundir una lista de los servicios de almacenamiento en cloud permitidos y prohibidos. De esta forma evitaremos el uso de servicios de almacenamiento que no consideremos seguros.

[SEG.09.C]	PROCESO DE BORRADO DE LA INFORMACIÓN EN LA NUBE
Para el borrado de datos almacenados en la nube debe tenerse en cuenta que también se tiene que vaciar la papelera del servicio de almacenamiento, así como todas las copias ubicadas en los equipos sincronizados, incluidas las papeleras de reciclaje de dichos equipos.	
	Tendremos una Política de borrado de la información que también debemos aplicar cuando se elimina información almacenada en la información en la nube.

[SEG.09.D]	TIPO DE INFORMACIÓN ALMACENADA Y TRATAMIENTO
Toda información crítica, confidencial o sensible debe ser cifrada antes de ser almacenada en la nube.	
	El empleado debe conocer qué tipo de información puede almacenarse en la nube (y cual no) y en qué casos tendrá que almacenarse cifrada. La política de clasificación de la información incluirá este dato.

[SEG.09.E]	CONTRATACIÓN DE SERVICIOS DE ALMACENAMIENTO EN LA NUBE
Los servicios de almacenamiento en cloud contratados por la entidad deben cumplir con los criterios organizativos y de seguridad establecidos en la normativa vigente de protección de datos. No es decisión del usuario.	
	A la hora de contratar un servicio de almacenamiento en cloud, tenemos que asegurarnos que cumple con los criterios de seguridad específicos que precisa la información que vamos a almacenar en la nube (garantía de confidencialidad, disponibilidad de la información, copias de seguridad, etc.), así como con las necesidades legales si se trataran de datos personales.

[SEG.09.F]	COPIAS DE SEGURIDAD EN LA NUBE
Los servicios de copia de seguridad en la nube pueden ser muy útiles, pero hay que analizar las ventajas y los inconvenientes de este servicio. El empresario debe decidir si se permite o no las copias de seguridad en la nube.	

	Se han de valorar las ventajas e inconvenientes de realizar copias de seguridad en la nube antes de realizarlas.
	• ***Ventajas:***
	  • *Disponer de más espacio para realizar la copia de seguridad a medida que lo necesitemos.*
	  • *La mayoría de los servicios en la nube realiza copias de seguridad como garantía de disponibilidad.*
	  • *Disponer de una copia fuera de las dependencias de la empresa. En caso de que se produjera un incidente, nuestra información no se vería afectada y podríamos recuperarla.*
	• ***Inconvenientes:***
	  • *Depender de terceros que tendrán sus riesgos propios que pueden quedar fuera de nuestro control.*

[SEG.09.G]	POLÍTICA DE SEGURIDAD DEL PROVEEDOR
Es necesario analizar la política de seguridad del proveedor de servicios para asegurarse del cumplimiento de las normativas vigentes.	
	Antes de contratar servicios en la nube que traten información de la empresa debemos leer y comprender la política de seguridad del proveedor de servicios para asegurar que cumple todas nuestras necesidades. *Es imprescindible disponer de medios que demuestren y garanticen que el proveedor de servicio cumple con la normativa de protección de datos y está ha implementado las medidas de seguridad técnicas y organizativas para velar por la integridad, confidencialidad y disponiblidad de la información.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

ALMACENAMIENTO EN DISPOSITIVOS EXTRAIBLES (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Los dispositivos de almacenamiento extraíble (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) permiten una transferencia rápida y directa de información. Hoy en día son imprescindibles y muy utilizados. Debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus.

La empresa debe decidir si se permite el uso de dispositivos de almacenamiento externo, y de ser así, debe disponer de una normativa que contemple en qué situaciones pueden utilizarse y qué tipo de información se permite guardar en ellos.

Si se necesita almacenar información sensible o confidencial se utilizarán dispositivos externos corporativos debidamente protegidos, se almacenarán en lugares seguros y se informará al responsable si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.).

En el caso de que se permita el uso de dispositivos personales (dispositivos extraíbles propiedad del empleado) se aplicarán las normas de seguridad recogidas en la política correspondiente.

Para asegurar la información contenida en los dispositivos extraíbles tendremos que aplicar medidas de seguridad como: cifrar los datos almacenados, establecer permisos de acceso, cambiar periódicamente la contraseña, etc.

Otro de los aspectos importantes a tener en cuenta es la eliminación de la información almacenada. Para asegurar que estos datos no volverán a ser accesibles, debemos utilizar los métodos de borrado seguro: destrucción física del dispositivo, desmagnetización o sobre-escritura, según convenga en cada caso.

En definitiva, debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren, así como concienciar a los empleados para su buen uso. De esta forma protegeremos tanto la información contenida en ellos como la de los dispositivos a los que se conectan.

El objetivo es establecer unas normas de uso de los dispositivos extraíbles que garanticen la seguridad de la información corporativa que almacenan y la de los equipos a los que se conectan.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.10.A]	ALTERNATIVAS A LOS MEDIOS DE ALMACENAMIENTO EXTRAIBLE
Siempre que sea posible se debe evitar el uso de dispositivos de almacenamiento externo y optar por medios alternativos (repositorios comunes o carpetas compartidas, clouds autorizados, etc.)	
	Para evitar la necesidad del uso de estos soportes pueden implantarse las siguientes alternativas: • *utilizar repositorios comunes para el intercambio de información;* • *implantar la posibilidad de acceso remoto para poder trabajar desde fuera de la oficina;* • *usar los servicios de almacenamiento en la nube autorizados por la organización.*

[SEG.10.B]	REGISTRO DE USUARIOS Y DISPOSITIVOS
Debe existir una lista actualizada de los dispositivos extraibles autorizados, usuarios asignados e información que almacena, por lo que no se deben utilizar dispositivos extraíbles no inventariados.	
	Tenemos que mantener un registro de dispositivos detallando los privilegios de acceso asignados a cada usuario que los necesite.

[SEG.10.C]	MEDIDAS TÉCNICAS PARA GARANTIZAR LA SEGURIDAD POR DISPOSITIVOS CONECTADOS
No se deben conectar dispositivos extraíbles no autorizados pues pueden ser portadores de malware. Se deben aplicar medidas para el almacenamiento seguro de la información en el dispositivo extraíble (cifrado de datos, autenticación, cambio periódico de contraseñas, etc.)	

	Estas medidas podrán aplicarse sobre los dispositivo extraíbles que se conecta. Por ejemplo:
	• *Sobre el **dispositivo extraíble**:*
	  • *Programar cambios periódicos de contraseña de acceso al dispositivo.*
	• *Sobre los **dispositivos a los que se conectan**:*
	  • *Implementar mecanismos de autenticación de usuarios.*
	  • *Evitar que dispositivos no registrados puedan conectarse a cualquier equipo de la organización.*
	  • *Desactivar la opción de autoarranque en los equipos para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles son enchufados.*
	  • *Deshabilitar por defecto los puertos USB y habilitarlos para el personal que necesite dicha funcionalidad de manera periódica o gestione ficheros de gran tamaño.*

[SEG.10.D]	MEDIDAS TÉCNICAS PARA GARANTIZAR UN ALMACENAMIENTO SEGURO DE LA INFORMACIÓN SOBRE LOS DOCUMENTOS
Se deben aplicar medidas para el almacenamiento seguro de la información en los documentos que se transfieren (control de accesos, cifrado, etc.)	
	Estas medidas podrán aplicarse sobre los documentos que se transfieren. Por ejemplo • *Establecer control de accesos con permisos de lectura, escritura y ejecución.* • *Implementar mecanismos de cifrado de la documentación.*

[SEG.10.E]	NORMATIVA DE ALMACENAMIENTO EN DISPOSITIVOS EXTRAIBLES
Deberá existir una normativa que regule el uso de dispositivos extraibles	
	Si no disponemos aún de ella tendremos que elaborar una normativa que regule el uso de dispositivos extraíbles que incluya: • *llevar un registro de los dispositivos autorizados;* • *definir en qué condiciones o casos se permite su uso;* • *definir cómo se accede y si la información debe ir cifrada;* • *establecer las configuraciones de seguridad necesarias para poder utilizarlos, etc.*

[SEG.10.F]	CONCIENCIACIÓN DE LOS EMPLEADOS
El personal deberá tomar conciencia sobre la criticidad del almacenamiento en dispositivos extraibles	
	El robo o extravío, la manipulación, y la infección por virus de los dispositivos extraíbles son las causas más frecuentes por las que puede perderse la información contenida en ellos. Por eso es importante involucrar a los usuarios en la protección, vigilancia y buen uso de estos dispositivos, concienciándolos de la trascendencia de la protección del mismo y de los datos que contiene.

[SEG.10.G]	CUMPLIMIENTO DE LA NORMATIVA
El personal deberá de aceptar el cumplimiento de la normativa	
	Tendremos que comunicar esta normativa y asegurarnos de que los empleados la conocen y se comprometen a cumplirla antes de utilizar dispositivos extraibles en el entorno de trabajo.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

BORRADO SEGURO Y GESTIÓN DE SOPORTES (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Cuando la información deja de ser necesaria para la organización llega a la última fase de su ciclo de vida y es necesario destruirla de forma segura. Esta opción es indispensable si queremos que la información no vuelva a ser accesible y cumplir con la Ley de Protección de Datos, cuando contenga datos de carácter personal.

También debemos utilizar el borrado seguro cuando queremos:

- reutilizar un soporte:
  - que ya contiene datos corporativos;
  - que no funciona correctamente;
- o deshacernos de un soporte que se ha quedado obsoleto.

En el caso de que la información esté en soportes no electrónicos (papel, negativos fotográficos, radiografías, cintas magnéticas, etc.) es necesario usar una trituradora para deshacernos de la información. En caso contrario podría llegar a manos de terceros y utilizarse de forma perjudicial para la empresa.

Por otro lado, si vamos a contratar a terceros la destrucción de nuestros datos o de los soportes, debemos elegir la destrucción certificada si se trata de (o si contienen) datos personales o confidenciales. Esta opción nos asegura la destrucción de la información con las máximas garantías de seguridad y confidencialidad, desde la recogida del material documental hasta su destrucción física y eliminación final.

El objetivo es establecer normas para el borrado seguro de la información obsoleta y para destrucción de soportes acorde a las necesidades de la empresa.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
  - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.11.A]	INVENTARIO DE ACTIVOS
Existe un inventario y se hace seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad de los datos.	
	Tendremos que realizar un seguimiento de los dispositivos que están en funcionamiento (CD, DVD, Flash USB, discos magnéticos, tarjetas de memoria…), las personas o departamentos responsables de esos dispositivos, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.

[SEG.11.B]	GESTIÓN DE SOPORTES
Se supervisan los dispositivos que almacenan información corporativa, en particular aquellos que se utilizan para realizar copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc.	
	Supervisaremos los dispositivos que almacenan información corporativa, en particular los que se usan para realizar las copias de seguridad, documentando cualquier operación realizada sobre los mismos: mantenimiento, reparación, sustitución, etc.

[SEG.11.C]	ELIMINACIÓN DE LA INFORMACIÓN EN SOPORTES NO ELECTRÓNICOS Y SOPORTE MAGNÉTICOS
Se debe utilizar el proceso de triturado para destruir la información de los soportes no electrónicos (papel y soportes magnéticos)	
	Para eliminar la información que ya no se considera necesaria para la organización en este tipo de soportes (documentos impresos, CD, DVD, cintas magnéticas, radiografías, etc.) debemos utilizar la opción de triturado como modo seguro de eliminación.

[SEG.11.D]	ELIMINACIÓN DE LA INFORMACIÓN PARA LA REUTILIZACIÓN DE SOPORTES ELECTRÓNICOS
Se debe optar por el proceso de formateo y sobreescritura cuando se quiera reutilizar un soporte todavía en buen estado.	
	Si queremos reutilizar un soporte que ya contiene datos, debemos utilizar la opción de sobreescritura para garantizar un borrado total de la información. La sobreescritura se puede utilizar en todos los dispositivos regrabables (discos duros, pendrives o pinchos USB, etc.) siempre que el dispositivo no esté dañado.

[SEG.11.E]	ELIMINACIÓN DE LA INFORMACIÓN ANTES DE DESHACERNOS DE SOPORTES ELECTRÓNICOS
Se debe usar el proceso de desmagnetización o de destrucción física antes de desechar el soporte de almacenamiento.	
	Cuando queremos desechar algún soporte de almacenamiento porque ya no funcione o porque se haya quedado obsoleto debemos utilizar los métodos de desmagnetización o destrucción física. Cualquiera de estos dos métodos imposibilita la reutilización del dispositivo.

[SEG.11.F]	BORRADO DE INFORMACIÓN EN OTROS DISPOSITIVOS
Se debe eliminar la información en teléfonos móviles, impresoras, GPS, etc. (memoria y tarjetas) antes de deshacernos de ellos.	
	Prestar una especial atención cuando queramos deshacernos de dispositivos móviles (smartphones, tabletas, etc.) y dispositivos que almacenan información de uso (impresoras, GPS, etc.) ya que también pueden contener información empresarial confidencial.

[SEG.11.G]	DOCUMENTACIÓN DE LAS OPERACIONES DE BORRADO REALIZADAS
Se debe utilizar una herramienta de borrado que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado. Consulta con el personal técnico.	
	Al seleccionar una herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado.

[SEG.11.H]	DESTRUCCIÓN CERTIFICADA
En caso de optar por la contratación de servicios de destrucción, este debe certificar la destrucción de los datos confidenciales.	
	Existe la opción de contratar una empresa que realice una destrucción certificada. Esta empresa se encargará de llevar a cabo el proceso de eliminación de la información garantizando la gestión y control de recogida, transporte y destrucción del material confidencial. Después de llevar a cabo la destrucción, la empresa emite un certificado que garantiza la validez de todo el proceso. *Esta alternativa es muy útil si queremos garantizar la destrucción de datos confidenciales (cumpliendo la normativa de la RGPD) y en el caso de que nos viéramos obligados a ello por un contrato o acuerdo con otra empresa.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

CONTROL DE ACCESO (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Controlar quien accede a la información de nuestra empresa es un primer paso para protegerla. Es esencial que podamos decidir quién tiene permisos para acceder a nuestra información, como, cuando y con qué finalidad.

A la hora de gestionar el control de acceso a nuestros datos debemos tener en cuenta que la información, los servicios y las aplicaciones utilizadas no tienen por qué ubicarse de manera centralizada en nuestras instalaciones, sino que pueden estar diseminadas en equipos y redes remotas propias o de terceros. También tenemos que considerar que cada vez es más habitual el uso de dispositivos móviles en los centros de trabajo. En ocasiones estos dispositivos son propiedad del propio empleado lo que dificulta esta tarea.

Por otra parte, el registro de los accesos en logs de los sistemas va a ser determinante para analizar los incidentes de seguridad.

El objetivo es establecer quien, como y cuando puede acceder a los activos de información de la empresa y registrar convenientemente dichos accesos.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.12.A]	POLÍTICA DE USUARIOS Y GRUPOS
Se han definido roles de usuarios y de grupos en función del tipo de información al que podrán acceder.	
	Definiremos una serie de grupos que tendrán determinados accesos para cada tipo de información establecido. Esta clasificación se puede hacer teniendo en cuenta los siguientes aspectos: • *en función del área o departamento al que pertenezca el empleado;* • *en función del tipo de información a la qué accederá;* • *en función de las operaciones permitidas sobre la información a la que se tiene acceso.* *En función de los criterios anteriores podemos establecer diversos perfiles de usuarios.*

[SEG.12.B]	ASIGNACIÓN DE PERMISOS
Cada usuario o grupo dispone de los permisos necesarios y únicos para realizar las acciones oportunas sobre la información a la que tienen acceso y estrictamente necesarias para el desempeño de sus actividades laborales.	
	Una vez establecidos los tipos de información, los perfiles de usuarios y los grupos existentes, podremos concretar los tipos de acceso a la información a los que tienen derecho. Los permisos concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el mínimo privilegio en el establecimiento de los permisos.

[SEG.12.C]	CREACIÓN, MODIFICACIÓN Y BORRADO DE CUENTAS DE USUARIOS CON PERMISOS
Únicamente podrán realizarlo personal técnico autorizado.	
	Para permitir el acceso real a los sistemas de información de la empresa debemos tener un procedimiento que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios (por ejemplo: cuenta de correo, acceso al CRM, etc.) indicando quién debe autorizarlo. Detallaremos los datos identificativos de las mismas, las acciones que se permiten y las dotaremos de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales, así como de la Política de contraseñas.

[SEG.12.D]	CUENTAS DE USUARIO ADMINISTRADORES
En la medida de lo posible, se evitará el uso de las cuentas de usuarios con privilegios de administrador.	
	Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Tendremos en cuenta los siguientes aspectos: • *utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración;* • *implantar un control de acceso basado en un doble factor de autenticación;* • *registrar convenientemente todas sus acciones (registro de logs);* • *cuando accedemos a un sistema en modo administrador, este debe indicarnos claramente tal situación a través de su contexto;* • *el acceso como administrador debería ser notificado convenientemente;* • *evitar que los privilegios de las cuentas de administrador puedan ser heredados;* • *las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia;* • *pueden ser sometidas a auditorías periódicas.*

[SEG.12.E]	MECANISMOS DE AUTENTICACIÓN
Cada usuario debe disponer de su usuario y contraseña unipersonal, incluso si usan el mismo equipo o tienen el mismo rol y privilegios.	

