Política de Seguridad de la Información

Versión Pública

Norma ISO/IEC 27001:2022
Reglamento General Europeo 679/2016 de
Protección de Datos de Carácter Personal
Ley Orgánica 3/2018, de Protección de Datos Personales
y Garantía de los Derechos Digitales

REAL CLUB PINEDA
SEVILLA

21 de abril de 2025

ÍNDICE DE CONTENIDOS

1. OBJETIVO, ALCANCE Y VERSIÓN 4
1.1. OBJETIVO 4
1.2. ALCANCE 4
1.3. VERSIÓN 4
2. ENTORNO CORPORATIVO 4
3. POLÍTICA GESTIÓN CONTRASEÑAS 5
4. UTILIZACIÓN DEL EQUIPO INFORMÁTICO Y DE COMUNICACIONES 6
4.1. USOS ESPECÍFICAMENTE PROHIBIDOS 6
4.2. NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE INFORMACIÓN 6
4.3. NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y MÓVILES 7
4.4. USO DE DISPOSITIVOS PERSONALES (BYOD) 7
4.5. NORMAS ESPECÍFICAS PARA MEMORIAS USB, CDs y DVDs 8
4.6. IMPRESORAS EN RED, FOTOCOPIADORAS Y DIGITILIZACIÓN DE DOCUMENTOS 8
4.7. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL 8
4.8. PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS 9
4.9. SALIDA DE SOPORTES FUERA DE LAS INSTALACIONES DEL CLUB 9
4.10. VIDEOCONFERENCIAS 9
4.11. PIZARRAS Y FLIPCHARTS 10
4.12. POLÍTICA DE USO DE LA INTELIGENCIA ARTIFICIAL 10
5. USO EFICIENTE DE EQUIPOS Y RECURSOS INFORMÁTICOS 10
5.1. ELIMINACIÓN AUTOMÁTICA DE ARCHIVOS Y METADATOS 11
6. ACCESO Y PERMANENCIA DE TERCERAS PERSONAS EN LAS INSTALACIONES 11
7. CONFIDENCIALIDAD DE LA INFORMACIÓN 12
8. TRATAMIENTO DE LA INFORMACIÓN 13
9. CLASIFICACIÓN DE LA INFORMACIÓN 13
10. CONEXIÓN DE DISPOSITIVOS A LAS REDES DE COMUNICACIONES 14
11. USO DEL CORREO ELECTRÓNICO CORPORATIVO 14
11.1. NORMAS GENERALES 14
11.2. USOS ESPECIALMENTE PROHIBIDOS 15
11.3. RECOMENDACIONES ADICIONALES 15
12. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN 16

12.1. NORMAS GENERALES 16
12.2. USOS ESPECÍFICAMENTE PROHIBIDOS 16
12.3. ACCESOS REMOTOS 16
13. DESCONEXIÓN DIGITAL 17
14. INCIDENCIAS DE SEGURIDAD 17
15. COMPROMISOS DE LAS PERSONAS USUARIAS 17
16. USO ABUSIVO DE LOS SISTEMAS DE INFORMACIÓN. 18
17. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA 18
18. RÉGIMEN DISCIPLINARIO 19
19. APROBACIÓN Y ENTRADA EN VIGOR 20

1. OBJETIVO, ALCANCE Y VERSIÓN

1.1. OBJETIVO

El objetivo de esta Política de Seguridad es garantizar la seguridad de toda la información estableciendo las medidas organizativas, técnicas, físicas y legales, necesarias para proteger los activos de información del REAL CLUB PINEDA DE SEVILLA contra accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo o mal uso, que se pueda producir de forma intencionada o accidental.

1.2. ALCANCE

Esta política es aplicable y de obligado cumplimiento para toda persona usuaria del REAL CLUB PINEDA DE SEVILLA que pueda realizar cualquier tratamiento de datos de carácter personal o pueda acceder a las instalaciones donde se traten dichos datos, así como cualquier tipo de información, incluyendo los proveedores externos, cuando utilicen los Sistemas de Información de la entidad, así como cualquier otra parte interesada.

En el ámbito de la presente normativa, se entiende por persona usuaria cualquier persona empleada perteneciente o ajeno la entidad, así como personal de organizaciones públicas o privadas externas, entidades colaboradoras, profesionales y autónomos y autónomas, o cualquier otra persona con algún tipo de vinculación con el REAL CLUB PINEDA DE SEVILLA y que utilice o posea acceso a los Sistemas de Información del Club.

1.3. VERSIÓN

Esta versión de la Política está disponible públicamente y su acceso no está restringido. El REAL CLUB PINEDA DE SEVILLA se compromete a mantener la transparencia en sus prácticas y proporciona esta versión accesible para garantizar que todas las partes interesadas, tanto internas como externas, tengan conocimiento y comprensión de las medidas adoptadas para salvaguardar la seguridad y la integridad de los datos. Valoramos la confianza de nuestros socios, proveedores y demás partes interesadas, por lo que nos esforzamos en ofrecer esta información de forma abierta y accesible para promover la transparencia en nuestra gestión de datos.

2. ENTORNO CORPORATIVO

El tratamiento de datos personales por las personas usuarias se hará siguiendo las directrices indicadas en el PROTOCOLO INTERNO DE PROTECCIÓN DE DATOS, así como la normativa aneja, y siempre utilizando los medios y sistemas específicos dispuestos para ello. Fuera de estos medios establecidos, no podrán tratar datos de carácter personal.

Las personas usuarias están obligadas a cumplir con el principio de seguridad de los datos, garantizando la integridad (impidiendo que la información pueda ser alterada de manera

incorrecta y sin autorización previa) y confidencialidad (los datos solamente pueden ser conocidos por aquellas personas autorizadas para ello) en todo momento de los mismos.

3. POLÍTICA GESTIÓN CONTRASEÑAS

Todas las personas empleadas y terceros con acceso a sistemas del REAL CLUB PINEDA DE SEVILLA deberán utilizar un gestor de contraseñas aprobado por la organización, con el fin de evitar contraseñas débiles o reutilizadas. Se realizarán auditorías periódicas para verificar su uso, y se elaborará un informe trimestral sobre su adopción y posibles riesgos detectados.

Asimismo, se empleará una herramienta de control de inventario en tiempo real para gestionar los dispositivos tecnológicos y detectar posibles equipos no autorizados. Esta herramienta permitirá también aplicar actualizaciones y ofrecer soporte remoto.

Todos los dispositivos utilizados en la organización deberán contar con soluciones de protección activa frente a malware y amenazas avanzadas. Estas soluciones permitirán detectar y neutralizar ataques de forma automática.

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos y son, por tanto, protegidas especialmente. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales. Por ello, cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al responsable de seguridad técnico y subsanada en el menor plazo de tiempo posible. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos y servicios de nuestra entidad.

Recomendaciones generales

- ✓ **No utilizar las contraseñas por defecto.**
- ✓ **Doble factor para servicios críticos.**
- ✓ **No compartir las contraseñas con nadie.**
- ✓ **Utilizar distintas contraseñas para servicios diferentes.**
- ✓ **Cambiar las contraseñas periódicamente.**
- ✓ **No hacer uso del recordatorio de contraseñas.**

4. UTILIZACIÓN DEL EQUIPO INFORMÁTICO Y DE COMUNICACIONES

La organización facilitará a las personas usuarias que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la entidad ponga a disposición de las personas usuarias deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

Los medios electrónicos corporativos son exclusivamente herramientas de trabajo y sólo pueden emplearse para esta finalidad.

4.1. USOS ESPECÍFICAMENTE PROHIBIDOS

Están terminantemente prohibidos los siguientes comportamientos:

1. Ejecución remota de archivos de tipo audiovisual (música, vídeo, animaciones, etc.).
2. Utilización de cualquier tipo de software dañino.
3. Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
4. Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la organización.
5. Instalación y utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

4.2. NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE INFORMACIÓN

Se recomienda trabajar en el servidor o, en caso de hacerlo en local, se recomienda a los usuarios la realización de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.

No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales.

Se entiende por fichero temporal, aquel generado exclusivamente para la realización de trabajos temporales o auxiliares, con objeto de atender a unas finalidades concretas y limitadas en el tiempo.

Dichos ficheros deberán ser borrados o destruidos una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Los ficheros temporales que se generen en el desarrollo de la actividad, se guardarán y almacenarán por los usuarios en las Carpetas de Red habilitadas al efecto. Está prohibido almacenar este tipo de ficheros en el disco duro de los ordenadores de las personas usuarias, debido al riesgo existente de pérdida de información y falta de actualización de los mismos, al no estar sometidos estos ficheros a los procesos de copia de seguridad correspondientes.