	Definiremos e implantaremos los mecanismos de autenticación más adecuados para permitir el acceso a la información de nuestra empresa. Tendremos en cuenta aspectos tales como:
	• *utilizar mecanismos de autenticación internos o basados en servicios de autenticación de terceros (como la federación de identidades o el social-login)*
	• *las tecnologías que utilizaremos:*
	  • *autenticación vía web*
	  • *servicios de directorio*
	  • *LDAP*
	• *factores de los mecanismos de autenticación (uno o varios):*
	  • *algo que somos (a través de técnicas biométricas)*
	  • *algo que sabemos (a través de contraseñas)*
	  • *algo que tenemos (a través de dispositivos personales, tokens criptográficos)*

[SEG.12.F]	REGISTRO DE EVENTOS
Se han establecido mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa.	
	Estableceremos los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa. Registraremos convenientemente quién accede a nuestra información, cuando, cómo y con qué finalidad.

[SEG.12.G]	REVISIÓN DE PERMISOS
Cada cierto tiempo se revisan los permisos concedidos a los usuarios para confirmar que son los adecuados.	
	Revisaremos periódicamente que los permisos concedidos a los usuarios son los adecuados.

[SEG.12.H]	REVOCACIÓN DE PERMISOS Y ELIMINACIÓN DE CUENTAS
Se desactivarán los permisos de acceso y se eliminarán las cuentas de usuario una vez finalizada la relación contractual	
	Al finalizar la relación contractual con el empleado es necesario revocar sus permisos de accesos a nuestros sistemas e instalaciones. Eliminaremos sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, exigiremos la devolución de cualquier activo de información que se le hubiese asignado (tarjetas de acceso o de crédito, equipos, dispositivos de almacenamiento, tokens criptográficos, etc.).

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
ANTI-MALWARE (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

La aparición constante de nuevos virus y otros tipos de malware es una de las principales amenazas a las que se enfrentan hoy en día nuestros sistemas.

Las vías de contagio por malware son numerosas, destacando entre otras:

- las descargas de ficheros de todo tipo, adjuntos en correos o desde páginas web;
- la navegación por webs de dudosa fiabilidad;
- y la utilización de dispositivos ajenos, por ejemplo, pendrives.

El enorme daño que pueden causar a nuestra organización hace obligatorio el establecimiento de una política de control de malware. De este modo podremos prevenir, detectar, controlar y eliminar la ejecución de cualquier software malicioso en nuestros sistemas.

El objetivo es proteger todos los activos de información de la empresa contra la infección por virus o cualquier otro tipo de malware.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.13.A]	INSTALACIÓN DE SOLUCIÓN ANTI-MALWARE
Todos los equipos deben disponer de una solución anti-malware instalada, activada y actualizada.	

	Dependiendo del tamaño de nuestra organización, del nivel de seguridad necesario y de la complejidad de las configuraciones para la protección de nuestros activos de información, podremos determinar distintos tipos de soluciones:
	• *herramientas para el puesto de trabajo, el portátil o los dispositivos móviles,*
	• *soluciones globales corporativas entre ellas:*
	  • *UTM o gestión unificada de amenazas;*
	  • *servicios gestionados que nos pueden facilitar nuestros proveedores de servicios de internet (ISP) u otros proveedores desde un centro de operaciones de seguridad o SOC;*
	  • *soluciones de seguridad ofrecidas como servicios en la nube que monitorizan nuestros equipos de forma remota.*
	Para el tipo de solución elegida, seleccionaremos la más apropiada de entre las disponibles en el mercado buscando la compatibilidad con nuestras infraestructuras y la versatilidad (anti-malware, antiphishing, antispam, análisis de web y correo…) de la herramienta.

[SEG.13.B]	CONFIGURACIÓN DE HERRAMIENTAS DE DETECCIÓN DE MALWARE
Se deben configurar correctamente todas las funcionalidades de las herramientas de control de malware. Solicita soporte técnico.	
	Para un uso eficiente de las herramientas de control de malware se debe realizar una correcta configuración de todas sus funcionalidades. La configuración deberá permitirnos, entre otros, establecer los siguientes controles: • *realizar análisis automáticos y periódicos para detectar malware;* • *realizar comprobaciones automáticas de los ficheros adjuntos al correo y de las descargas web, ya que pueden contener código malicioso ejecutable;* • *bloquear el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas negras;* • *permitir el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas blancas;* • *permitir el análisis de páginas web para detectar posibles amenazas incluidas en las mismas.*

[SEG.13.C]	ACTUALIZACIÓN DE LAS HERRAMIENTAS DE MALWARE
Se debe activar el proceso de actualización automática de las herramientas de detección y control de malware instaladas en el equipo.	
	Debemos determinar la periodicidad con la que las herramientas de detección de malware son actualizadas. Actualmente se crean miles de virus al día, por lo que las actualizaciones de la base de datos de firmas de virus deberían ser automáticas y tener una periodicidad como mínimo diaria. Por otro lado, y como cualquier otra aplicación crítica, tendremos que actualizar convenientemente el propio software antivirus.

[SEG.13.D]	PROGRAMADO PERIÓDICO DE ANÁLISIS DE MALWARE
Se deben programar análisis periódicos de búsqueda de malware en los dispositivos.	
	El personal técnico adecuado deberá configurar el análisis de malware en los dispositivos de forma periódica. Debera de establecerse una frecuencia análisis adecuada para asegurarse que el dispositivo se mantiene limpio.

[SEG.13.E]	ESTABLECIMIENTO DE RESPUESTA ANTE INFECCIÓN POR EJECUCIÓN DE MALWARE
En caso de infección de malware, se debe apagar inmediatamente el equipo y desconectar en cable de red. Avisar urgentemente al equipo técnico	
	*En primer lugar, determinaremos qué **sucesos** serán considerados como incidencias por ejecución de malware, analizando:* • *el impacto del ataque;* • *los activos que puedan estar comprometidos;* • *la forma de recuperar los activos impactados;* • *los canales adecuados de aviso y notificación.* *Después estableceremos las **responsabilidades** y la **operativa** a seguir en cada caso:* • *desinfección de ficheros;* • *eliminación de ficheros;* • *aviso a soporte técnico del fabricante;* • *reinstalación de software afectado;* • *desconexión y asilamiento del equipo afectado;* • *y el registro formal del incidente.*

[SEG.13.F]	BUENAS PRÁCTICAS PARA EL CONTROL DE MALWARE
El personal debe seguir las directrices básicas para prevenir las infecciones por malware.	

	Con el fin de reforzar las medidas establecidas para el control del malware es conveniente tener concienciada a la plantilla en los siguientes aspectos:
	• *Se deben considerar todos los contenidos y las descargas como potencialmente inseguros hasta que no sean convenientemente analizados por una herramienta de detección de malware.*
	• *Deben prohibirse las siguientes acciones:*
	  • *Ejecutar ficheros descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.*
	  • *Configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.*
	  • *Alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.*
	• *Debe utilizarse únicamente el software permitido por la organización. Este además debe estar convenientemente actualizado.*
	• *Para evitar la recepción de spam se deben seguir las directrices incluidas en la política de correo electrónico.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

RESPUESTA A INCIDENTES (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Es un hecho que a pesar de las medidas que implantemos, siempre existe el riesgo de que ocurra un incidente de ciberseguridad. Por ello, debemos preparar un plan de acción que nos indique cómo actuar de la manera más eficaz posible en estos casos.

Existen muchos tipos de incidentes de ciberseguridad, algunos son más habituales que otros que podrían encajar en una de las siguientes tipologías:

- incidentes no intencionados o involuntarios;
- daños físicos;
- incumplimiento o violación de requisitos y regulaciones legales;
- fallos en las configuraciones;
- denegación de servicio;
- acceso no autorizado, espionaje y robo de información;
- borrado o pérdida de información;
- infección por código malicioso.

Para ejecutar correctamente el plan y evitar que el daño se extienda se deben detallar las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

Tras un incidente, si hemos aplicado el plan, tendremos una valiosa información para conocer y valorar los riesgos existentes, y así evitar incidentes similares en el futuro.

En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el plan de contingencia y continuidad del negocio.

El objetivo es asegurarnos de que todos los miembros de la organización conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.14.A]	EQUIPO RESPONSABLE
Existe un equipo responsable que se encargará de gestionar los incidentes de seguridad. Consulta con tu supervisor	
	Para garantizar una respuesta eficaz durante el tratamiento de incidentes de ciberseguridad, nombraremos un equipo responsable de su gestión. Tendremos que considerar no solo al personal técnico encargado de su resolución (interno o externo), sino también personal de la dirección que debiera estar informado en todo momento del estado del incidente.

[SEG.14.B]	MEJORA CONTINUA
Es importante aportar toda la información posible ante los incidentes, con el objetivo de documentarlo y disponer de una mejora continua.	
	Es conveniente analizar la utilidad de usar la información recogida en la gestión de los incidentes para medir y evaluar la posibilidad de modificar procedimientos o añadir nuevas mejoras o controles para limitar futuros daños. Podemos realizar acciones preventivas con el fin de entrenar a la plantilla ante la aparición de un posible incidente. *Determinaremos la periodicidad con la que debe actualizar el plan y las medidas a adoptar. También puede ser necesaria una actualización del plan tras un cambio significativo en nuestros sistemas.*

[SEG.14.C]	DETECCIÓN DEL INCIDENTE
Cualquier incidente debe ser comunicado inmediatamente al personal responsable en cuanto se detecte.	
	Debemos concretar las situaciones que se considerarán incidentes. Desplegaremos herramientas con mecanismos de detección automáticos y estableceremos un sistema de alerta que nos informe detalladamente de lo sucedido en tiempo real.

[SEG.14.D]	EVALUACIÓN DEL INCIDENTE
El equipo responsable de gestionar el incidente categorizará convenientemente el incidente y le otorgará la criticidad correspondiente	
	Una vez detectado el incidente debemos categorizarlo convenientemente y establecer la gravedad y la prioridad en su tratamiento.

[SEG.14.E]	NOTIFICACIÓN DE INCIDENTES
El procedimiento para la notificación de un incidente es de primera mano, es decir, comunicado personalmente al supervisor o equipo responsable de gestionar los incidentes.	
	Procuraremos establecer un punto de contacto único donde los empleados deben notificar los posibles incidentes o puntos débiles detectados. Asimismo, se debe indicar la información a recabar y las acciones inmediatas a seguir en el momento de la notificación. Conviene tener un listado de contactos para actuar con rapidez en caso de incidente.

[SEG.14.F]	RESOLUCIÓN DE INCIDENTE
El equipo de gestión de incidentes desarrollará procedimientos detallados de actuación para dar respuesta a cada tipología de incidente de seguridad.	
	Desarrollaremos y documentaremos procedimientos de respuesta para cada uno de los tipos de incidentes definidos previamente, poniendo especial énfasis en aquellos incidentes más habituales y peligrosos. Se detallarán al menos los procedimientos para las siguientes acciones. • *recogida de evidencias tan pronto como sea posible tras la aparición del incidente, con cuidado de mantener la cadena de custodia, la integridad de las evidencias (cifrándolas si es necesario), soportes, etc.;* • *estimación del tiempo de resolución;* • *realización de un análisis forense en los supuestos requeridos;* • *escalado conveniente del incidente en caso de no poder ser solventado;* • *ejecución de acciones concretas para intentar reparar, mitigar o contener los daños causados por el incidente.*

[SEG.14.G]	TRATAMIENTO DEL REGISTRO DEL INCIDENTE
Se debe llevar un registro de forma conveniente de toda la información relativa a la gestión del incidente.	
	Para disponer de toda la información acerca del incidente se registrarán convenientemente, almacenándose, entre otra, la información relativa a: • *fecha y hora de aparición del incidente;* • *tipología y gravedad del mismo;* • *recursos afectados;* • *posibles orígenes;* • *estado actual del incidente;* • *acciones realizadas para solventarlo y quienes las ejecutaron;* • *fecha y hora de resolución y cierre del incidente.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
TÉCNICAS CRIPTOGRÁFICAS (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

La información sensible y confidencial que manejamos en la empresa:

- bases de datos, registros de usuarios, correos electrónicos confidenciales;
- información sujeta a protección legal;
- backups;
- información confidencial en dispositivos extraíbles y móviles;
- credenciales de acceso y para pagos online, etc.

Por su trascendencia para nuestro negocio debe estar especialmente protegida tanto en tránsito como cuando está almacenada.

Para proteger esta información, además de controlar el acceso a la misma y proteger los sistemas con los que la manejamos, utilizaremos herramientas criptográficas que cifren nuestros datos, haciéndolos ilegibles por aquellos que no dispongan de la clave de cifrado. De esta manera garantizaremos la confidencialidad e integridad de la información sensible cuando está almacenada.

Las técnicas criptográficas permiten también firmar digitalmente documentos y correos electrónicos relevantes (como facturas, contratos, etc.), lo que garantiza además la autenticidad y no repudio de los mismos. Esto es muy útil en el caso de realizar ciertas gestiones online, como las realizadas con la administración.

Tanto para el cifrado de la información como para el uso de la firma digital, se debería realizar un análisis previo que determine claramente que datos de la empresa se deben cifrar y que situaciones o usuarios requieren de firma digital.

Asimismo, cabe destacar la importancia de utilizar protocolos seguros en nuestras comunicaciones, tanto para nuestros empleados como para los usuarios de nuestros servicios. En particular se aconseja el uso de certificados web de validación extendida para los servicios gestionados a través de la web (sobre todo si conllevan transacciones económicas como en las tiendas online) o el uso de VPN para el acceso de teletrabajadores.

El objetivo es garantizar que se hace un uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad, integridad, autenticidad y el no repudio de la información sensible manejada por la empresa, tanto almacenada como en tránsito. Por ejemplo: datos de carácter personal, información sensible o información confidencial, backups en la nube o en proveedores externos, datos en móviles o dispositivos extraíbles, contratos, facturas e intercambios comerciales o con las Administraciones Públicas, accesos remotos, etc.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.15.A]	INFORMACIÓN SUSCEPTIBLE DE SER CIFRADAS
Cualquier información confidencial, crítica, sensible, de salud, datos penales o sanciones administrativas, y de menores.	
	La clasificación de la información nos ha de servir para saber qué información debe ser cifrada para garantizar su confidencialidad e integridad. Dicha información puede ser: • *información sensible, de carácter personal o confidencial;* • *registros con credenciales de autenticación;* • *información almacenada en dispositivos personales o de terceros (incluidos los servicios cloud) que carecen de los controles de seguridad adecuados;* • *información transferida a través de redes de telecomunicación no confiables o en soportes de almacenamiento físicos no protegidos adecuadamente.*

[SEG.15.B]	USO DE FIRMA ELECTRÓNICA
Para los intercambios comerciales y con las sedes electrónicas de la Administración Pública, es obligatorio el uso de la firma electrónica.	
	Haremos uso de la firma electrónica en aquellos escenarios en los que sea imprescindible garantizar la autenticidad y el no repudio de la información, como para realizar trámites con las Administraciones Públicas o emitir facturas. Tendremos que elegir qué tipo de certificado de representación legal queremos implantar: • *certificado de persona jurídica;* • *certificado de pertenencia a empresa;* • *certificado de representante;* • *certificado de factura electrónica.* *Seleccionaremos el prestador de servicios que generará nuestros certificados. Además, controlaremos:* • *periodo de validez;* • *posibilidad de revocación;* • *cumplimiento con la legislación (prestadores cualificados);* • *gestión de su almacenamiento.*

[SEG.15.C]	CIFRADO DE DATOS SENSIBLES CUANDO SE CONTRATAN SERVICIOS EXTERNOS
Es especialmente importante comprobar que se utilizan canales cifrados para las comunicaciones y herramientas de cifrado en el tratamiento de la información sensible al contratar servicios.	
	Si necesitamos contratar servicios externos que traten datos confidenciales o sensibles verificaremos que las trasferencias de datos son seguras, bien cifrando los datos antes de transferirlos o bien utilizando canales seguros. Estos son algunos ejemplos: • *si contratamos un servicio de gestión que incluya el tratamiento de datos personales (por ejemplo: nóminas, seguridad social…) o confidenciales nos aseguraremos que las transferencias de datos se realizan con canales cifrados (por ejemplo vía VPN o cifrando los datos antes de enviarlos);* • *si hacemos backup en la nube de ficheros que contengan datos confidenciales o datos personales de empleados o clientes, tendremos que cifrarlos;* • *si contratamos pasarelas de pago para nuestra tienda online, siempre que sea posible, es preferible no almacenar datos de transacciones en nuestra web (cuentas, tarjetas…), eligiendo proveedores que hagan toda la transacción cumpliendo el estándar PCI-DSS.*

[SEG.15.D]	CIFRADO DE DATOS SENSIBLES CUANDO SE SOLICITAN DESARROLLOS DE APLICACIONES
Las credenciales de acceso deben ser cifradas cuando se solicitan desarrolles web o apps que impliquen *login* de usuarios.	
	Si vamos a contratar el desarrollo de un aplicativo web o una app para dispositivos móviles que ofrezca acceso a nuestros usuarios (login), las claves de acceso han de almacenarse cifradas. Todos los desarrollos que traten datos personales deben contemplar criterios de privacidad por defecto y por diseño. • *La privacidad por diseño es la que incorpora, desde que se concibe un servicio hasta en su despliegue y operación, las medidas tecnológicas para preservar la privacidad de los usuarios.* • *La privacidad por defecto protege los datos del usuario en los ajustes por defecto. El diseñador de los servicios, bien por su construcción, o en los parámetros configurables por el usuario, elegirá los más respetuosos con la privacidad, no permitiendo funcionalidades extendidas por defecto que afecten a los datos de los usuarios, a no ser que este las elija explícitamente.*

[SEG.15.E]	ACCESO DESDE EL EXTERIOR CON VPN
El acceso desde el exterior a los sistemas y dispositivos corporativos deben realizarse mediante canales VPN cifrados.	
	Si tenemos teletrabajadores o autorizamos el acceso desde el exterior a los servidores de nuestras instalaciones, tendremos que habilitar canales VPN cifrados que garanticen la confidencialidad e integridad de las comunicaciones siguiendo la Política de uso de wifis y conexiones externas.