4.3. NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y MÓVILES

1. Este tipo de dispositivos estará bajo la custodia de la persona usuaria que los utilice, debiendo adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas, incluidas otros usuarios de la organización.
2. La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de la entidad.
3. Los equipos portátiles y móviles deberán utilizarse únicamente para fines profesionales autorizados, especialmente cuando se usen fuera de las instalaciones.
4. En general, los equipos portátiles no deberán conectarse directamente a redes externas (con excepción de la red o el acceso a Internet del usuario/a en su domicilio). El REAL CLUB PINEDA DE SEVILLA proporcionará accesos remotos.
5. Para el teletrabajo, la conexión deberá realizarse exclusivamente conforme al procedimiento establecido por el área técnica, asumiendo que cualquier red externa es potencialmente insegura.
6. El uso de conexiones alternativas requerirá autorización previa y el cumplimiento de las medidas de seguridad indicadas por la entidad.

4.4. USO DE DISPOSITIVOS PERSONALES (BYOD)

Existen ciertos riesgos que debemos conocer antes usar los dispositivos personales en el ámbito corporativo:

- La exposición a redes inseguras en el ámbito personal. La conexión a este tipo de redes 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.

4.5. NORMAS ESPECÍFICAS PARA MEMORIAS USB, CDs y DVDs

1. Con carácter general, el uso de memorias USB, CDs o DVDs, no está autorizado. La salida de soportes con información fuera de las instalaciones del REAL CLUB PINEDA DE SEVILLA, deberá ser previamente autorizada por el Delegado de Protección de Datos (DPD).
2. Por razones de seguridad, los interfaces USB, CDs o DVDs, de los puestos de trabajo estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por la persona usuaria y requerirá la previa autorización del Delegado de Protección de Datos.

4.6. IMPRESORAS EN RED, FOTOCOPIADORAS Y DIGITILIZACIÓN DE DOCUMENTOS

1. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. En ningún caso la persona usuaria podrá hacer uso de impresoras y/o fotocopiadoras que no hayan sido proporcionados por la organización y, en su consecuencia, estén debidamente inventariados.
2. Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.
3. Si se encontrase documentación abandonada, la persona usuaria intentará localizar a su propietario/a para que la recoja inmediatamente. Caso de no encontrar a su titular, lo pondrá inmediatamente en conocimiento del Compliance Officer o del Delegado de Protección de Datos.
4. Cuando los documentos con datos personales pierdan la finalidad para la que fueron tratados, deberán ser eliminados en las máquinas destructoras o desechados en los contenedores de destrucción de documentación, de forma que no sea recuperable la información que pudieran contener.

4.7. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

1. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información sin la correspondiente licencia de uso.
2. Los programas informáticos propiedad de la organización están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa del Responsable de Seguridad Técnico.

3. Asimismo, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual.

4.8. PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS

El REAL CLUB PINEDA DE SEVILLA está profundamente comprometido con la defensa de la dignidad personal, la privacidad e intimidad, y los demás derechos personales de todas aquellas personas que lo componen, manteniendo un entorno laboral en el que no existan situaciones discriminatorias o de acoso, y se respeten los principios y valores éticos generales establecidos en el CÓDIGO ÉTICO vigente.

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

Asimismo, no se permiten discriminaciones respecto a la raza, origen, nacionalidad, religión, sexo, edad, orientación sexual o ideología de otro/a empleado/a, socio/a o terceras partes. Tampoco puede existir ningún tipo de conductas de acoso, ni laboral ni sexual.

Ante cualquier situación de falta de respeto a la legalidad, los usuarios deberán informar al Club mediante el CANAL DE DENUNCIAS establecido al efecto en la dirección web https://www.rzs.es/canal-denuncias/.

4.9. SALIDA DE SOPORTES FUERA DE LAS INSTALACIONES DEL CLUB

El tratamiento de datos de carácter personal fuera de las instalaciones del REAL CLUB PINEDA DE SEVILLA, tiene que ser expresamente autorizado, de forma previa, por el Delegado de Protección de Datos, conforme al procedimiento establecido en el PROTOCOLO INTERNO DE PROTECCIÓN DE DATOS.

4.10. VIDEOCONFERENCIAS

En videoconferencias, antes de compartir pantalla, la persona usuaria deberá asegurarse de ocultar cualquier información relacionada con la organización. Asimismo, deberá evitar que en el campo de visión de la cámara aparezcan documentos u otros elementos que puedan comprometer la seguridad de la información o la imagen de la entidad.