[SEG.15.F]	CERTIFICADOS WEB
Se deberán de uitilizar certificado web válidos para la encriptación de las comunicaciones web especialmente cuando se traten de tiendas online.	
	Para garantizar la seguridad de la información en nuestro sitio web, en especial si se trata de una tienda online adquiriremos un certificado web (SSL/TLS): • *para un dominio, múltiples dominios y subdominios, wildcard;* • *validación de dominio, de la organización y validación extendida (para tiendas online).*

[SEG.15.G]	ALGORITMOS DE CIFRADO AUTORIZADOS
Se deberán de utilizar algoritmos de cifrado vigentes para asegurar la confidencialidad de la informaición. En caso de que se conozca que el algoritmo que se esté utilizando deja de ser seguro, será necesario cambiar el algoritmo para evitar que existan vulnerabilidades.	
	Para evitar el uso de sistemas de cifrado obsoletos debemos aplicar algoritmos de cifrado actuales comprobando que estén vigentes. Se tendrán en cuenta de forma prioritaria los algoritmos y sistemas de cifrado de carácter abierto y de especificación pública (conocidos y evaluados ampliamente). Se aconseja el uso de sistemas de cifrado asimétrico en detrimento de los sistemas de cifrado simétrico.

[SEG.15.H]	APLICACIONES AUTORIZADAS PARA USOS CRIPTOGRÁFICOS
La entidad dispone de una lista de aplicaciones autorizadas para el cifrado de datos y de dispositivos. Solicita información al personal técnico.	
	Conviene tener una lista de las aplicaciones autorizadas para fines criptográficos. Asimismo, podemos detallar el uso concreto de cada una de ellas. • *cifrado del disco de arranque;* • *cifrado de discos internos y extraíbles;* • *cifrado de correo;* • *cifrado de backups;* • *cifrado de ficheros y directorios;* • *cifrado de dispositivos móviles.*

[SEG.15.I]	USO DE PROTOCOLOS SEGUROS DE COMUNICACIÓN
Se deben implementar protocolos seguros para acceder (administración, transferencia de ficheros, etc.) a los servidores tanto si están en nuestras instalaciones como si están en algún proveedor.	
	Tendremos que proporcionar a los empleados, si las necesitan para su actividad, formación y herramientas de comunicación que utilicen protocolos criptográficos actualizados. De esta forma podremos garantizar la confidencialidad al acceder a nuestros sistemas, tanto si se ubican en nuestras instalaciones como si se ubican en las instalaciones de proveedores. Entre otros se incluyen los siguientes protocolos: • *SSH para el acceso seguro remoto a la administración de equipos (no utilizar Telnet que no va cifrado);* • *SFTP/FTPS para la transferencia segura de ficheros;* • *HTTPS para la transferencia segura de datos en servicios web críticos (pagos online, descarga de información sensible, etc.).*

[SEG.15.J]	CIFRADO DE LA RED WIFI DE LA EMPRESA
La red WiFi de la empresa debe estar configurada con el estándar de cifrado más seguro, actualmente el WPA2.	
	Configuras la wifi de la empresa con el estándar de cifrado más seguro, actualmente WPA2, y cambiaremos su clave de acceso por defecto.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
COPIAS DE SEGURIDAD (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Los medios de almacenamiento contienen uno de nuestros activos más preciados: la información. Estos dispositivos pueden verse involucrados en situaciones como robos, incendios, inundaciones, fallos eléctricos, rotura o fallo del dispositivo, virus, borrados accidentales, etc. En estos casos nos sería imposible acceder a nuestra información, llegando a ponerse en peligro la continuidad de nuestro negocio.

La empresa debe realizar un inventario de activos de información y una clasificación de los mismos en base a su criticidad para el negocio. El objetivo de esta clasificación es tener un registro de todo el software y los datos imprescindibles para la empresa de manera que sirva para determinar la periodicidad de los backups y su contenido.

La empresa identificará a los responsables de realizar los backups y de definir el procedimiento para hacer las copias de seguridad y restaurarlas que incluirá:

- de qué hacer copia,
- el tipo de copia,
- el programa necesario,
- los soportes,
- la periodicidad,
- la vigencia,
- su ubicación,
- y las pruebas de restauración.

Así mismo se llevará un control de los soportes utilizados, se vigilará que sólo tiene acceso personal autorizado y que se destruyen los soportes de forma segura, en caso de tener que desecharlos. Los mismos criterios de seguridad serán aplicables en caso de hacer copias en la nube o en proveedores externos.

El objetivo es verificar que se realizan copias de seguridad que garantizan la continuidad de negocio.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.16.A]	INVENTARIO DE ACTIVOS DE LA INFORMACIÓN
Se mantendrá un inventario actualizado de activos de información (software, datos, soportes, responsables, ubicación, etc.) y serán clasificados para identificar los necesarios (críticos) para reanudar el negocio en caso de desastre o incidente grave.	
	El empresario, junto con los técnicos, deben identificar toda la información necesaria para reanudar el negocio en caso de desastre o de incidente grave. Se incluirá el software necesario y los datos críticos, los dispositivos que lo albergan, los responsables, la ubicación, etc.

[SEG.16.B]	CONTROL DE ACCESO
Se controlará el acceso a las copias de seguridad (solo personal autorizado).	
	Las copias de seguridad han de estar sometidas a un control de acceso restringido al personal autorizado.

[SEG.16.C]	COPIAS DE SEGURIDAD DE LA INFORMACIÓN CRÍTICA
Se realizarán copias de seguridad de la información crítica corporativa, la exigida por la ley y la establecida en los contratos.	
	Tendremos que verificar que hacemos copia de seguridad de la información crítica corporativa, de la exigida por la ley (por ejemplo, por la LOPD/GDD o RGPD) y de la establecida en los contratos con terceros.

[SEG.16.D]	PERIODICIDAD DE LAS COPIAS DE SEGURIDAD
Se realizarán copias de seguridad como mínimo semanalmente, aunque se sugiere hacerlas diariamente.	
	Fijaremos con cuanta frecuencia hacer las copias de seguridad teniendo en cuenta: • *la variación de los datos generados;* • *el coste de almacenamiento;* • *y las obligaciones legales, por ejemplo, la Ley de Protección de Datos obliga a cualquier empresa que trate datos de carácter personal, a establecer procedimientos de actuación para la realización de copias de respaldo.*

[SEG.16.E]	TIPO DE COPIA APROPIADAD
Las copias de seguridad semanales deberán ser completas y las diarias serán incrementales o diferenciales.	
	Decidiremos qué tipo de copia de seguridad es la idónea estimando los recursos y tiempo necesarios para llevarlas a cabo: • *completa: se copian todos los datos a un soporte;* • *incremental: sólo se graban los datos que han cambiado desde la última copia;* • *diferencial: se copian los datos que han cambiado desde la última copia completa.*

[SEG.16.F]	CADUCIDAD DE LAS COPIAS DE SEGURIDAD
Se conservarán las copias de seguridad de 6 meses	
	También debemos decidir cuánto tiempo conservar las copias en función de: • *si la información almacenada sigue vigente;* • *la duración del soporte en el que realizan las copias;* • *la necesidad de conservar varias copias anteriores a la última realizada.*

[SEG.16.G]	UBICACIÓN DE LAS COPIAS DE SEGURIDAD
Se deberá disponer de al menos una copia completa fuera de las instalaciones de la organización. Se guardarán las copias de seguridad en una caja ignífuga y bajo llave.	
	Es necesario buscar un lugar adecuado para guardar las copias, con los siguientes criterios: • *cuenta con al menos una copia fuera de la organización;* • *no guardes backups con datos de carácter personal (datos de clientes o de empleados, por ejemplo) en casa;* • *valora contratar servicios de guarda y custodia según los datos que contienen*

[SEG.16.H]	COPIAS EN LA NUBE
Si se realizan copias de seguridad en la nube, se deberán tomar las medidas de seguridad necesarias (firmar acuerdo de encargo del tratamiento con el proveedor, cifrar las copias, comprobar la confidencialidad de los canales de transmisión).	
	Si decides realizar tu copia en la nube toma las siguientes precauciones para garantizar la seguridad de la información: • *cifra la información confidencial antes de realizar la copia;* • *firma Acuerdos de Nivel de Servicios (ANS) con el proveedor, que garanticen la disponibilidad, integridad, confidencialidad y control de acceso a las copias;* • *considera el ancho de banda que necesitas para subir y bajar las copias.*

[SEG.16.I]	PROCEDENCIA DE COPIA Y RESTAURACIÓN
Se elabora y aplica procedimientos de copia y restauración, revisándolos anualmente y con cada cambio importante en los activos de información.	
	Se han de elaborar y aplicar procedimientos que describan cómo hacer las copias y cómo restaurarlas. De esta forma se minimiza el tiempo necesario de recuperación de los datos en caso de necesitar una restauración. Se han de revisar anualmente y con cada cambio importante del inventario de activos de información.

[SEG.16.J]	COMPROBACIÓN QUE LAS COPIAS ESTÁN BIEN REALIZADAS
Trimestralmente debe comprobarse la fiabilidad de las copias verificando que pueden restaurarse.	
	Fijaremos una periodicidad para realizar pruebas de restauración para garantizar que la información necesaria para la continuidad de negocio puede ser recuperada en caso de desastre.

[SEG.16.K]	SOPORTE DE LAS COPIAS DE SEGURIDAD
Deben estar etiquetados y llevar un registro de los soportes sobre los que se ha realizado alguna copia.	
	Decidiremos dónde hacer las copias teniendo en cuenta los siguientes aspectos: • *coste, fiabilidad, tasa de transferencia y capacidad de los distintos soportes: discos duros externos, USB, cintas, DVD y la nube;* • *utiliza soportes que no estén obsoletos o en mal estado.*

[SEG.16.L]	CONTROL DE LOS SOPORTES DE COPIA
Se llevará un registro con los diferentes soportes que se utilizan para realizar copias de seguridad	
	Tendremos que etiquetar e identificar los soportes dónde se realizan las copias de seguridad de manera que se pueda llevar un registro de los soportes sobre los que se ha realizado alguna copia. Así en el caso de tener que recuperar una información concreta, agilizaremos el proceso al poder consultar fácilmente en qué soporte se ha almacenado.

[SEG.16.M]	DESTRUCCIÓN DE SOPORTES DE COPIA
Cuando se desechen los soportes utilizados para copias de seguridad, deben destruirse de forma segura.	
	Cuando se desechan los soportes utilizados para copias de seguridad debemos destruirlos de forma segura. Es muy importante asegurar que esta información nunca volverá a ser accesible para evitar posibles accesos malintencionados.

[SEG.16.N]	CIFRADO DE LAS COPIAS DE SEGURIDAD
Se debe cifrar las copias de seguridad que contengan información confidencial o sensible y la que se sube a la nube.	
	Cifraremos la información confidencial y la que requiera de almacenamiento en la nube. De esta manera protegemos los datos en caso de robo de información o accesos no autorizados.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
CLASIFICACIÓN DE LA INFORMACIÓN (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

No cabe ninguna duda de que la información es uno de los activos más importante de cualquier entidad u organización, por lo que se debe proteger adecuadamente.

Debemos tener en cuenta que la información podemos disponerla en diferentes tipos de soportes:

1. **Formato digital** (Texto, imagen, multimedia, bases de datos, etc.)
2. **Otros tipos de formatos** (Archivadores, papel, película fotográfica, radiografías, etc.)

Y no debemos olvidar que la información contenida en formato digital panas por programas y aplicativos que los utilizan y procesa, hasta los equipos y sistemas que soportan estos servicios.

Con el objetivo de aplicar las medidas de seguridad más adecuadas y ajustadas a cada activo de información, se debe realizar un inventario y clasificar la información, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidenciliadad, integridad y disponibilidad. De esta forma, podremos determinar qué información debemos crifrar, quién puede utilizarla, quién es responsable de su seguridad, cada cuanto hacer un backup, etc.

Además, al clasificar los activos de información se debe establecder su ciclo de vida, que dependerá no sólo de la vida útil del soporte sino también de la vigencia de su contenido. Si el soporte caduca antes que el contenido tendremos que regenerarlo en otro soporte. El ciclo de vida de la información determinará el momento en el cual dejará de ser útil, y por tanto cúando tenemos que eliminarla convenientemente.

A continuación se detallan una serie de instrucciones con el objetivo de clasificar los activos de la información para garantizar una eficaz gestión de su seguridad con criterios de confidenciliadad, disponibilidad e integridad.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.17.A]	INVENTARIO DE LA INFORMACIÓN
Se debe elaborar un inventario de los activos de información que utilizamos	
	Es necesario establecer un inventario de los activos de información disponible en la empresa, considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes son sus reponsables, etc.

[SEG.17.B]	CRITERIOS DE CLASIFICACIÓN DE LA INFORMACIÓN
Debermos determinar claramente los criterios de seguridad con los que clasificarás los activos de información que utilizamos	
	Debemos establecer claramente los criterios de clasificación que vamos a aplicar a los activos de información. Estos deberán estar relacionados con las medidas de seguridad que plantearemos aplicar a nuestra información. Algunos de estos criterios podrían ser: ***Por el nivel de accesibilidad o confidencialidad:*** • *Confidencial. Accesible solo por la dirección o personal concreto* • *Interna. Accesible solo al personal de la empresa* • *Pública. Accesible públicamente* ***Por su utilidad o funcionalidad:*** • *información de clientes y proveedores* • *información de compras y ventas* • *información de personal y gestión interna* • *información sobre pedidos y procesos de almacén* ***Por el impacto por robo, borrado o pérdida:*** • *daño de imagen* • *consecuencias legales* • *consecuencias económicas* • *paralización de la actividad* *Asignaremos a cada tipo de información una etiqueta según los criterios de clasificación establecidos.*

[SEG.17.C]	CLASIFICACIÓN DE LA INFORMACIÓN
Se deben etiquetar los activos de información según los criterios de seguridad establecidos	
	Asignaremos a cada tipo de información una etiqueta según los criterios de clasificación establecidos

[SEG.17.D]	TRATAMIENTOS DE SEGURIDAD DISPONIBLES
Se deben establecer una lista con todos los tratamientos de seguridad de la información disponibles	
	Elaboraremos un listado con todos los tratamientos de seguridad de los que dispone la empresa, tales como herramientas de cifrado, sistemas de copias de seguridad, sistemas de control de accesos, etc.

[SEG.17.E]	ESTABLECER Y APLICAR LOS TRATAMIENTOS QUE CORRESPONDEN A CADA TIPO DE INFORMACIÓN
Se deben aplicar correctamente los tratamientos de seguridad que corresponden a cada activo de información	
	Una vez clasificada la información, debemos asignar y aplicar los tratamientos de seguridad oportunos para cada tipo de información. Entre estos tratamientos, podríamos contemplar los siguientes: • Limitar el acceso a las personas o grupos correspondientes • Cifrar la información • Realizar copias de seguridad • Medidas específicas como las reflejadas en el reglamento del RGPD • Información sujeta a acuerdos de confidencialidad concretos • Control del acceso y/o modificación de la información

[SEG.17.F]	AUDITORÍAS
Se deben realizar acitorías de comprobación al menos anualmente, aunque lo recomendable es semestralmente.	
	Conviene realizar periódicamente auditorías de seguridad que certifiquen que se aplican los tratamientos estipulados para proteger nuestra información.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
GESTIÓN DE RECURSOS HUMANOS (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

No cabe la menor duda de que «el eslabón más importante de la seguridad es el empleado», pues centrarse en evitar el error humano nos lleva a la clave para proteger nuestros sistemas y nuestra información. Por ello es necesario, no solo una oportuna concienciación y formación del personal, sino tomar medidas de seguridad en la gestión de los llamados «recursos humanos».

La mejor manera de garantizar de contar con una plantilla responsable en materia de ciberseguridad es establecer los oportunos **filtros, pruebas y controles** en la relación con nuestros colaboradores y empleados, especialmente en las **fases de firma** y **finalización del contrato**. En ambas fases se tendrán en cuenta aspectos tales como:

- Requisitos y acuerdos relativos a la seguridad que deben conocer, aceptar y cumplir;
- Políticas internas que deben aplicar: uso del correo corporativo, clasificación de la información, aplicaciones permitidas, uso del puesto de trabajo, etc.;
- Formación que les vamos a proporcionar;
- Cuáles son los procesos para darles de alta/baja en nuestros sistemas, etc.

Esta política tiene el objetivo de asegurar que todo el personal tiene conocimiento sobre los **derechos, deberes y responsabilidades** en relación a la seguridad de la información, haciendo hincapié en las posibles **sanciones** ante un acto negligente que ponga en riesgo los activos de información de la organización.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.18.A]	CLÁUSULAS CONTRACTUALES
Se deben reflejar en los contratos laborales de los empleados los aspectos más importante en materia de ciberseguridad	
	El empresario, con el departamento de recursos humanos, establecerán qué aspectos relevantes en relación a la seguridad de la información deben ser reflejados en el contrato de trabajo. Se considerarán todas las responsabilidades y derechos legales en lo relacionado con la propiedad intelectual o con datos de carácter personal.

[SEG.18.B]	ACUERDOS DE CONFIDENCIALIDAD
Se debe concretar en los acuerdos de confidencialidad o en sus anexos, la manera de gestionar el acceso a la información más sensible	
	Los empleados y colaboradores firmarán acuerdos relativos a la confidencialidad de la información de la empresa, que contendrán la siguiente información: • *partes intervinientes;* • *qué información tendrá carácter confidencial;* • *compromisos por ambas partes;* • *posibles sanciones y legislación aplicable.*

[SEG.18.C]	REVISIÓN DE LAS REFERENCIAS DE LOS CANDIDATOS
Se deben revisar las referencias de los candidatos antes de su contratación en aqullos puestos que requieran acceso a información muy confidencial, sensible o crítica.	
	En ciertas ocasiones (sobre todo para puestos de especial criticidad o con acceso a información muy confidencial, sensible o crítica) detallaremos las comprobaciones a realizar antes de incorporar a algún candidato a la plantilla. Será necesario determinar las referencias que han de ser revisadas y qué datos del currículum tienen que verificarse. Además, indicaremos qué puestos concretos necesitarán una acreditación especial de estar libre de antecedentes penales.

[SEG.18.D]	PLAN DE FORMACIÓN Y CONCIENCIACIÓN EN PROTECCIÓN DE DATOS Y CIBERSEGURIDAD
Se debe mantener concienciada, formada y reciclada a la plantilla en aspectos relacionados con la protección de datos y la ciberseguridad	
	Estableceremos las actividades oportunas para mantener a la plantilla concienciada y formada en todo momento en aspectos relativos a la seguridad de la información.

[SEG.18.E]	POLÍTICA DE SANCIONES Y EXPEDIENTES
Se debe informar al empleado de las sanciones que conlleva el uso negligente de la información en la empresa	
	Elaboraremos un procedimiento disciplinario formal que recoja las sanciones a aplicar en aquellos casos en los que se haya producido una negligencia en relación con la seguridad de la información (fuga o pérdida de datos confidenciales o sensibles, actuaciones intencionadas, ataques a la reputación en redes sociales, permitir ataques de terceros como infecciones por malware, etc.). Este procedimiento debe ser notificado a los empleados y estar accesible en todo momento.

[SEG.18.F]	FINALIZACIÓN DEL CONTRATO
Se debe comunicar a los empleados las obligaciones que deben cumplir con la información de la empresa al finalizar su contrato	
	Para evitar fugas de información es importante comunicar a los empleados las responsabilidades y obligaciones de seguridad y confidencialidad que deberán cumplir una vez finalizada la relación contractual.

[SEG.18.G]	CONCESION AUTORIZADA DE LOS PERMISOS DE ACCESO
Se deben conceder únicos y oportunos para garantizar que cada empleado solo accede a la información conveniente	
	Si queremos garantizar que cada empleado solo acceda a la información oportuna, deberemos darle de alta en los sistemas de acuerdo con las políticas de control de acceso (físico y lógico) correspondientes. En este punto, entre otras, realizaremos las siguientes acciones: • *entregar las tarjetas de acceso físico;* • *asignar las cuentas de correo electrónico;* • *conceder los permisos de acceso a servicios, aplicativos y recursos compartidos;* • *asignar el puesto de trabajo, los dispositivos y equipos*

[SEG.18.H]	REVOCACIÓN DE PERMISOS DE ACCESO
Se debe eliminar los permisos y cuentas de usuario de los empleados que finalizan su contrato	
	Del mismo modo que en su incorporación damos los accesos y permisos oportunos a los nuevos empleados para que puedan realizar su trabajo, al finalizar la relación contractual los revocaremos: • *recogiendo las tarjetas de acceso y los dispositivos entregados;* • *eliminando sus cuentas de correo;* • *eliminando sus permisos de acceso a sistemas y aplicativos.*

[SEG.18.I]	ACEPTACIÓN DE LAS CLÁUSULAS Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
Todos los empleados deben leer, entender y firmar los acuerdos, cláusulas y políticas relacionadas con la seguridad de la información	
	Cada empleado de la empresa debe asegurarse de leer, comprender y firmar cada uno de los acuerdos, contratos, cláusulas y documentos de políticas relacionados con la seguridad de la información.

[SEG.18.J]	APROVECHAMIENTO DE LAS SESIONES FORMATIVAS Y DE CONCIENCIACIÓN
Todos los empleados deben participar de manera activa en las sesiones formativas de la empresa en materia de protección de datos y ciberseguridad.	
	Debemos aprovechar al máximo las posibles sesiones formativas y de concienciación que la empresa ponga a disposición de los empleados. De esta forma nos aseguraremos de comprender los riesgos a los que se enfrenta la empresa en materia de ciberseguridad.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
RELACIÓN CON PROVEEDORES (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Hoy en día casi todas las empresas necesitan contratar servicios especializados externos que den soporte a parte de su actividad. En estos casos de nada sirve asegurar al máximo los sistemas internos si no exigimos la misma seguridad a los **proveedores externos** que puedan gestionar parte de la información (sobre todo si es información sensible como la contemplada en el RGPD). Entre estos proveedores podemos destacar los siguientes grupos:

- **Proveedores de servicios tecnológicos.** Aquellos que ofrecen servicios como alojamiento web, emisión de certificados, servicio de pasarelas de pago, servicios de almacenamiento en la nube, servicios de soporte informático (tanto presencial como remoto), etc.
- **Proveedores de servicios no tecnológicos pero que acceden a datos corporativos.** Tales como proveedores de servicios financieros, viajes, transporte, publicidad y marketing, etc.
- **Suministradores de productos tecnológicos.** Incluyen todos aquellos dónde se adquieren los dispositivos, los componentes hardware y las aplicaciones informáticas.

La conectividad y complejidad de los sistemas de información actuales, hacen indispensable mantener el **control sobre la seguridad de la información** de la empresa, aun cuando esta esté siendo gestionada por terceros.

Esta política tiene como objetivo controlar que toda relación con proveedores, y en particular aquellos que tienen acceso a la información, está suficientemente protegida en base a los **acuerdos y contratos** correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio.. Nos aseguraremos también de que los productos y servicios contratados cumplen con los requisitos de seguridad establecidos por la empresa.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería
- Todas las ORGANIZACIONES PRESTADORAS DE SERVICIOS que intervengan en los sistemas de procesamientos de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN, que hayan asumido alguna de las responsabilidades que se detallan a continuación y con independencia de que dichos procesos se realicen dentro de las instalaciones de COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN o en las instalaciones del prestador de servicios:
    - Encargado del tratamiento; Servicios sin Tratamiento de Datos

[SEG.19.A]	REQUISITOS DE SEGURIDAD EN PRODUCTOS Y SERVICIOS
Se deben establecer los requisitos de seguridad mínimos que deben cumplir los productos que se adquieren y los servicios que se contratan	
	Se deben definir los requisitos en Ciberseguridad que deben cumplir los productos o servicios que se adquieran de proveedores. Estos requisitos serán coherentes con las políticas de seguridad de la información de la organización y se extenderan a proveedores, suministradores, colaboradores, partners, canales de ventas y distribución, etc.

[SEG.19.B]	DEFINIR LAS CLÁUSULAS CONTRACTUALES EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN
Se debe ser riguroso en la elaboración y aceptación de las cláusulas contractuales en materia de ciberseguridad	

	Con el fin de establecer contratos y acuerdos rigurosos en materia de ciberseguridad, se deben detallar las cuestiones más relevantes a contemplar en los contratos con proveedores. Todos estos aspectos se pueden reflejar en contratos y acuerdos de confidencialidad y de acceso a datos:
	• *Determinar qué información es accedida, cómo puede ser accedida y la clasificación y protección de la misma;*
	• *Asegurar de que una vez finalizado el contrato, el proveedor ya no podrá acceder o mantener la información sensible de la organización;*
	• *Reflejar los requisitos legales oportunos:*
	  ◦ *cumplimiento del RGPD,*
	  ◦ *cumplimiento de la LSSI,*
	  ◦ *cumplimento de los derechos de propiedad intelectual.*
	• *Reflejar el derecho de auditoría y de control sobre aspectos relevantes del acuerdo;*
	• *Incluir las situaciones que conlleven la finalización del contrato;*
	• *Definir las garantías específicas:*
	  ◦ *penalizaciones económicas en caso de incumplimiento,*
	  ◦ *perjuicios económicos por inactividad,*
	  ◦ *certificaciones y garantías adicionales.*

[SEG.19.C]	DEFINIR LAS RESPONSABILIDADES CONCRETAS POR AMBAS PARTES
Se deben delimitar las reponsabilidades en materia de ciberseguridad de cada una de las partes involucradas	
	Se debe establecer por contrato, y con posibles penalizaciones, si es el proveedor o la organización son los responsables de cada aspecto relativo a la seguridad: • *controlar quién accede o transforma la información sensible y por qué;* • *realizar el backup y cuando;* • *controla los logs, etc.;* • *activar, mantener y controlar los sistemas de seguridad: antimalware, firewall, cifrado de comunicaciones, etc*

[SEG.19.D]	DEFINIR LOS ANS (ACUERDOS DE NIVEL DE SERVICIOS)
Se deben definir en detalle los ANS a los que se someten los servicios contratados	

	Con el fin de establecer las características de calidad y las garantías del servicio adquirido, se deben definir y firmar los ANS (o SLA en inglés) correspondientes con los proveedores. Los aspectos más relevantes para definir un ANS son:
	• *responsabilidades de cada una de las partes;*
	• *duración del acuerdo;*
	• *detalle del nivel de servicio ofrecido. Incluyendo:*
	  ◦ *tasas de error permitidas,*
	  ◦ *disponibilidad horaria,*
	  ◦ *tiempos de respuesta y resolución,*
	  ◦ *canales de contacto,*
	  ◦ *proceso de escalado y notificación ante incidentes,*
	  ◦ *procedimientos para la resolución de problemas e incidencias.,*
	  ◦ *personal asignado al servicio.*
	• *procedimientos para el seguimiento y control del servicio;*
	• *sanciones en caso de incumplimiento;*
	• *medición de la satisfacción por el servicio recibido.*

[SEG.19.E]	CONTROLES DE SEGURIDAD OBLIGATORIOS
Se deben determinar los controles de seguridad que son de obligado cumplimiento en las relaciones con los proveedores de servicios tecnológicos	
	Para asegurar la contratación de un servicio externo seguro se deben identificar los controles de seguridad que se consideren de obligado cumplimiento. Estos controles deben tener en cuenta los siguientes aspectos: • *servicios y componentes informáticos a los que la organización permite el acceso;* • *qué información relevante de la organización puede ser accedida y con qué método de acceso;* • *como gestionar cualquier incidencia relacionada con el acceso de los proveedores a nuestros sistemas;* • *revisión del cumplimiento de los ANS acordados.*

[SEG.19.F]	FORMAR PARTE DE LOS FOROS Y ORGANIZACIONES DE USUARIOS DE LOS PRODUCTOS/SERVICIOS SOFTWARE UTILIZADOS
Estar al corriente y participar en las organizaciones de usuarios de los productos y servicios software que se contraten, a fin de controlar la reputación de los proveedores	
	Puede resultar de gran interés participar en foros y asociaciones sobre productos adquiridos. De esta manera se tendrá la posibilidad de consultar las principales funcionalidades, novedades y vulnerabilidades acerca de los mismos. Además, se podrá revisar la reputación de los proveedores así como las certificaciones y sellos de calidad que poseen.

[SEG.19.G]	CERTIFICACIÓN DE LOS SERVICIOS CONTRATADOS
Se debe exigir a los proveedores certificaciones que garanticen la calidad en materia de seguridad de ciertos servicios contratados de especial criticidad	
	En servicios especialmente críticos se pueden exigir a las empresas la garantía de que posean algunas de las certificaciones referentes a la calidad en la gestión de la seguridad de la información. Entre estas, cabría destacar las siguientes: • *certificación ISO 27001 de Sistemas de gestión de la seguridad de la información;* • *certificación ISO 22301 de Gestión de continuidad de negocio.*

[SEG.19.H]	AUDITORÍA Y CONTROL DE LOS SERVICIOS CONTRATADOS
Se debe supervisar que los productos y servicios contratados responden a lo acordado en materia de ciberseguridad	
	Para asegurar en todo momento la calidad del servicio contratado se debe establecer la manera de monitorizar, revisar y auditar el servicio de los proveedores en aspectos relacionados con la ciberseguridad. Se necesitará establecer la manera de gestionar cualquier problema surgido con productos o servicios de los proveedores. Se deben extender estas prácticas a toda la cadena de suministro

[SEG.19.I]	FINALIZACIÓN DE LA RELACIÓN CONTRACTUAL
Se garantiza la seguridad de la información tras la finalización del servicio o contrato	
	Es importante garantizar la seguridad de la información tras la finalización de los servicios contratados. Para ello se deben formalizar las acciones a llevar a cabo una vez finalizado el servicio: • *señalar los activos que han de ser devueltos;* • *eliminación de permisos de acceso;* • *borrado de información sensible de la organización almacenada en los sistemas del proveedor.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
AUDITORÍA DE SISTEMAS (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Ante el incesante aumento de los **ataques** de ciberseguridad, la empresa debe determinar su **nivel de seguridad** actual y establecer el nivel que ha de conseguir para proteger los sistemas y la información corporativos. Por este motivo es necesario realizar auditorías que permitan la **evaluación y análisis** de la seguridad de los sistemas. Dichas auditorias se realizarán normalmente por personal externo especializado, y ayudarán a mejorar la seguridad, eficacia y eficiencia de nuestros procesos.

Por otro lado, en ciertos casos es necesario solicitar auditorías especializadas, como por ejemplo auditorias de revisión de **cumplimientos legales** (auditoría RGPD y LSSI-CE), o auditorías **forenses** para investigar lo ocurrido tras un incidente grave (brecha de datos, botnet, ransomware, DDoS, etc.).

El objetivo de esta política es obtener **evidencias** de que cómo los sistemas de información de la entidad cumplen con los **requisitos de seguridad** deseados. Utilizar estas evidencias para llevar a cabo un proceso de mejora continua de la ciberseguridad.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.20.A]	DETALLAR LOS ELEMENTOS CLAVE QUE QUEREMOS QUE SEAN AUDITADOS
Se deben tener identificados todos los activos más relevantes que deben ser auditados	
	Para llevar a cabo con éxito el proceso de auditoría, es necesario identificar los activos de información más importantes (críticos) de la empresa cuya seguridad se quiere que sean revisada. Estos activos pueden ser desde ficheros, bases de datos, páginas web, equipos o programas hasta servicios completos. Para estos activos se revisarán los aspectos de ciberseguridad, entre otros: • *sistemas antimalware* • *procesos de gestión de permisos* • *procesos para el cumplimiento legal* • *políticas de prevención de fraude y de fuga de datos* • *sistema de actualizaciones* • *sistemas de monitorización de recursos*

[SEG.20.B]	MEJORA CONTINUA Y MODELOS DE MADUREZ
Se debe enfocar el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez	
	Para garantizar que los resultados de las auditorías conllevan la implantación de mejoras permanentes en ciberseguridad, es necesario enfocar el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez.

[SEG.20.C]	AUDITORÍAS LEGALES
Se deben realizar auditorías específicas para verificar el cumplimiento de los requerimientos legales del RGPD, LSSICE y demás normativas de seguridad	
	Para garantizar el cumplimiento de ciertos requisitos legales puede ser conveniente u obligatorio, realizar auditorías específicas, por ejemplo, el cumplimiento por parte la empresa del RGPD, LSSICE, LOCM, etc.

[SEG.20.D]	AUDITORIAS FORENSES
Se deben realizar auditorías forenses para determinar lo ocurrido tras un incidente de seguridad	
	Para identificar las causas que han producido un incidente y recabar evidencias para su análisis posterior, para depurar responsabilidades o para iniciar una denuncia.

[SEG.20.E]	PROCEDIMIENTOS
Se deben definir/revisar los procedimientos detalladas para auditar la seguridad de cada activo clave de los sistemas de información.	
	Se seleccionará el tipo de auditoría más conveniente: • *test de penetración* • *auditoría de red* • *auditoría de seguridad perimetral* • *auditoría web* • *auditoría forense* • *auditoría legal* *Se definirá con detalle los procedimientos y logs necesarios para realizar cada tipo de auditoría. Asimismo, se concretará cómo registrar los resultados de estas revisiones.*

[SEG.20.F]	REALIZACIÓN DE AUDITORÍAS PERIÓDICAS
Se deben realizar auditorías periódicas de los sistemas de información	
	Se deben realizar auditorías periódicas independientes con la finalidad de revisar y evaluar todos los aspectos relacionados con la seguridad de la información de la empresa. Se debe fijar esta periodicidad al menos con carácter anual. Se debe evaluar si hay que repetir estas auditorías tras la implantación de algún cambio significativo en los sistemas.

[SEG.20.G]	ANÁLISIS DEL RESULTADO DE LA AUDITORÍA
Se deben analizar los resultados de la auditoría en busca de debilidades a corregir	
	Se analizan los resultados de la auditoría en busca de errores o debilidades. Se llevan a cabo acciones para corregir las vulnerabilidades detectadas: • *identificación de las causas y motivos del resultado desfavorable* • *evaluación de las medidas correctoras* • *implantación y revisión de dichas medidas*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

COMERCIO ELECTRÓNICO (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

El comercio electrónico ha cambiado los hábitos de compra de la población. Su aceptación y continuo crecimiento entre comerciantes se debe a los beneficios asociados: mayor alcance de público objetivo, oportunidad de crecimiento, no requiere una gran inversión, flexibilidad en los medios de pago, etc.

Para conseguir que los clientes confíen en la tienda online se deben contemplar los siguientes aspectos de seguridad:

- Seguir una política de web segura.
- Contemplar los aspectos legales mostrando el aviso legal, la política de cookies y las condiciones de contratación.
- Si utilizas un Marketplace (eBay, Amazon, Vibbo, etc.) hay que tener en cuenta sus particularidades legales y de seguridad.
- Utilizar una pasarela de pago segura que ofrezca canales cifrados para las transacciones (https) o bien verificar que las pasarelas de pago contratadas cumplen con el estándar de seguridad PCI-DSS que garantiza que los titulares de tarjetas pueden realizar compras seguras y que la información de sus tarjetas está protegida ante posibles fraudes online.
- Avalar la seguridad mostrando sellos de confianza preferiblemente aquellos que auditen la web periódicamente.
- Disponer de copias de seguridad que permitan restaurar el sitio web en caso de sufrir un ataque.
- Vigilar las transacciones para evitar el fraude.