4.11. PIZARRAS Y FLIPCHARTS

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

4.12. POLÍTICA DE USO DE LA INTELIGENCIA ARTIFICIAL

El REAL CLUB PINEDA DE SEVILLA reconoce el valor de la Inteligencia Artificial (IA) para mejorar procesos, decisiones y servicios. No obstante, su uso debe realizarse de forma responsable, ética y conforme a la normativa vigente, especialmente en materia de protección de datos y transparencia.

La entidad se compromete a garantizar que todas las aplicaciones de IA se utilicen con seguridad, respetando los derechos fundamentales y aplicando las medidas necesarias para prevenir riesgos. Entre estos riesgos se incluyen el uso indebido de datos personales, sesgos en los resultados, fallos de seguridad, decisiones poco fiables o incumplimiento legal.

Para reducir estos riesgos, se aplicarán controles técnicos y organizativos que garanticen el cumplimiento normativo, la protección de la información y la fiabilidad de los sistemas. También se promoverá la formación del personal y se establecerá un Comité de Ética para supervisar el uso de estas tecnologías.

La IA podrá emplearse en tareas como la gestión interna, el análisis de datos o la mejora de servicios, siempre que se garantice la seguridad, la legalidad y la equidad. No se permitirá su uso en actividades que pongan en riesgo la privacidad, generen discriminación o afecten a derechos fundamentales sin una evaluación previa.

Todos los miembros del personal deberán seguir esta política, participar en las formaciones previstas y actuar de forma responsable. La entidad realizará controles y auditorías periódicas para asegurar el buen funcionamiento y cumplimiento normativo de los sistemas de IA, aplicando medidas correctivas si es necesario.

5. USO EFICIENTE DE EQUIPOS Y RECURSOS INFORMÁTICOS

Dentro del REAL CLUB PINEDA DE SEVILLA se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de las personas usuarias:

1. Apagar el ordenador al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
2. Imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color.

3. Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todo el personal, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.

5.1. ELIMINACIÓN AUTOMÁTICA DE ARCHIVOS Y METADATOS

El REAL CLUB PINEDA DE SEVILLA aplica una política de eliminación automática de archivos temporales, de la carpeta de descargas y de la papelera de reciclaje, con el fin de optimizar el almacenamiento y reforzar la seguridad de la información.

Esta medida se aplica a todos los sistemas utilizados por el personal, y no puede ser modificada por las personas usuarias. Los archivos temporales se eliminan semanalmente si no han sido utilizados recientemente, los archivos en la carpeta de descargas se eliminan tras 30 días sin abrirse, y la papelera se vacía automáticamente cada 90 días.

Es responsabilidad de cada persona usuaria guardar en ubicaciones permanentes los archivos que necesite conservar antes de que se cumplan los plazos de eliminación. En caso de pérdida de un archivo relevante, deberá notificarse de inmediato al área correspondiente para su evaluación y posible recuperación.

Asimismo, todo el personal y/o terceros que trabajen con el REAL CLUB PINEDA DE SEVILLA, deberá eliminar los metadatos de todos los documentos y archivos que gestione y se compartan fuera de la organización, con el objetivo de proteger la privacidad, evitar la divulgación de información sensible y cumplir con la normativa de protección de datos. La eliminación se realizará utilizando herramientas autorizadas, asegurando que no interfieran con los sistemas de protección de datos existentes.

Se ofrecerá formación periódica a las personas empleadas sobre cómo eliminar correctamente los metadatos y se actualizarán los procedimientos conforme a los avances tecnológicos.

Además, los archivos subidos a la web corporativa serán limpiados automáticamente mediante un sistema programado que elimina metadatos. Cualquier incumplimiento será registrado y gestionado conforme al PROTOCOLO DE BRECHAS DE SEGURIDAD.

6. ACCESO Y PERMANENCIA DE TERCERAS PERSONAS EN LAS INSTALACIONES

Aquella persona ajena que, eventualmente, permanezcan en las instalaciones del Club, deberán observar las siguientes normas:

1. En caso de que deba temporalmente acceder a los Sistemas de Información deberá hacerlo siempre bajo la supervisión de persona acreditada de la organización y previa autorización del Delegado de Protección de Datos.