Esta política tiene como objetivo verificar que se aplican las medidas necesarias para garantizar la seguridad de los clientes, y evitar el fraude en las compras online.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.21.A]	CUMPLIMIENTO DE POLÍTICAS RELACIONADAS
Se debe cumplir con lo establecido en la Política de Seguridad Web y la Política de relación con proveedores si aplicara	
	*La tienda online es una página web y como tal está sujeta a la **Política de seguridad web**. Por otra parte si se contrata el servicio de alojamiento, el desarrollo o su mantenimiento se tendrá en cuenta la **Política de Relación con proveedores**.*

[SEG.21.B]	CERTIFICADO WEB CON VALIDACIÓN EXTENDIDA
Se debe adquirir un certificado web para la tienda online que asegure las transacciones de los clientes, preferiblemente con validación extendida	
	La tienda online debe contar con un certificado web preferiblemente con validación extendida. Los certificados web proporcionan garantías en la identificación de la web (candado) y en el cifrado (https://) de las comunicaciones entre el cliente web y el servidor: Estas garantías están avaladas por una Autoridad de Certificación. En el caso de los de validación extendida la verificación de la seguridad de la tienda online es más exhaustiva ofreciendo por tanto mayores garantías y mayor confianza a los clientes en sus compras.

[SEG.21.C]	SELLOS DE CONFIANZA PARA EL COMERCIO ELECTRÓNICO
Se recomienda obtener sellos de confianza para garantizar la seguridad y la calidad de la tienda online	
	Para cumplir las expectativas de seguridad del cliente, la web debería contar con sellos de confianza. Estos distintivos son proporcionados por empresas privadas, entidades públicas y organizaciones sin ánimo de lucro. Algunas de estas organizaciones realizan auditorías para comprobar si la web cumple los requisitos para obtener el sello de confianza y otras ofrecen mecanismos para adherirse a códigos de buenas prácticas. Para las tiendas online se recomiendan aquellos que realizan auditorías de seguridad.

[SEG.21.D]	MEDIDAS DE CARÁCTER LEGAL
Hay que asegurarse de que la web o tienda online cumple con todas las medidas legales (Aviso Legal, Condiciones de Contratación, Cookies, ...)	
	Las tiendas de comercio electrónico deben cumplir las cuestiones legales recogidas en: • *LSSI-CE (Ley de Servicios de la Sociedad de Información y Comercio Electrónico).* • *El Reglamento europeo de protección de Datos (RGPD).* • *Ley de Cookies.* • *Ley de Ordenación del Comercio Minorista*

[SEG.21.E]	PREVENCION DE COMPRAS FRAUDULENTAS
Es muy recomendable elaborar listas blancas y negras de los clientes y contratar servicios de empresas IPSP (Servicios de pago por Internet)	
	Para evitar posibles compras fraudulentas se recomienda: • ***La creación de listas blancas y listas negras.** Las blancas contendrán los clientes fiables, mientras que las negras los clientes con los que se ha tenido problemas, especificando cuál es el motivo del mismo.* • ***Contratar los servicios de empresas especializadas en pagos online denominadas IPSP** (Internet Payment Service Providers). Este tipo de empresas (PayPal, Google Wallet, Amazon Payments, etc.) sirven como intermediario entre el cliente y la entidad bancaria de la tienda virtual. Proporcionan herramientas antifraude, pasarelas de pago seguras y un panel de administración para realizar el seguimiento de todas las operaciones.*

[SEG.21.F]	PAGO VIRTUAL CON TARJETAS DE CRÉDITO
Se debe cumplir, o revisar el cumplimiento de las pasarelas de pago que se contraten, con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS)	
	El método de pago virtual con tarjetas de crédito debe de cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI DSS. Se trata de un conjunto de requerimientos y procesos para ayudar a garantizar que los titulares de tarjetas pueden realizar compras seguras y que la información de sus tarjetas está protegida ante posibles fraudes online. En cualquier caso se recomienda elegir pasarelas de pago que no nos obliguen a guardar ningún dato de las tarjetas o cuentas de los clientes.

[SEG.21.G]	CONTROL DE ACCESO
Se debe aplicar la Política de Control de Acceso y la Política de Contraseñas para acceder al gestor de contenidos	
	Se debe seguir la Política de control de accesos y la Política de contraseñas para el acceso al panel de administrador del gestor de contenido y del servicio de alojamiento de la tienda online. Si es posible se utilizara doble factor de autenticación. Se debe ejercer cuidado de acceder siempre desde un ordenador cuya seguridad esté controlada y verificar que la conexión es cifrada (https://)

[SEG.21.H]	DETECCIÓN DE COMPRA FRAUDULENTA
Se deben comprobar los intentos de compra, los datos del comprador y las opciones de envío	
	Existen diferentes indicadores para detectar una posible compra fraudulenta a los que hay que prestar una especial atención: • *Comprobar que no se han producido varios intentos de compra erróneos en el TPV antes de que la operación sea aceptada.* • *Verificar que la dirección de email existe y los datos del cliente son coherentes.* • *Sospechar cuando se elige la opción de envío urgente del pedido cuando esta encarece considerablemente el producto.* *Comprobar que no existen distintos clientes con la misma dirección de destino. Puede tratarse de un mismo receptor intermediario que después entregará las compras fraudulentas a sus destinatarios*

[SEG.21.I]	PREVENCIÓN DEL FRAUDE: COMPROBACIONES A REALIZAR PARA ACEPTAR NUEVOS CLIENTES
Se debe comprobar si los datos del cliente están incluídos en alguna lista negra, si la cuantía del pedido es muy elevada, si la dirección de destino es nacional o internacional, si el método de pago mantiene registros de fraude y si, éste se realiza con tarjeta, comprobar si la dirección de destino del pedido coincide con los datos de localización del cliente	
	Para garantizar la fiabilidad de la compra de un cliente nuevo se debe comprobar: • *Si los datos del cliente están incluidos en alguna lista negra corporativa.* • *Si la cuantía del pedido realizado es muy elevada.* • *Si la dirección destino del pedido es nacional o internacional.* • *Si el método de pago seleccionado mantiene registros de fraude, comprobar si existen datos del cliente para verificar su reputación.* • *Si el método de pago seleccionado es tarjeta, comprobar que la dirección destino del pedido coincide con los datos de localización del cliente (ubicación del registro de la tarjeta, localización de la IP desde la que se realiza el pedido, configuración regional del dispositivo desde el que se realiza el pedido,...).* • *Si algún dato del pedido nos resulta extraño, llamar al cliente para realizar la comprobación de una manera más directa e inmediata.*

[SEG.21.J]	PREVENCIÓN DEL FRAUDE: COMPROBACIONES A REALIZAR PARA CLIENTES REGISTRADOS
Se debe comprobar si los datos del cliente están en la lista blanca, si en el historial aparece algún problema en el pago, si el método de pago es el habitual y si los datos bancarios y la dirección de destino coinciden con los de los pedidos anteriores	
	Cuando el cliente está registrado por compras anteriores se debe comprobar: • *Si los datos del cliente están incluidos en la lista blanca corporativa.* • *Si en el historial de pedidos aparece algún problema previo en el pago.* • *Si el método de pago seleccionado es el habitual.* • *Si los datos bancarios del pedido coinciden con los de los pedidos anteriores.* • *Si la dirección destino del pedido concuerda con la de los pedidos anteriores*

[SEG.21.K]	ACTUACIÓN ANTE LA DETECCIÓN DE COMPRA FRAUDULENTA
No se enviará la mercancía, se contactará con el banco para comprobar la transacción se contactará con el cliente para que verifique sus datos, no se usará el dinero proviniente de la compra, y se acudirá a las FCSE (Fuerzas y Cuerpos de Seguridad del Estado) para interponer una denuncia	
	Cuando se sospecha ser víctima de una compra fraudulenta esta es la forma correcta de actuar: • *No enviar nunca la mercancía.* • *Contactar con el banco para comprobar que la transacción es correcta pidiendo una respuesta por escrito.* • *Contactar con el cliente para que verifique los datos. Pedir que envíe sus datos personales por correo electrónico.* • *Nunca usar el dinero proveniente de una posible compra fraudulenta ya que puede ser reclamado por la entidad emisora de la tarjeta.* • *Acudir a las Fuerzas y Cuerpos de Seguridad del Estado para interponer una denuncia.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
PROTECCIÓN DE LA PÁGINA WEB (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Tener presencia en internet mediante una página o portal web es una necesidad para la mayoría de empresas. Esto permite ofrecer servicios de manera global, una comunicación más estrecha con el cliente, ahorro de recursos, publicidad constante, posibilidad de venta *online*, etc.

Una página web es un servicio que ofrecemos desde un equipo conectado a internet, con un software específico (servidor web). Los contenidos de la web los administramos a través de un gestor de contenidos o CMS (Drupal, Joomla o Wordpress por ejemplo), donde está desarrollada la página. Todas las combinaciones son posibles: tener todo en nuestras instalaciones, hacernos una página básica con nuestros medios o con herramientas online (Wix, Weebly, Jimdo,..), contratar el servicio de alojamiento (servidor y CMS) a un proveedor y contratar el diseño de nuestra web.

A la hora de contratar o diseñar la web corporativa se debe tener en cuenta, y exigir a los proveedores en su caso, los siguientes aspectos de seguridad:

- garantías de seguridad, auditorías, sellos;
- utilizar metodologías de desarrollo seguro a la hora de construir la web, como por ejemplo la metodología OWASP;
- garantizar un acceso seguro al panel de control del sitio web;
- si se trata de una web de venta *online* tendremos que contratar medios de pago seguros;
- realizar copias de seguridad periódicas de todos los elementos que conforman el servicio web;
- mantener el gestor de contenidos (CMS) siempre actualizado;
- guardar registros de la actividad generada en el servidor;
- cumplir con la legislación marcada por el RGPD, LSSI, LOCM y la LPI;
- disponer de un certificado digital que garantice la seguridad del sitio web.

Con las medidas de seguridad anteriores se podrán evitar posibles ataques a la web o sus consecuencias, tales como:

- denegación de servicio;
- la modificación de los contenidos del portal web (*defacement*), como cambios no autorizados en los precios, descripción de productos, medios de pago, etc.;
- la sustracción de la base de datos de clientes de la web o de información confidencial;
- la manipulación del portal para realizar ataques de *phishing* o de almacenamiento y distribución de malware.

El objetivo de esta política es proteger la página web o tienda *online* de posibles ataques, cumplir con la legislación y garantizar a los usuarios de la web la protección de sus datos personales.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.22.A]	CERTIFICADO WEB
Se deben proteger los canales por los que se transmite información sensible (correo electrónico, página web, etc.) mediante el cifrado de las comunicaciones, adquiriendo un certificado web de confianza	
	Si existen usuarios que hacen login en la página o pueden interactuar con ella de alguna forma (formularios, comentarios,…), es necesario proteger los canales por los que se transmite información mediante el cifrado de las comunicaciones, adquiriendo un certificado web de confianza

[SEG.22.B]	INFORMACIÓN DEL USUARIO
Se deben aplicar las normas de seguridad exigidas por el RGPD para los datos personales de los clientes	

	Si la web recoge información del cliente, el RGPD obliga a tomar estas medidas de seguridad:
	• *no recabar más datos de los necesarios;*
	• *tomar las medidas de seguridad adecuadas a los datos (autenticación, control de accesos, control de incidencias, gestión de soportes, copias de seguridad,…);*
	• *solicitar el consentimiento explícito del usuario, en un lenguaje claro y conciso, para tratar sus datos personales;*
	• *contar con una política de cookies*
	• *garantizar, indicando cómo ejecutarlos en el Aviso Legal, los derechos:*
	  • *acceso, rectificación, cancelación y oposición;*
	  • *y otros derechos: limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas, incluida la elaboración de perfiles.*

[SEG.22.C]	DESARROLLO DE TERCEROS
Se deben tener en cuenta los criterios de seguridad en los desarrollos llevado a cabo por terceros	
	Si contratamos el desarrollo de la web a un tercero, al solicitar el desarrollo debemos incluir requisitos de seguridad como: autenticación y cifrado de credenciales, cumplimiento legal, copias de seguridad, privacidad por diseño y por defecto, y solicitar que se utilicen metodologías de desarrollo seguro

[SEG.22.D]	CUMPLIMIENTO LEGAL
Se debe cumplir con los aspectos legales contemplados en la legislación nacional (LSSI y LPI)	

	La página web debe cumplir, además de con el RGPD, con otra legislación vigente:
	• *si se utiliza con fines lucrativos, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), indicando con claridad:*
	  • *las condiciones de contratación o las condiciones de uso*
	  • *lo relativo a las comunicaciones comerciales*
	• *si se utilizan contenidos de terceros, la Ley de Propiedad Intelectual (LPI)*

[SEG.22.F]	ALOJAMIENTO EN SERVIDOR PROPIO
Se dispone de medidas de seguridad en los sistemas de alojamiento propio	
	Si se dispone de un servidor web para la página web en las instalaciones de la entidad, deberá comprobrarse que: • *se encuentran en la DMZ corporativa;* • *dispone de medidas de seguridad perimetrales: cortafuegos y sistemas de prevención y detección de intrusiones (IDS/IPS);* • *dispone de medidas de seguridad contra malware;* • *se han deshabilitado los servicios innecesarios (transferencia de ficheros, mantenimiento remoto,…);* • *el/los administradores utilizan dispositivos y canales seguros para administrar los servidores.*

[SEG.22.G]	ALOJAMIENTO EN SERVIDOR EXTERNO
Se debe asegurar que el alojamiento contratado al proveedor disponga de las medidas de seguridad adecuadas y pactadas	
	Si la web está alojada en un proveedor se revisará que el contrato: • *incluye cláusulas de confidencialidad;* • *estipula quién es el encargado del tratamiento de datos si fuera necesario;* • *incluye acuerdos de nivel de servicio con responsabilidades de seguridad (copias de respaldo, actualizaciones, auditorías,…);* • *establece la propiedad del código fuente.*

[SEG.22.H]	ADMINISTRACION POR TERCEROS
Se debe mantener un registro de la actividad de los administradores externos	
	Si la web la administra un tercero, debe existir un registro de la actividad de los administradores que se pueda consultar y obtener en caso de fraude o de incidentes de seguridad.

[SEG.22.I]	CONFIGURACIÓN DEL CMS
Se aplican medidas de seguridad al gestor de contenidos	
	Tanto si lo administra la propia entidad como si lo hace un proveedor para proteger el gestor de contenidos se deben aplicar y verificar las siguientes medidas de seguridad: • *deshabilitar los módulos que no se utilicen;* • *eliminar el directorio de instalación;* • *cambiar el nombre del usuario «admin» y el prefijo de la base de datos;* • *utilizar CAPTCHA en los formularios (evitar spam);* • *eliminar metadatos de los documentos e imágenes;* • *vigilar los cambios en los contenidos y los accesos al panel de control;*

[SEG.22.J]	ACCESO AL PANEL DE CONTROL
Se asegura que las claves de acceso al panel de control sean fuertes y cumplan los criterios de seguridad	
	Independientemente del gestor de contenidos utilizado, se debe asegurar que las claves de acceso al panel de control se generan cumpliendo los criterios de seguridad. Es recomendable: • *cambiar los nombres y las contraseñas de todos los usuarios por defecto y deshabilitarlos si no se van a utilizar;* • *proteger al administrador (contraseñas fuertes y cambios frecuentes de contraseña, doble factor de autenticación,…);* • *utilizar comunicaciones seguras para administradores y usuarios*

[SEG.22.K]	LIMITACIÓN DE ACCESOS
Los servidores web se han configurado con un límite de accesos concurrentes para evitar ataques de denegación de servicios	
	Los servidores web se deben configurar (tanto en las instalaciones propias de la entidad como en las del proveedor) con un límite de accesos concurrentes para evitar ataques de denegación de servicio.

[SEG.22.L]	USUARIOS POR DEFECTO
Se deben eliminar los usuarios por defecto de las herramientas y software que soporta la web	
	Se tendrá que eliminar o comprobar que se han eliminado los usuarios por defecto de las herramientas y software que soporta la web (servidores web, gestores de contenidos,…).

[SEG.22.M]	GUARDADO DE REGISTROS (logging)
Se debe guardar un registro de cualquier interacción con la página durante un periodo de tiempo conveniente	
	Para poder investigar cualquier incidente relacionado con la web o incluso poner los registros a disposición judicial (si se diera el caso), es necesario guardar un registro de cualquier interacción con la página. Si la gestión del servidor la lleva el técnico de la empresa será él quien guarde esos registros durante un período de tiempo conveniente. Si la gestión del servidor es externa, este aspecto deberá estar reflejado en el contrato con el proveedor, especificando el tipo de registros que se guardan, durante cuánto tiempo y la forma de acceso a dichos registros.

[SEG.22.N]	COMERCIO ELECTRÓNICO
Si la web dispone de comercio electrónico, se debe elaborar una normativa de seguridad que siga las pautas indicadas en la política de comercio electrónico	
	Si la web se utiliza para tener una tienda online se debe elaborar y cumplir una normativa específica de seguridad para prevenir el fraude y proteger a los clientes online con las pautas indicadas en la política de comercio electrónico

[SEG.22.Ñ]	SELLOS DE CONFIANZA
Es recomendable disponer de un sello de confianza que acredite la seguridad del sitio web	
	Si la web es una tienda online, es recomendable que este acreditada con un sello que garantice la seguridad del sitio. Los mejores sellos son los que auditan nuestra web periódicamente.

[SEG.22.O]	COPIAS DE SEGURIDAD
Se deben realizar copias de seguridad periódica de la web y de sus bases de datos	
	Se deben realizar copias periódicas de la web, incluida la BBDD, tanto si está alojada en un servidor propiedad de la empresa como si está en un servidor externo.

[SEG.22.P]	AUDITORÍAS
Se deben realizar auditorías externas para verificar la seguridad	
	También se realizará auditorías externas para verificar la seguridad de la web

[SEG.22.Q]	SOFTWARE ACTUALIZADO
Se debe actualizar periódicamente el gestor de contenidos, sus complementos y el software del servidor donde se aloja la web. Es recomendable estar suscrito a un servicio de avisos de seguridad del fabricante del CMS así como de cualquier otro software	
	La actualización del gestor de contenidos y sus complementos, además de la actualización del software del servidor deben ser algunas de las tareas periódicas o puntuales a realizar tanto si la gestión de la página web se desarrolla en la empresa como si la realiza un tercero. Por otra parte se considera conveniente estar suscrito a los servicios de avisos o alertas de seguridad del propio fabricante del gestor de contenidos, así como de cualquier otro software que utilicemos que nos indicará de la existencia de actualizaciones puntuales.

[SEG.22.R]	PROTECCIÓN FRENTE AL MALWARE
Se deben instalar antivirus en equipos y servidores	
	Se debe instalar un antivirus en todos los equipos y servidores de la empresa, que sirva tanto para el correo electrónico como para la navegación web. Se actualizará periódicamente o puntualmente cuando sea necesario, configurándolo y comprobando que está activo.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
ACTUALIZACIONES DE SOFTWARE (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Todo software es susceptible de necesitar actualizaciones por motivos de seguridad, esto incluye el *firmware* de los equipos electrónicos, los sistemas operativos y aplicaciones informáticas e incluso los propios programas antimalware. Los fabricantes de software lanzan **actualizaciones** y **parches** que mejoran y añaden nuevas funcionalidades, o que corrigen errores y agujeros de seguridad.

Si no se mantienen **convenientemente actualizados** los equipos y aplicaciones se expone a la empresa a todo tipo de **riesgos.** Los sistemas no actualizados son aprovechados por los delincuentes para introducirse en ellos y dejarlos inactivos, **infectarlos** (con lo que serían menos eficientes), aprovechar su capacidad de proceso para crear **botnets** con fines delictivos y **robar** todo tipo de datos (credenciales de acceso, datos confidenciales, etc.).

Se debe tomar conciencia sobre la necesidad de mantener permanentemente actualizado y parcheado todo el software. Se tendrá en cuenta que existen aplicaciones que incluyen sistemas de **actualizaciones automáticas** que es recomendable aplicar. En los casos de actualización manual se tendrá muy en cuenta que las fuentes de dónde obtenemos el software sean de confianza. En los casos en lo que se disponga de servicios subcontratados a terceros, también se deberá exigir que el software este convenientemente actualizado.

Todo el software tiene un **ciclo de vida**, por lo que llegado el momento puede quedar **obsoleto** y sin soporte oficial por parte del fabricante. En ese momento es un blanco fácil para los ciberdelincuentes (sobre todo si estamos conectados a internet) y deberíamos dejar de utilizarlo.

El objetivo de esta política es revisar la existencia de **actualizaciones** y **parches** de seguridad para el software y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en los equipos de forma **segura** y **controlada**.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.23.A]	DETERMINAR EL SOFTWARE QUE DEBE SER ACTUALIZADO
Se deberá realizar un listado del software existente en la empresa para incluirlo en el plan de actualizaciones	
	Se tendrá que realizar un inventario de todo el software y el firmware instalado, ya que pueden descubrirse errores o mejoras de funcionalidad. Para corregir dichos errores y garantizar un comportamiento óptimo se deben instalar, en cuando se tenga conocimiento de ellos, las correspondientes actualizaciones y parches de seguridad.

[SEG.23.B]	DETERMINAR CUÁNDO Y QUÉ ACTUALIZACIONES INSTALAR
Se deben revisar las características y los requisitos de las actualizaciones y parches antes de instalarlos	
	El equipo técnico determinará el momento en que ejecutar las actualizaciones para no interferir con las operaciones de la empresa. Aunque los principales programas comerciales disponen de funcionalidades de actualización automática, cabe la posibilidad de que se tenga software instalado que no disponga de estas opciones de actualización. En este caso se usarán los canales de alerta y los procedimientos oportunos para detectar e instalar las actualizaciones correspondientes. Antes de su instalación se considerará la utilidad de las nuevas mejoras y la gravedad los errores que subsanan, así como los requisitos hardware/software necesarios.

[SEG.23.C]	PROBAR LAS ACTUALIZACIONES
Se debe analizar y contrastar en un entorno de pruebas las actualizaciones que se deseen instalar	
	Siempre se deben instalar actualizaciones provenientes de fuentes confiables. No obstante, se debe sopesar la necesidad de disponer de un entorno de pruebas o preproducción donde instalar y probar las actualizaciones, de este modo se podrá verificar que su funcionamiento es el esperado. Es obligatorio realizarlo así en las actualizaciones de aplicaciones críticas instaladas en servidores (CMS, servidores web, servidores de correo, etc.).

[SEG.23.D]	DESHACER LOS CAMBIOS
Se debe contar con los mecanismos y procedimientos para deshacer los cambios sufridos tras ejecutar una actualización en caso de no resultar conveniente	
	Antes de aceptar la instalación de una actualización, se debe considerar la forma de deshacer los cambios realizados. Así si el comportamiento del software actualizado no responde a lo esperado se podrá volver a la situación anterior. Siempre es recomendable disponer antes de cualquier cambio de copias de seguridad recientes localizadas y probadas.

[SEG.23.E]	HERRAMIENTAS DE DIAGNÓSTICO Y ACTUALIZACIÓN
Se deberían utilizar herramientas de autodiagnóstico para detectar software no actualizado en los equipos	
	Existen herramientas que revisan si el software de nuestros equipos está actualizado o no. Una vez detectadas las actualizaciones pendientes, se podrá proceder a su instalación en todos los equipos de manera centralizada. Esto puede ser útil en entornos con muchos equipos en los que se quiere que el software instalado sea homogéneo y esté especialmente controlado.

[SEG.23.F]	CONFIGURACIÓN DE LOS SISTEMAS DE ALERTAS
Se debería tener configurado un sistema de alertas para recibir avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad	
	Conviene configurar un sistema de alertas para recopilar avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad del software utilizado. Estas alertas pueden ser de varios tipos: • *suscripciones a boletines genéricos sobre avisos y vulnerabilidades en la red;* • *suscripciones a boletines específicos sobre actualizaciones y novedades acerca de los productos y servicios software que utilizamos;* • *seguimiento en redes sociales de las publicaciones especializadas en ciberseguridad;* • *revisión periódica de medios y fuentes especializados;* • *configuración de sistemas de avisos RSS.*

[SEG.23.G]	REGISTRO DE ACTUALIZACIONES
Se debe registrar cada una de las actualizaciones y parches que se instalan	
	Se realizará un registro de las actualizaciones que se han instalado en los sistemas. De esta forma se podrá tener en todo momento un conocimiento exhaustivo del software operativo en los equipos.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
CONCIENCIACIÓN Y FORMACIÓN (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

El creciente uso de las nuevas tecnologías en las empresas hace indispensable la **concienciación** sobre los riesgos asociados a las mismas. Es necesario que los empleados conozcan y apliquen buenas prácticas en el uso de todo tipo de dispositivos (de escritorio, portátiles, móviles, pendrives,...) y soluciones tecnológicas (página web, servicios en la nube, redes sociales, correo electrónico,...) para lo cual se les debe proporcionar **formación** en ciberseguridad adecuada a su puesto ya que de este modo se pueden **prevenir** la mayoría de los incidentes.

Para alcanzar los objetivos fijados con esta política, será necesario el **compromiso total** por parte de la dirección, que ha de ser consciente que la formación debe ser una actividad continua que ha de repetirse y revisarse periódicamente, para que surta su efecto preventivo de incidentes y esté adaptada a las nuevas tecnologías que inevitablemente iremos utilizando.

El objetivo de esta política es asegurar que, en todo momento, los empleados **conocen, entienden y cumplen** las normas y las medidas de protección en materia de ciberseguridad adoptadas, advirtiéndoles de los **riesgos** que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.24.A]	DIFUSIÓN DE LA POLÍTICA DE SEGURIDAD
Se debe documentar y difundir las normas de ciberseguridad de la empresa para que estén siempre accesibles	
	Las normas de seguridad de la información de la organización deben estar correctamente documentadas y al alcance de todo el personal en todo momento.

[SEG.24.B]	CONCRETAR EL PLAN DE FORMACIÓN
Se debe elaborar o revisar el plan de formación para elevar el nivel de seguridad de la plantilla	
	Para garantizar el éxito del programa formativo, se deben seleccionar los aspectos que se quiere que sean cubiertos: • *procedimientos y controles de seguridad básicos;* • *necesidad de conocer y cumplir normas, leyes, contratos y acuerdos;* • *seguridad en el puesto de trabajo, aplicaciones permitidas, uso correcto de los recursos, propiedad intelectual, protección datos personales, etc.;* • *conciencias a los empleados sobre la existencia y peligros de la ingeniería social;* • *responsabilidad personal por acción u omisión y posibles sanciones.*

[SEG.24.C]	PROGRAMAS DE FORMACIÓN ESPECÍFICOS
Se debe desarrollar y aplicar programas de formación en ciberseguridad adecuados a los distintos puestos de trabajo	
	Es conveniente analizar si se deben desarrollar programas de formación y concienciación especializados para ciertos perfiles de empleados, tales como técnicos de soporte, administradores de sistemas, etc. Además, sería de gran utilidad elaborar una actividad formativa introductoria para los nuevos empleados.

[SEG.24.D]	PERIODICIDAD DE LA FORMACIÓN
Los empleados deberían realizar cursos o asistir a charlas de concienciación de forma periódica	
	Se debe establecer una periodicidad en las actividades formativas y de concienciación. De esta manera se consigue tener unos contenidos actualizados en materia de ciberseguridad y se refuerzan las debilidades detectadas o los mensajes de mayor importancia.

[SEG.24.E]	EVALUAR EL APRENDIZAJE OBTENIDO
Se debe comprobar la asimilación del conocimiento adquirido por los empleados	
	Se debería considerar la necesidad de realizar evaluaciones entre los empleados para determinar el grado de concienciación y formación que han alcanzado

[SEG.24.F]	PROMOVER UNA CULTURA DE SEGURIDAD DE LA INFORMACIÓN
Se debe promover una cultura de seguridad de la información que abarque a toda la cadena de suministro de la empresa y a sus clientes	
	Además de concienciar y formar a los empleados en ciberseguridad, es conveniente exigir a las entidades externas que interactúan con los sistemas de información de la entidad que sus políticas de ciberseguridad estén alineadas con la de la entidad. Se debe intentar extender el plan de concienciación a la mayoría de los proveedores y clientes.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

ALMACENAMIENTO EN LA RED CORPORATIVA (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir información entre los diferentes usuarios de la empresa se puede disponer de servidores de almacenamiento en red.

En la red corporativa es necesario distinguir entre información general de la empresa que deben utilizar todos los usuarios, e información de trabajo de los empleados almacenada en esta red corporativa. Los controles de acceso a esta información son definidos por la dirección y el responsable de sistemas, con el objetivo de limitar quién puede acceder y a dónde.

El contenido de la información almacenada se determina a través de una Política de clasificación de la información que debe cubrir al menos los siguientes aspectos: tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema, además de las personas encargadas de la actualización de dicha información en caso de modificación. Se prestará una especial atención cuando la información haya sido catalogada como confidencial o crítica o si está sujeta a algún requisito legal.

Las empresas que necesitan almacenar gran cantidad de información utilizarán los sistemas de almacenamiento en redes del tipo *NAS* (*Network Attached Storage*), para archivos compartidos, o *SAN* (*Storage Area Network*) de alta velocidad para bases de datos de aplicaciones. Estos sistemas presentan un volumen de almacenamiento grande, ya que unen la capacidad de múltiples discos duros en la red local como un volumen único de almacenamiento.

El objetivo de esta política es conseguir que los trabajadores hagan un buen uso de los servidores de almacenamiento disponibles para un óptimo tratamiento de la información.

Concienciar a los empleados de la relevancia de la información corporativa para un buen desempeño de su trabajo y de la necesidad de almacenarla en un sitio centralizado para evitar duplicidades y problemas de versiones, evitar pérdidas de documentos, centralizar las copias de seguridad, compartir información para la elaboración de proyectos y documentos, etc.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.25.A]	INVENTARIO DE LOS SERVIDORES DE ALMACENAMIENTO
Se debe informar a los empleados sobre los servidores de almacenamiento disponibles, y la información que se comparte, qué datos deben almacenarse en ellos y las responsabilidades que conlleva	
	El empresario debe poner en conocimiento de los empleados cuáles son los servidores de almacenamiento disponibles en la red corporativa, la información que se comparte, qué datos deben ser almacenados en los mismos y las responsabilidades que conlleva. Esto se deberá reflejar en la formación de los nuevos empleados y refrescarse cada cierto tiempo.

[SEG.25.B]	CRITERIOS DE ALMACENAMIENTO
Se debe informar a los empleados sobre los criterios de almacenamiento corporativos (qué se puede almacenar, quién tiene acceso y cuándo se elimna la información)	
	Se deberá elaborar una normativa que establezca que la información debe almacenarse en la red corporativa teniendo en cuenta los siguientes aspectos: • *qué información debe o no debe almacenarse en estos directorios;* • *las personas que tienen acceso a la información y si son encargadas su actualización en caso de necesidad de modificación;* • *cuándo es necesario eliminar la información por quedarse obsoleta.*

[SEG.25.C]	CLASIFICACIÓN DE LA INFORMACIÓN
Se debe informar al empleado sobre la necesidad de cumplir la política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa	
	El empleado debe conocer y cumplir la Política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa. De esta forma se almacenará en la forma y lugar correctos.

[SEG.25.D]	CONTROL DE ACCESO
Se debe establecer e implementar reglas de acceso que permitan llevar un control de quién tiene acceso y a qué discos/directorios	
	Es esencial establecer implementar reglas de acceso que permitan llevar un control de quién tiene acceso y a qué directorios o sistemas de almacenamiento.

[SEG.25.E]	COPIAS DE SEGURIDAD
Se debe definir un plan de copias de seguridad en el que se detalle la información a guardar, cada cuánto tiempo se va a realizar, dónde se va a almacenar y el tiempo de conservación de la copia	
	Se deberá ejecutar el plan de copias de seguridad en el que se detalla la información a guardar, cada cuánto tiempo se va a realizar, dónde se va a almacenar y el tiempo de conservación de cada copia.

[SEG.25.F]	ACCESO LIMITADO
Se debe permitir el acceso a los empleados únicamente a los repositorios necesarios para el desempeño de su trabajo	
	Según lo establecido en la política de clasificación de la información se definen perfiles de acceso (y se asignan a los usuarios) que limitan el uso de la información, de manera que cada usuario acceda solo a los directorios necesarios para el desempeño de su actividad laboral.

[SEG.25.G]	ALMACENAMIENTO CLASIFICADO
Se deben crear carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Se deben asignar los permisos de accesos pertinentes según el perfil del empleado	
	Se deberán crear carpetas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Se asignarán los permisos de acceso pertinentes según el perfil del empleado.

[SEG.25.H]	AUDITORÍA DE SERVIDORES
Se debe revisar periodicamente el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.	
	Cada cierto tiempo, que se deberá especificar, se tendrá que revisar el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.

[SEG.25.I]	CIFRADO DE LA INFORMACIÓN
Se debe cifrar la información crítica almacenada en los servidores	
	Según la política de clasificación de la información, se deberá cifrar la información crítica que se almacene en la red corporativa.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD

POLÍTICA DE TELETRABAJO (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Esta política surge como respuesta a los riesgos derivados del teletrabajo, los cuales muchas veces no son tenidos en suficiente consideración

Si bien aplica a cualquier tipo de teletrabajo, también se centra en la creciente tendencia a trabajar esporádicamente desde casa con equipos propios o a la necesidad durante periodos vacacionales de conectar con el entorno laboral, ya sea para llevar el seguimiento de tareas o proyectos, como para solventar temas urgentes cuando por la distancia no es posible trasladarse físicamente al lugar habitual de trabajo.

Se hace especial hincapié en los riesgos derivados de la utilización de dispositivos personales en el entorno corporativo (también conocido como Bring Your Own Device - BYOD), así como a usuarios que conecten de continuo desde casa o remotamente desde otras ubicaciones (como puede ser la oficina del cliente).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, debe implantarse una política de protección en teletrabajo. A continuación, se facilita una serie de obligaciones y buenas prácticas en materia de seguridad que aplican al Teletrabajo, con el objetivo es garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de Teletrabajo.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.26.A]	MARCO NORMATIVO INTERNO
La organización debe establecer un marco normativo interno con el fin de procedimentar y estandarizar el modo y las condiciones bajo las cuales la dirección desea que se desarrolle el teletrabajo.	
	Dependiendo del tamaño y naturaleza de la organización puede ser necesario definir normativas y pautas que abarquen los siguientes puntos: • *Tipos de usuarios que dispondrán de modalidad de teletrabajo y los permisos de acceso remoto de que dispondrán* • *Procedimiento para solicitud y autorización del teletrabajo* • *Procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales* • *Posible utilización de equipos personales para el teletrabajo así como las medidas de seguridad aplicables a los mismos* • *Criterios para la conexión de equipos no confiables al entorno corporativo, ya sea remota o localmente* • *Medidas de seguridad extraordinarias aplicables a los dispositivos utilizados para el teletrabajo* • *Normativas referentes al almacenamiento de información de negocio fuera de las instalaciones, ya sea en equipos de la organización, equipos personales de empleados o dispositivos extraibles* • *Cualquier otra que se considere necesaria por la organización*

[SEG.26.B]	APROBACIÓN FORMAL POR DIRECCIÓN
Cualquier forma de teletrabajo debería estar aprobada formalmente por la dirección y se debería llevar un control de qué usuarios utilizan esta modalidad.	
	Esta modalidad permite, entre otras ventajas, llevar un control del equipamiento que el usuario utiliza y saca de las instalaciones, permite la localización del usuario en caso de incidentes, facilita la justificación de ausencia de la oficina en caso de accidentes personales durante la jornada laboral, pero lo más importante es que permite implantar y aplicar a quien corresponda las diferentes medidas técnicas y organizativas dependiendo del perfil del usuario, la información que maneja, y los riesgos a los que está expuesto.