2. Cualquier incidencia que surja en el transcurso del acceso a las instalaciones del Club deberá ponerlo en conocimiento del Responsable de Seguridad Técnico, del Compliance Officer o del Delegado de Protección de Datos.
3. Para los accesos a los sistemas de información, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.
4. Tales personas, en lo que les sea de aplicación, deberán cumplir puntualmente la presente POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, así como cualquier otra Política o Protocolo afín al mismo, con especial indicación del PROTOCOLO INTERNO DE PROTECCIÓN DE DATOS vigente en el REAL CLUB PINEDA DE SEVILLA.
5. Una vez en el interior de las instalaciones del Club, las personas ajenas sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado.
6. En todo caso atenderán los requerimientos que le hiciere el personal de control y seguridad.

7. CONFIDENCIALIDAD DE LA INFORMACIÓN

Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. A fin de dar debido cumplimiento de la misma, es obligatoria la observancia de las siguientes indicaciones:

a) Como medida de protección de la información tratada por la organización, está terminantemente prohibido el envío al exterior de información por cualquier medio tecnológico. La salida de información al exterior deberá estar autorizada en todo caso por el Delegado de Protección de Datos.

b) Todo el personal de la organización, propio o ajeno a la misma que hubiere tenido acceso a información gestionada por la entidad (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

c) Las personas usuarias sólo podrán acceder a aquella información para la que tengan la debida autorización, no pudiendo en ningún caso acceder a información perteneciente a otras personas usuarias o departamentos para los que no se posea tal autorización.

d) Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base al principio de mínimo privilegio.

e) La información contenida en los Sistemas de Información es propiedad del REAL CLUB PINEDA DE SEVILLA, por lo que las personas usuarias deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceras

personas (externas o internas no autorizadas) dicha información, salvo autorización expresa del Delegado de Protección de Datos.

f) Los soportes de información que vayan a ser reutilizados o desechados deberán ser previamente tratados para eliminar permanentemente la información que pudieran contener, de manera que resulte imposible su recuperación.

8. TRATAMIENTO DE LA INFORMACIÓN

Queda prohibido con carácter general transmitir o alojar información con datos personales en servidores externos a la organización, incluida cualquier aplicación de Cloud Computing o servicios en la nube, salvo aquellos previamente autorizados por el Delegado de Protección de Datos, tras evaluación de conformidad realizada por el servicio técnico.

9. CLASIFICACIÓN DE LA INFORMACIÓN

Para aplicar las medidas de seguridad ajustadas a cada activo de información hay que clasificarla, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidencialidad, integridad y disponibilidad.

Atendiendo al nivel de accesibilidad o confidencialidad, en el REAL CLUB PINEDA DE SEVILLA se establece la siguiente clasificación:

- **Confidencial**. Accesible solo por la alta dirección. La información Confidencial deberá ser etiquetada como tal y no podrá ser compartida con ningún usuario/a distinto del destinatario/a. En caso que la técnica lo permita, deberá cifrarse la información.
- **Restringido**. Sólo accesible para usuarios/as de la organización. La información no podrá ser compartida con ningún usuario/a distinto del destinatario/a.
- **Interna**. Accesible solo a usuarios/as de la organización. La información podrá ser compartida con otros usuarios/as pertenecientes a la organización, si no se le ha dado un carácter restringido.
- **Pública**. Accesible públicamente.

10. CONEXIÓN DE DISPOSITIVOS A LAS REDES DE COMUNICACIONES

No se podrá conectar en la red de comunicaciones corporativa ningún dispositivo distinto de los admitidos, habilitados y configurados por la organización, salvo autorización previa del Responsable de Seguridad Técnico.

11. USO DEL CORREO ELECTRÓNICO CORPORATIVO

Normas de uso de obligado cumplimiento:

11.1. NORMAS GENERALES

1. Todas las personas usuarias que lo precisen para el desempeño de su actividad profesional dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.
2. Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por la organización.
3. El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, quedando totalmente prohibido el uso privado del mismo.
4. Se deberá notificar al Responsable de Seguridad Técnico, cualquier tipo de anomalía detectada, así como los correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas. El Responsable de Seguridad Técnico notificará la incidencia al Delegado de Protección de Datos para el registro de la misma.
5. Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la procedencia de los mismos, se deberá notificar esta circunstancia al Responsable de Seguridad Técnico, quien notificará a su vez al Delegado de Protección de Datos para el registro de la incidencia.
6. Verificar por otras fuentes la procedencia de los correos sospechosos. Los ciberdelincuentes pueden suplantar la identidad de algún miembro del REAL CLUB PINEDA DE SEVILLA, mediante correo electrónico, mensajería, redes sociales, o incluso llamadas telefónicas, con la finalidad de filtrar datos confidenciales de nuestra entidad, por lo que es sumamente importante verificar la identidad de cada persona al transferir y compartir información. Dicha suplantación de identidad por parte de los ciberdelincuentes también puede darse con proveedores o cualquier otra parte interesada, incluido socios, socias y colaboradores, por lo que por prevención se comprobará el contenido por medio distinto al sospechoso.

7. Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo legalmente establecido. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

11.2. USOS ESPECIALMENTE PROHIBIDOS

Las siguientes actuaciones están explícita y especialmente prohibidas:

1. El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a las personas usuarias, identidad e imagen corporativa y a los propios sistemas de información de la organización.
2. El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.
3. La difusión de la cuenta de correo de la persona usuaria en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional de dicha persona usuaria.
4. Responder mensajes de los que se tenga sospechas sobre su autenticidad y contenido, o mensajes que contengan publicidad no deseada.
5. La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información confidencial.
6. La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a la organización o el reenvío automático del correo corporativo a buzones ajenos a la organización.

11.3. RECOMENDACIONES ADICIONALES

1. Hay que asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a las personas destinatarias apropiadas.
2. Los buzones de correo se configuran con un tamaño para almacenamiento limitado. El sistema indicará cuándo se encuentra al límite de su capacidad, tras el cual no se permitirá enviar y recibir correos. Es importante en este aspecto seguir las pautas indicadas en el PROTOCOLO DE CONSERVACIÓN DE DATOS en lo referente al correo electrónico, por el cual todos aquellos correos que hayan perdido la finalidad para la que fueron tratados y expirado el plazo legal de conservación, deberán ser suprimidos.

12. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

La organización velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

12.1. NORMAS GENERALES

1. Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
2. Sólo se podrá acceder a Internet mediante el navegador configurado por el Responsable de Seguridad Técnico en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización de aquél.
3. Deberá notificarse al Responsable de Seguridad Técnico cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso, quien lo pondrán en inmediato conocimiento del Delegado de Protección de Datos.

12.2. USOS ESPECÍFICAMENTE PROHIBIDOS

Quedan prohibidas las siguientes actuaciones:

1. La descarga de programas informáticos sin la autorización previa del Responsable de Seguridad Técnico, o la de ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio web visitado es confiable.
2. El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

12.3. ACCESOS REMOTOS

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

En la actualidad, todas las comunicaciones que se realizan fuera de las instalaciones del REAL CLUB PINEDA DE SEVILLA se realizan a través de RDS (Remote Desktop Services) y VPN que garantiza un nivel equivalente al acceso en modo local.

13. DESCONEXIÓN DIGITAL

En el REAL CLUB PINEDA DE SEVILLA garantizamos el derecho a la desconexión digital del personal empleado, conforme a lo establecido en la POLÍTICA INTERNA DERECHO A LA DESCONEXIÓN DIGITAL Y TRABAJO A DISTANCIA. Este derecho faculta a sus titulares a limitar el uso de las tecnologías de la comunicación fuera del horario de trabajo, garantizando el tiempo de descanso y vacacional en cada caso.

El ejercicio de esta facultad se reconoce en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio de la persona empleada que está vinculada al uso con fines laborales de las pertinentes herramientas y medios electrónicos.

En algunos casos, este descanso puede ser interrumpido por diferentes causas que lo justifiquen: fuerza mayor, extraordinaria necesidad, o diferentes posibilidades en función del nivel de responsabilidad y funciones de cada persona usuaria.

14. INCIDENCIAS DE SEGURIDAD

Cuando cualquier persona usuaria detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información, deberá informar inmediatamente al Responsable de Seguridad Técnico, al Compliance Officer o al Delegado de Protección de Datos.

15. COMPROMISOS DE LAS PERSONAS USUARIAS

1. Es responsabilidad directa de las personas usuarias:
    - Custodiar las contraseñas que se le proporcionen y seguir todas las recomendaciones de seguridad vigente.
    - Cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.
    - Garantizar la disponibilidad de toda la información importante alojada en su equipo, para lo que deberá realizar la correspondiente copia en los servidores corporativos.

2. Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos para desarrollar actividades que persigan o tengan como consecuencia:

- El uso intensivo de recursos, memoria, almacenamiento o comunicaciones, para usos no profesionales.
- La destrucción o modificación no autorizada de la información, de manera premeditada.
- La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
- El deterioro intencionado del trabajo de otras personas.
- Dañar intencionadamente los recursos informáticos de la organización.
- Incurrir en cualquier otra actividad ilícita, sea del tipo que sea.

16. USO ABUSIVO DE LOS SISTEMAS DE INFORMACIÓN.

Desde el REAL CLUB PINEDA DE SEVILLA defendemos el derecho a la libertad de expresión, de ideas u opiniones, pero el uso indebido de Internet fuera del lugar de trabajo o fuera del horario laboral, puede provocar a la organización riesgos legales, de reputación o seguridad.

Por tal motivo, en ningún caso se puede compartir en las redes corporativas, información o documentación confidencial o no permitida, salvo supuestos excepcionales, previa y debidamente autorizados por el responsable que corresponda.

Si decide publicar opiniones personales en Internet, deberá tener en cuenta el sentido común con la debida precaución de no hablar en nombre del REAL CLUB PINEDA DE SEVILLA.

En el uso de las redes sociales (Facebook, LinkedIn, Twitter, WhatsApp, Instagram, etc.), se recomienda que sea adecuado (no excesivo), prudente, pacífico y acorde con el CÓDIGO ÉTICO y los valores del REAL CLUB PINEDA DE SEVILLA.

17. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

1. La organización, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:
    - Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
    - Monitorizará los accesos a la información contenida en sus sistemas.
    - Auditará la seguridad de las contraseñas y aplicaciones.
    - Monitorizará los servicios de Internet, correo electrónico y otras herramientas de colaboración.

2. Se llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de las personas usuarias. En este sentido cabe indicar que el conflicto entre el derecho fundamental a la intimidad y al secreto de las comunicaciones establecido en el artículo 18 de la Constitución Española, y el derecho empresarial a ejercer un poder de vigilancia y control que garantice la buena marcha de la organización (artículo 20 del Estatuto de los Trabajadores), ha sido resuelta por la jurisprudencia de la Sala de lo Social del Tribunal Supremo en el sentido de avalar la legitimidad de la actuación empresarial que somete a vigilancia y control el uso de tales medios cuando previamente se ha dado a conocer a las personas empleadas la existencia de instrucciones y prohibiciones claras al respecto, sin que dicha vigilancia y control atente a los derechos fundamentales de la persona trabajadora.

3. Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa que motivó su bloqueo o suspensión desaparezca. Todas las personas usuarias, los directores y directoras de departamentos y demás partes interesadas, velarán por el cumplimiento escrupuloso de la presente POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, y pondrán en conocimiento del Responsable de Seguridad Técnico, del Compliance Officer o del Delegado de Protección de Datos, cualquier incumplimiento o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas, previo registro del incidente que corresponda.

4. El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o incumplimiento de las normas del presente documento.

5. El sistema que proporciona el servicio de conexión a Internet podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas con conexión no segura o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar al Responsable de Seguridad Técnico dichos accesos.

6. Con la presente Política se pretende delimitar el uso de los medios informáticos, redes de comunicaciones, telefonía y otros medios necesarios para las funciones profesionales, al objeto de que los usuarios no alberguen falsas expectativas de privacidad en el uso de dichos medios.

18. RÉGIMEN DISCIPLINARIO

El mal uso de las prácticas definidas en el presente documento podrá ser motivo de amonestación, sin perjuicio de la aplicación del régimen disciplinario correspondiente en cada supuesto, y/o la determinación de las acciones judiciales que procedan.

Es responsabilidad de todos los usuarios y partes interesadas, garantizar el cumplimiento de las disposiciones y conductas definidas en esta POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Cualquier usuario o parte interesada que tuviera conocimiento de alguna infracción de la presente Política, deberá comunicarla a través del CANAL DE DENUNCIA establecido al efecto, conforme se dispone en el CÓDIGO ÉTICO de nuestra entidad.

19. APROBACIÓN Y ENTRADA EN VIGOR

El REAL CLUB PINEDA DE SEVILLA aprueba por unanimidad la presente POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, en reunión de su Junta Directiva del día 22 de febrero de 2022, según consta en el acta correspondiente, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de la información de nuestra entidad, con el fin de que sea cumplida en su integridad por todas aquellas partes interesadas, y ordena su inmediato cumplimiento y supervisión periódica, entrando en vigor desde el día de la fecha su aprobación.