[SEG.26.D]	CONTROLES GENERALES
Son aquellos que toda la organización debe cumplir independientemente del tipo de trabajo, y que sin un correcto seguimiento pueden quedar sin implantar ya sea por utilizar equipos propios del usuario, por el desconocimiento del usuario o por las diferencias tecnológicas en los entornos de trabajo.	
	Algunos ejemplos pueden ser la periodicidad de las copias de seguridad, actualizaciones automáticas de software, ejecución y actualización periódica del antivirus, tiempos de bloqueo de equipos por inactividad, control de accesos de usuarios, o similares, los cuales no siempre están correctamente configurados o tenidos en cuenta en una instalación personal o doméstica.

[SEG.26.D]	CONTROLES ADICIONALES
Aquellos de los que no siempre se dispone de forma genérica ya sea en el lugar de trabajo o en el entorno organizativo.	
	Hablamos de capas de cifrado de información, cláusulas de responsabilidad adicionales, cumplimiento de procedimientos específicos, contraseña en BIOS, software para asistencia remota y localizar el equipo en caso de pérdida o robo, inventario de información del dispositivo, procedimientos de emergencia para revocar los permisos del usuario (también en caso de pérdida), o herramientas de borrado remoto de dispositivos.

[SEG.26.E]	EQUIPO Y SISTEMA OPERATIVO
Cualquier equipo que vaya a conectarse a los entornos corporativos, ya sea propiedad de la organización, proveedor o del empleado, debe cumplir con unos mínimos de seguridad	
	Entre los estándares mínimos de seguridad se encuentran: • *Instalación del sistema operativo y software desde fuente original o fiable* • *Sistema operativo y aplicaciones actualizadas* • *Software antivirus* • *Cuentas de usuario sin permisos para instalar software* • *Control de acceso robusto* • *Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.)* • *Bloqueo automático por inactividad* • *Software antirookits* • *Control de software original* • *Cifrado de disco* • *Comprobación periódica de la adecuación de las salvaguardas.*

[SEG.26.F]	EQUIPOS NO CONFIABLES
Si la información a tratar en los equipos de teletrabajo es considerada importante o crítica, pero no se considera el equipo lo suficientemente confiable en los términos mencionado en el apartado anterior, es posible aplicar medidas compensatorias para conseguir niveles aceptables de seguridad.	
	Entre las diferentes opciones para conseguir niveles aceptables de seguridad se encuentran: • **Diferentes cuentas de usuario:** Se trata simplemente de tener diferentes cuentas de usuario en el mismo equipo donde se utilizará una para entornos confiables (teletrabajo) y otra para asuntos personales. Se recomienda almacenar la información de forma cifrada. • **Arranque dual:** Consiste en instalar en un mismo equipo dos sistemas operativos, iguales o diferentes, de los cuales cada uno se utilizará para un entorno (teletrabajo o personal). Se recomienda almacenar la información de forma cifrada. • **Distribuciones "live":** Se trata de instalaciones completas de sistemas operativos que son totalmente independientes de lo que haya en el PC ya que se cargan antes de que el sistema operativo del equipo arranque. De esta forma, se utilizaría el sistema operativo del PC para temas personales y la distribución "live" para el teletrabajo.

[SEG.26.G]	PROTECCIONES ANTIROBO
Para evitar robos de equipos portátiles suele ser suficiente tomar algunas medidas de sentido común como no djarlo en el coche (aunque no esté a la vista), no dejarlo desatendido, evitar sacarlo de casa si no es necesario, etc.	
	Además, pueden adquirirse candados de seguridad para portátiles, lo cuales sirven para anclar el dispositivo a algún elemento del mobiliario, aunque bien es cierto que no son extremadamente robustos y según su calidad pueden romperse con herramientas simples. *Su utilidad está más enfocada a proteger el equipo del robo fácil por descuido que no de una intrusión en casa o en la oficina.* *Otra solución pasa por adquirir un armario de seguridad donde almacenar el equipo y otros artículos de relativo valor, los cuales evitarán que ante una "intrusión relámpago" en el domicilio se sustraiga el equipo de trabajo.*

[SEG.26.H]	BORRADO REMOTO
Deben implementarse aplicaciones tanto para dispositivos móviles como para PC que permitan administrar remotamente los dispositivos extraviado o robados.	
	Entre las funcionalidades típicas de estos programas se encuentran: • *Activar el GPS del dispositivo (si lo tiene) para intentar localizarlo* • *Lo anterior podría permitir hacer un borrado completo del equipo si no va a ser posible recuperarlo* • *Instalar aplicaciones que permitan acceder remotamente al equipo para recuperar datos necesarios antes de borrar el disco, monitorizar el uso que se está haciendo del equipo, o incluso activar la webcam para intentar averiguar la identidad del ladrón.* • *Cabe recordar que estas aplicaciones evidentemente deben instalarse antes de que el dispositivo se extravíe ya que por lo general después será demasiado tarde.*

[SEG.26.I]	DAÑOS FISICOS
Se deben implementar mecanismos para evitar el daño físico	
	• *Para el transporte entre la oficina y el lugar de teletrabajo es necesario disponer de una **funda o maletín que ofrezca buena resistencia** a caídas, golpes, aplastamiento o incluso líquidos.* • *Se debe prestar **atención al cableado**. El no estar en la oficina no significa que se puede tener todo desastrado. Un correcto cableado evitará tropiezos que acabarían con el dispositivo.* • ***Guardar el dispositivo en lugar seguro** mientras no se utiliza. Aunque no es frecuente tener intrusiones en el lugar de teletrabajo, existen otros peligros con los que no contamos en la oficina: mascotas subiendo a las mesas, niños pequeños intentando alcanzar cualquier cosa de la mesa, o sobrinos en busca de algo conectado a internet para consultar una red social. Si no se está utilizando lo más recomendable es retirarlo* • *Considerar **cambiar el disco duro** por un SSD. Los discos duros tradicionales funcionan mediante agujas que leen los datos y que nunca deben tocar los discos que giran a gran velocidad. Cualquier vibración o caída en un momento delicado puede conllevar una pérdida total de los datos. Los discos SSD no disponen de partes móviles y son mucho más resistentes. Además, son más rápidos y reducen el consumo de recursos.*

[SEG.26.J]	TABLETS Y SMARTPHONES
Los dispositivos móviles no se limitan a leer documentos ofimáticos. También se utilizan para recibir correos electrónicos, atender llamadas de trabajo, almacenar información corporativa, tener acceso remoto a documentos en la nube, o incluso tener conversaciones por mensajería instantánea sobre temas laborales.	
	Entre los consejos más recomendados, se encuentran los siguientes: • *Limitar el acceso al dispositivo mediante un bloqueo con contraseña, patrón o similar* • *Cifrar la memoria del dispositivo o caso de contener información sensible* • *Disponer de medidas para localizar el dispositivo o hacer un borrado remoto del dispositivo en caso de pérdida o robo* • *Disponer de algún mecanismo lo más automatizado posible para hacer copias de seguridad de la información del dispositivo* • *Tomar medidas para prevenir y detectar malware en los dispositivos móviles* • *No se deben deshabilitar las medidas de seguridad de las que disponen los dispositivos. Esto incluye, conseguir permisos de administrador, o permitir instalar software de fuentes no fiables* • *Instalar siempre las últimas actualizaciones de seguridad de los programas y sistemas operativos.* • *Desactivar las conexiones inalámbricas que no se utilicen como Bluetooth, Wifi o NFC.*

[SEG.26.K]	DISPOSITIVOS BYODS
Si se permite la utilización de dispositivos personales (ordenadores, smartphone, tables, etc. propios del trabajador) debe implementarse una política de BYOD para tomar una serie de medidas de seguridad técnicas y organizativas.	
	Entre dichas medidas, están: • *Establecer políticas organizativas al respecto indicando lo que se considera un uso adecuado de los equipos y lo que no, además de un compromiso por parte del trabajador para con la seguridad de la información que se trate en el dispositivo.* • *Documentar los derecho y obligaciones de cada parte y detallar en qué casos el equipo podrá ser objeto de revisión por parte de la organización.* • *Disponer de un mecanismo de reemplazo de equipos en caso de pérdida o avería de los mismos para garantizar que el empleado pueda seguir desempeñando sus tareas habituales* • *Establecer medidas técnicas para garantizar las mismas condiciones de seguridad que tendría la información en caso de estar almacenada en un equipo local propio de la organización en lugar del empleado. Se recomienda el uso de cuentas de usuarios independientes, uso de sistemas operativos o máquinas virtuales separadas, además de implantar el resto de controles habituales (borrado remoto, cifrado, copias de seguridad, control de acceso, etc.)* • *Establecer medidas para evitar el acceso fortuito a información corporativa por otros usuarios del equipo aparte del propio empleado: familiares o similar.* ***VEASE**: Política [SEG.05] Uso de dispositivos móviles no corporativos.*

[SEG.26.L]	COMUNICACIONES
Se debe realizar una correcta configuración de la estructura de comunicaciones entre los empleados en teletrabajo y la organización	
	Estas son las principales consideraciones a tener en cuenta a la hora de utilizar una conexión a internet para conectar con los recursos corporativos: • *No utilizar conexiones poco confiables (Wifi abiertas, redes públicas de hoteles, bibliotecas, locutorios, etc.) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por httpS. No basta con tener contraseña para conectar.* • *Si es posible se recomienda utilizar conexiones 3G o 4g, los cuales son bastante más seguras que las redes inalámbricas ajenas.* • *Los administradores deberán de llevar un seguimiento cercano de las conexiones remotas a los servicios corporativos de teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.* • *Se deben evitar las soluciones de administración remota gestionadas por terceros como pueden ser LogMeIn o TeamViewer ya que se evaden por completo de cualquier arquitectura de seguridad implantada, además de delegar el acceso a los sistemas a terceros externos a la organización.*

[SEG.26.M]	VPN (Virtual Private Network)
Estas redes hacen que un usuario pueda conectarse de forma segura, para él y para la organización, a servicio o servidores que no se encuentran directamente accesibles a Internet.	
	Entre las ventajas de usar este tipo de conexiones VPN se encuentran: • *El uso de sistemas de certificados digitales que permiten que el usuario tenga la certeza de que se está comunicando con las aplicaciones correctas (no es posible que le falsifiquen las direcciones de las empresas)* • *Asegura que todo lo que se envíe y reciba está cifrado y a salvo de intercepciones o robos de información.* • *Estas redes permiten trabajar desde casa como si fuese desde la propia oficina, teniendo acceso a todos los recursos internos que sean necesarios, pudiendo utilizar programas internos, clientes de correo electrónico, e incluso llegar a imprimir remotamente.* • *Su uso es relativamente sencillo pues, una vez hecha la configuración inicial, bastará con arrancar un programa e introducir la contraseña para que todo quede configurado.* • *Facilita la robusted y seguridad ya que pueden configurarse para que utilicen autenticación fuerte de doble factor.*

[SEG.26.N]	HERRAMIENTAS DE ADMINISTRACIÓN REMOTA
Se debe determinar en qué casos está permitida la conexión remota y en cuales no, además de cúales son los procedimientos oficiales y las aplicaciones permitidas para dicho propósito (LogMeIn, TeamViewer, etc).	
	En estos casos, debe darse consideración a: • *Al instalar este tipo de aplicaciones en realidad se está abriendo una puerta trasera al equipo y a la red interna de la organización, que tira por tierra muchas de las medidas de seguridad implantadas, como puede ser el filtrado de conexiones mediante cortafuegos, control de conexiones desde VPN, revisiones de usuarios con teletrabajo, robustez de contraseñas, etc., permitiendo que un atacante pueda probar contraseñas directamente contra un servicio web gestionado por un tercero y sobre el que tenemos poco control.* • *Además de lo anterior, cabría la posibilidad de que los empleados de estas compañías (LogMeIn, TeamViewer, etc.) pudieran conectarse a los equipos sin permiso, o incluso una intrusión en sus sistemas daría acceso a todos los equipos clientes, por lo que no son soluciones aconsejables.*

[SEG.26.Ñ]	COPIAS DE SEGURIDAD
En el teletrabajo no siempre se siguen las mejores prácticas en lo referente a las copias de seguridad de la información. Se debe ser consciente de que cualquier información que se saca de las instalaciones, especialmente en equipo portátiles, corre peligro de ser robada junto con el dispositivo, sufrir accidente doméstico que inutilice el acceso que se pierda por una subida de tensión en el lugar de teletrabajo.	
	El cómo operar dependerá principalmente de la modalidad de teletrabajo: • **Escritorios remotos:** Este viene a ser el único caso donde generalmente se gestionan correctamente las copias de seguridad de los datos del usuario ya que éste conecta directamente contra un servidor del entorno corporativo del cual se hacen copias de seguridad completas. • ***Perfil móvil, o sincronización automática:*** *En estos casos periódicamente se sincroniza de forma automática el contenido del PC del usuario con el entrono corporativo.* • ***Sincronización manual:*** *No es otra cosa que copiar periódicamente los ficheros actualizados contra algún servidor de la plataforma corporativa. Los principales problemas de esta solución son que no se hagan las copias con la frecuencia establecida por dejadez, o que la criticidad de la información y su volumen no hagan viable el hacer sincronizaciones manuales.* • ***Copias de seguridad offline:*** *Para este tipo de copias se recomienda utilizar un dispositivo externo con el fin de evitar un fallo físico, o que algún tipo de código malicioso corrompa la información almacenada en todo el equipo. Debería tenerse en cuenta también la posible necesidad de cifrar el soporte donde se almacenen las copias, almacenar el dispositivo bajo llave, o guardarlo en un lugar a salvo de peligros domésticos (fuego, agua, hijos pequeños, etc.)*

[SEG.26.O]	GESTIÓN Y TRASLADO DE CONTRASEÑAS
El robo de contraseñas en entornos de teletrabajo puede ser especialmente crítico ya que con una contraseña se podría acceder remotamente a los sistemas.	

	• *En caso de disponer de una conexión VPN que dé acceso a todos los demás servicios, se debe custodiar con extremo cuidado esta contraseña y seguir las mejores prácticas posibles: caducidad, complejidad, bloqueo por intentos fallidos, bloqueo por inactividad, revisiones de acceso, etc.*
	• *Si se trata de diferentes servicios (generalmente web) de los cuales cada uno dispone de una contraseña diferente la situación se complica ya que nunca se debe utilizar una única contraseña para todo*
	• *Para poder mantener las diferentes contraseñas y garantizar que no se van a olvidar, es muy recomendable almacenarlas en un gestor de contraseñas, el cual garantizará que están a salvo de robos además de permitir transportarlas, por ejemplo, en una memoria USB o incluso online en caso de necesitar movilidad.*
	• *Algunos de los gestores de contraseñas más utilizados son:*
	  • *Keepass (http://keepass.info)*
	  • *Teampass (http://teampass.net)*
	  • *OnePassword (https://agilebits.com/onepassword)*
	  • *1Password (https://1password.com/)*
	  • *LastPass (https://www.lastpass.com/es)*
	  • *Dashlane (https://www.dashlane.com/es)*
	  • *Enpass (https://www.enpass.io/)*
	  • *Keeper (https://keepersecurity.com/es_ES/)*
	  • *Bitwarden (https://bitwarden.com/)*
	  • *PasswordSafe (https://pwsafe.org/)*
	  • *Roboform (https://www.roboform.com/)*

[SEG.26.P]	CIFRADO DEL DISCO DURO Y SOPORTES
Proteger la información que se almacena fuera de la oficina debería ser una de las mayores prioridades de una organización a la hora de disponer de trabajadores en modalidad de teletrabajo, porque el robo o pérdida de un dispositivo portátil es algo que puede ocurrir con relativa facilidad. Es por ello que se debería cifrar la información	
	Existen diferentes soluciones de cifrado: • ***Cifrar una carpeta o el disco completo mediante el propio sistema operativo:*** *Los principales sistemas operativos disponen de herramientas de cifrado, ya sea para cifrar las carpetas personales del usuario llegando algunos incluso a permitir cifrar todo el disco duro.* • ***Crear un volumen de cifrado:*** *Existen herramientas que permiten, en lugar de cifrar una carpeta o un disco duro, crear un único fichero que contendrá la información cifrada.*

[SEG.26.Q]	PAPEL
En entornos de teletrabajo la información en papel debería ser menos susceptible de sufrir ataques deliberados (siempre y cuando no haya un trasiego habitual de documentación), pero el no estar en un ambiente laboral puede hacer que documentación relevante acaba junto con el papel y cartón para reciclar, se utilice para dibujar por detrás o que sufra algún accidente doméstico como que se derramen bebidas sobre él.	
	Es por ello que se deben tomar una serie de medidas de sentido común muy similares a las que se siguen en la oficina: • *Almacenar los documentos en lugar seguro mientras no se estén utilizando. Las medidas de seguridad se establecerán en base a los requisitos que su clasificación marque.* • *Se tomarán medidas de seguridad que se consideren oportunas para el transporte de la documentación, las cuales pueden ir desde no dejar la documentación desatendida, hasta utilizar contenedores especialmente preparados para ello.* • *Se debe estudiar a fondo el método de destruir la información en papel evitando tirarla directamente al contenedor de reciclaje (habitual en la mayoría de hogares), o peor aún, que se reutilice para labores domésticas (dibujar por detrás, hacer la lista de la compra, etc.)* • *Se deben aplicar el resto de buenas prácticas en cuanto a la gestión del papel, como pueden ser no dejar copias impresas desatendidas en la bandeja de la impresora, o configura el fax para que no imprima los faxes entrantes hasta que se solicite expresamente, evitando así que queden olvidado en la bandeja de impresión.*

[SEG.26.R]	SISTEMAS DE ALMACENAMIENTO ONLINE
El almacenamiento de datos en sistemas online conlleva una serie de riesgos que deben delimitarse	
	Se deben valorar: • *El nivel de seguridad de la información que se vaya a cargar en este tipo de servicios online ya que ante un ataque a la plataforma sería posible acceder a toda la información del usuario.* • *Dependiendo de la criticidad de la información puede ser necesario tomar medidas adicionales como el cifrado previo de la información, o el uso de medidas de protección de la propia plataforma, generalmente de pago, que aporten capas adicionales de seguridad.* • *También existen plugins y complementos que se encargan de cifrar la información de estos servicios online, pero dependiendo de la aplicación, una vez más pasamos a delegar la seguridad de los datos en un tercero, por lo que la situación final no siempre es un incremento de la seguridad.* • *Se debe considerar que, dependiendo de la naturaleza de los datos, se puede incurrir en el incumplimiento de normativas y leyes de protección de datos ya que en muchas ocasiones estos servicios se alojan en grupos de servidores repartidos por todo el planeta por lo que es muy difícil saber dónde está realmente la información, así como saber qué legislación le aplica.* • *Tampoco deben descuidarse otros temas como los contratos de prestación de servicio que ofrecen estas plataformas ya que no siempre se comprometen a garantizar la disponibilidad de la información, pudiendo tener falles técnicos que les dejen sin conectividad durante días, o pudiendo llegar al extremo de cerrar de un día para otro (o ser confiscados los servidores, como ya le sucedió a Megaupload) dejando al usuario sin posibilidad de recuperar sus datos.*

[SEG.26.S]	CONCIENCIACIÓN Y FORMACIÓN DEL USUARIO DE TELETRABAJO
Como eslabón más débil en la cadena de seguridad, el usuario es el que más expuesto está a los riesgos tecnológicos, pudiendo ser víctima de ataques de ingeniería social (engaños), robos, agresiones físicas, extorsión, etc.	
	Por desgracia, existen pocas medidas de seguridad que aplicar sobre las personas más allá del sentido común y la formación, por lo que es precisamente en estos puntos donde más esfuerzos se tienen que invertir. *Cualquier usuario que realice su actividad mediante teletrabajo debe estar familiarizado con todos los conceptos que aparecen en esta política, debe entender los riesgos a los que se enfrenta por no utilizar una arquitectura tradicional, y se le debe informar de las responsabilidades adicionales con respecto a la información y servicios de que disponga en comparación con un puesto de trabajo presencial.*

[SEG.26.T]	ENGAÑOS MEDIANTE INGENIERIA SOCIAL
Se conocen como ataques de ingeniería social aquellos que tratan de conseguir información mediante engaños a los usuarios.	
	• Los ataques de ingeniería social más frecuentes son: Correos electrónicos o llamadas telefónicas suplantando a algún compañero, proveedor o cliente y solicitando cualquier tipo de información, o llegando incluso a suplantar al soporte técnico y pedir al usuario que ejecute comandos en su equipo o que comparta las contraseñas de acceso. • Si bien este tipo de ataque puede afectar a cualquier empleado, el hecho de trabajar a distancia hace que sea posible que el usuario no conozca físicamente a sus compañeros, o que el comunicarse siempre por teléfono le haga ser más confiado ante una llamada maliciosa. • Para evitar este tipo de ataques se debe formar al usuario para que sepa en todo momento la información que puede dar por teléfono y la que no, como por ejemplo configuraciones de red, contraseñas o ficheros con información sensible. • Por otro lado, se debería establecer un protocolo para identificar al interlocutor en las llamadas telefónicas que vayan a requerir intercambiar información sensible, especialmente si los usuarios no se conocen. Puede ser algo tan sencillo como disponer de un listado de número de teléfonos autorizados, intercambiar verbalmente contraseñas pre-pactadas mediante métodos seguros, o sencillamente ser el propio usuario que haga la llamada hacia la sede de la organización y que sea la centralita quien redirija las conversaciones. • Cabe destacar que este tipo de ataques pueden llegar a ser muy elaborados pudiendo desde crearse perfiles falsos en redes sociales profesionales como Linkedin y hacerse pasar por alguien de la empresa, hasta llegar a entablar una relación amistosa en redes más generalistas para, con el tiempo, obtener información sensible.

[SEG.26.U]	AL FINALIZAR EL TRABAJO
En un entorno de teletrabajo donde es posible que el equipo se pierda, cuando se utiliza el equipo de casa para trabajar al cual tienen acceso otros miembros de la familia, o donde se utiliza un equipo que no es del propio usuario (jamás se debería trabajar desde un cibercafé u ordenador de un hotel/aeropuerto, pero sabemos que sucede), se recomienda seguir los siguientes consejos para protegar adecuadamente la información y las comunicaciones.	
	Aunque algunos puedan parecer excesivos, se deberán aplicar según la criticidad del equipo y su acceso por parte de otros usuarios: • *Cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción "desconectar" o "cerrar sesión"* • *Eliminar información temporal prestando especial atención a la carpeta de descargas, papelera de reciclaje, o posibles carpetas perdidas que se dejen en "Mis documentos"* • *Utilizar herramientas de borrado seguro para eliminar los ficheros en caso de información sensible o especialmente confidencial* • *Si se han utilizado certificados digitales, estos deben ser borrados de forma segura* • *Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el quipo.* • *Borrar el histórico de navegación, así como las cookies, y otros datos del navegador web, prestando especial atención a las contraseñas recordadas.*

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA DE SEGURIDAD
MENSAJERÍA INSTANTÁNEA

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

Los avances tecnológicos están en pleno auge y cada vez es más común el uso de la tecnología en las comunicaciones entre las personas. Sin embargo, se debe tener en cuenta los riesgos que suponen el uso de este tipo de tecnologías para la confidencialidad de los datos personales y para los derechos al honor y la intimidad de las personas.

Para garantizar un uso adecuado de las tecnológías de mensajería instantánea, se deben tomar ciertas medidas preventivas y establecer ciertos procedimientos y criterios que permitan a la organización realizar un buen uso de dichas tecnologías, tales como Whatsapp, Telegram, Signal y otros servicios similares, de los que no se tiene el control total de los datos transmitidos a traves de estos servicios.

A continuación, se facilita una serie de obligaciones y buenas prácticas en materia de seguridad y cumplimiento normativo que aplican al uso de la mensajería instantánea para la comunicación con otras personas, compartir información o documentos, crear grupos de comunicación o listas de distribución, etc.

2.- ALCANCE

La presente política es aplicable a:

- Todos los usuarios del que intervengan en los sistemas de procesamiento de datos personales de la organización COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN y que PERTENEZCAN a los siguientes PERFILES:
    - Presidencia; Vocal; Secretaría; Administración; Tesorería

[SEG.27.A]	xxxxxxxx
xxxxx	
	xxxx • *xx* • *xx*

[SEG.27.B]	BLOQUEO PROGRAMADO DE SESIÓN
Se debe programar el bloqueo automático de sesión en los equipos al no detectarse actividad del usuario durante un corto periodo de tiempo (Máximo 15 minutos)	
	El personal informático programará un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo. Adicionalmente se puede contemplar llevar a cabo la programación del apagado general de equipos una vez terminada la actividad empresarial.

COLEGIO PROFESIONAL DE MEDIADORES DE SEGUROS DE CASTELLÓN

POLÍTICA CUMPLIMIENTO NORMATIVO

[VID.01] VIDEOVIGILANCIA (v2.0)

COLEGIO PROFESIONAL MEDIADORES DE SEGUROS CASTELLÓN

1.- PROPÓSITO

El uso de cámaras de Video Vigilancia se está extendiendo de forma notable en los últimos años con el objetivo de garantizar la seguridad de las personas y la seguridad de los bienes. No cabe duda, que el uso de cámaras de Video Vigilancia ofrece unas óptimas garantías de seguridad para aquel que las utilice. Sin embargo, se ha de tener presente que la grabación de imágenes supone en la mayoría de casos grabación de personas, por lo que el uso de cámaras de Video Vigilancia constituye un tratamiento de datos personales (la imagen es un dato personal), lo que hace que dicha grabación este dentro del ámbito del 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, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales su Instrucción 1/2006 de Video Vigilancia.

La Organización que hace uso de estos sistemas de Video Vigilancia ha de ser consciente de que esta tecnología supone asimismo una fuerte intrusión a la privacidad e intimidad de las personas, por lo que se establece un choque entre la Seguridad y la Intimidad.

El objetivo de esta política es mantener un justo equilibrio entre estos dos derechos se ha procedido ha realizar una política de uso de cámaras de Video Vigilancia con el objeto de minimizar al máximo la intrusión a la intimidad de estos sistemas de Video Vigilancia

2.- ALCANCE

La presente política es aplicable a:

[VID.01.A]	PROPORCIONALIDAD
la instalación de las cámaras debe de ser proporcional, es decir, adecuado, pertinente y no excesivo con el objetivo que se persigue con la Videovigilancia de tal forma que no ataque al derecho a la intimidad.	
	Las cámaras se instalarán únicamente en aquellas zonas que necesite cumplir con el objetivo de seguridad (zonas como los accesos a las instalaciones, zonas sensibles de agresiones a la seguridad, etc.). Queda prohibida la instalación de cámaras de seguridad en zonas donde el derecho a la intimidad se hace más patente como zonas de descanso, baños, vestuarios, etc.
	Si se utilizan cámaras orientables y/o con zoom será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos, viviendas o cualquier otro espacio ajeno

[VID.01.B]	CARTELES INFORMATIVOS
Los carteles con distintivos informativos de videovigilancia deberán estar claramente visibles, tanto en espacios abiertos como cerrados.	
	El hecho de que los carteles de videovigilancia estén visibles no implica que estos deban estar ubicados necesiariamente en las mismas localizaciones que las cámaras.
	Es súmamente importante que los carteles de videovigilancia estén colocados en lugares estratégicos de modo que sean visibles y permitan advertir de la zona videovigilanda ANTES de que el individuo sea captado por las cámaras de videovigilancia.

[VID.01.C]	IMPRESOS INFORMATIVOS
Se debe establecer a un departamento determinado para que tenga a disposición de los interesados suficientes impresos en los que se detalle la información prevista en los artículos, 12 y 13 del Reglamento General de Protección de Datos.	
	***Artículo 12**. Respecto a las posibles personas objeto de videovigilancia se debe:* • *Informar de forma concisa, transparente, inteligible y de fácil acceso* • *Facilitar el ejercicio de los derechos que le amparan* • *Atender las solicitudes de ejercicio de derechos en un plazo máximo de 30 días* • *Informar al interesado que ejerce sus derechos incluso si no se disponen de imágenes suyas.* • *Se podrá solicitar una fotografía reciente para identificar al individuo en las imágnes de videovigilancia* • *Informar mediante carteles distintivos de videovigilancia*
	***Artículo 13**. Se debe informar al interesado de:* • *La identidad y los dtos de contacto del responsable de la videovigilancia* • *Los datos de contacto del Delegado de Protección de Datos, si lo hubiere* • *Los fines del tratamientos a que se destinan los datos captados por los sistemas de videovigilancia y las bases jurídicas que legitiman el tratamiento de las imágenes captadas.* • *Si la base jurídica sea "interés legítimo del resoposable del tratamiento", se deberán detallar dichos intereses legítimos.* • *Los posibles destinatarios o categorías de destinatarios a los que se comunican las imágenes de videovigilancia.* *Además de lo anterior, se deberá informar de:* • *El plazo de conservación de las imágenes (no superior a un mes) o los criterios utilizados para determinar dicho plazo* • *Los derechos que asisten al interesado (persona captada por los sistemas de videovigilancia)* • *Derecho del interesado a presentar una reclamación ante la AEPD en caso de que considere que el tratamiento no es conforme a lo establecido en el RGPD.* • *Si se realizara o estuviese prevista la realización de decisiones automatizadas o elaboración de perfiles, se debe informar previamente al interesado.*

[VID.01.D]	CONTROL DE ACCESO FÍSICO
Los sistemas de videovigilancia se ubicarán en un lugar vigilado y de acceso restringido, considerando las siguientes directrices:	
	La puerta de la sala del sistema de grabación debe de contar con dispositivos de control a través de mecanismos que obstaculicen su apertura bien a través del uso de llaves o del uso de sistema mediante huella digital para autorizar el acceso.
	Tiene autorizado el ingreso a sala del sistema de grabación el Responsable de Seguridad, personal autorizado específicamente para ello y el personal de servicio de vigilancia de la organización si estuviera contratado.
	Es recomendable mantener registros de acceso, en los que se indique identificación de la persona, fecha y hora de entrada. Estos registros deberán mantenerse por un plazo mínimo de un año.
	El ingreso de personal de soporte de terceras partes será autorizado cuando sea requerido. Los mismos deberán estar acompañados por personal de las áreas autorizadas al ingreso. En caso de que el trabajo a realizar justifique que los mismos ingresen en forma independiente, se le entregará una tarjeta de acceso individual. Para la entrega de la tarjeta de acceso, se deberá entregar un documento de identidad que se retornará una vez entregada la tarjeta. Se gestionará este tipo de acceso, registrando el nombre de la persona, empresa, persona que autorizó el ingreso, fecha y hora de entrega de la tarjeta, fecha y hora de devolución. La persona deberá firmar el registro al retirar la tarjeta y al momento de su devolución
	Los derechos de acceso deben ser revisados y actualizados semestralmente y serán revocados cuando sea necesario

[VID.01.E]	CONTROL DE ACCESO LÓGICO
El acceso a las imágenes de grabación del sistema de videovigilancia será restringido a personal autorizado.	
	Únicamente tendrán acceso al funcionamiento del equipo de grabación el Responsable de Seguridad, personal autorizado específicamente para ello y el personal de servicio de vigilancia de la organización si estuviera contratado. Dicho personal deberá garantizar la confidencialidad de las imágenes capturadas.
	Se prohíbe la ubicación de pantallas donde se puedan visualizar las imágenes de los sistemas de grabación en lugares donde puedan ser visualizadas por personal interno o externo no autorizado.
	Las imágenes que queden registradas en los soportes de grabación únicamente serán visionadas en el monitor si previamente se hubiese recibido constancia de alguna agresión a la seguridad, como robo, acceso indebido por la noche, etc. no pudiendo ser utilizada con ninguna otra finalidad, que no esté legitimada.

[VID.01.F]	AUDIO
Las videograbaciones no registrarán conversaciones de audio privadas	
	Solamente podrán registrarse grabaciones en audio en casos excepcionales, por causas legitimas imperiosas y previa ponderación de los derechos de los interesados con los objetivos del tratamiento del audio.

[VID.01.G]	PLAZO DE CONSERVACION
Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación	
	Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservadas para acreditar la comisión de actos que atenten contra la integridad de menores, bienes o instalaciones.

[VID.01.H]	CONTROL LABORAL
Si se pretende utilizar las imágenes de videograbación con fines de control laboral, deberá informarse al los trabajadores de forma previa.	
	Cuando las grabaciones del sistema grabación vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

[VID.01.I]	EJERCICIO DE DERECHOS
Se garantizará el ejercicio de los derechos de acceso de los interesados a las videograbaciones.	
	Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso
	No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

[VID.01.J]	PRESTADOR DE SERVICIOS DE VIDEOVIGILANCIA
Si los servicios de videovigilancia son contratados a un tercero, se deberá dar cumplimiento al Artículo 28 del Reglamento General de Protección de Datos	
	Se deberá elegir únicamente un prestador de servicios que ofrezca suficientes garantías para aplicar las medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento General de Protección de Datos y garantice la protección de los derechos del interesado.
	El prestador de servicios no recurrirá o otro prestador de servicios tercero con objeto de subcontratación sin la autorización previa por escrito, específica o general, de la organización responsable. En caso de que sea autorizada la subcontratación, el prestador de servicios será responsable de transmitir al tercero las instrucciones y obligaciones establecidas por la organización responsable.
	Se deberá celebrar una contrato u otro acto jurídico que vincule al prestador de servicios con la organziación y que establezca el objeto, la duración, la naturaleca y la finalidad del tratamiento de los datos, el tipos de los datos personales y las categorías de interesados, y las obligaciones y derechos de la organización responsable.
	El prestador de servicios únicamente tratará las imagenes de videovigilancia únicamente siguiendo las instrucciones documentadas de la organización responsable.
	Se deberá garantizar que todas las personas autorizadas para tratar los datos personales por parte del prestador de servicios se hayan comprometido a respetar la confidencialidad.
	El prestador de servicios deberá demostrar que ha adoptado las medidas de seguridad técnicas y organizativas que garanticen la integridad, disponibilidad y confidencialidad de la información.
	El prestador de servicios deberá ayudar a la organización responsable a demostrar el cumplimiento de la normativa de protección de datos.
	Se deberá determinar la forma de devolución o forma de destrucción de los datos a la finalización de la prestación de servicios.