



GRANADA
Club de Fútbol

REGLAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN TEMPORADA 2022/2023



Programa de Cumplimiento Normativo				
Fecha edición	Documento	Páginas	Version	Area
10-05-23	Reglamento de TI.	26	v.1/22-23	Dr. IT
EN VIGOR				
CREADO POR CUMPLIMIENTO NORMATIVO				10-05-23
APROBADO POR EL CONSEJO DE ADMINISTRACIÓN				12-05-23
PUBLICADO				12-05-23
ACTUALIZACIÓN RECOMENDADA				30-06-24

Control de cambios:



1. INTRODUCCIÓN

El Granada Club de Fútbol, S.A.D. (en adelante, el “Club”) así como la Fundación G.C.F. 1931 (en adelante la “Fundación”) son conscientes de la necesidad de utilizar nuevas tecnologías, lo que requiere que ambas (o en adelante “GCF”) adopten medidas para un uso responsable de las mismas, a fin de proteger la seguridad del Club, la privacidad y los derechos fundamentales de nuestros trabajadores junto con las leyes de propiedad intelectual y la revelación de secretos.

La política de actuación en materia de Tecnologías de la Información (en adelante, “TIC”) persigue la incorporación de este uso responsable, especialmente para tratar de evitar que se sucedan delitos comprendidos en el Código Penal español, relativos a la violación de la intimidad personal y familiar, revelación de secretos, prostitución, explotación sexual y corrupción de menores, delitos contra la dignidad de las personas, delitos informáticos y delitos contra la propiedad intelectual.

Con el término genérico TIC se integran las redes, las herramientas informáticas, los terminales, los servicios, programas de ordenador y cualquier tecnología relacionada con la información, la comunicación virtual y las nuevas tecnologías. Habitualmente, dispositivos utilizados y aceptados por la entidad serán los siguientes:

- Ordenadores portátiles
- Ordenadores de sobremesa
- Tabletas
- Teléfonos inteligentes
- Videocámaras
- Scanner
- Fax
- Fotocopiadora
- Dispositivos encuadrados como Tecnologías de la Información
- Discos duros portátiles y dispositivos de almacenaje de información
- USB encriptados para responsables y uso cotidiano de oficina

A través de estos dispositivos se podrá acceder a los siguientes recursos corporativos del Club:

- Dirección de correo electrónico corporativo con el dominio usuario@granadacf.es o usuario@ext.grnadacf.es
- Redes de acceso a internet (cables y Wifi)
- Red oficinas
- Prensa, Patrocinadores y familiares jugadores dentro del Estadio
- Árbitros estadio
- Tiendas
- Ciudad Deportiva (prensa, oficina y exterior)



- Servidores para ficheros NAS controlados por usuarios
- Servidor para contabilidad

1.1. Ámbito de aplicación

El presente Reglamento va dirigido a todas las personas vinculadas al Club y a la Fundación, concretamente a miembros del Consejo de Administración, apoderados, representantes legales, directivos, jugadores, técnicos, empleados y colaboradores (en adelante, "Personas vinculadas"), y engloba las siguientes áreas de regulación:

1. Uso de las TICs propiedad del Club entregadas a las personas vinculadas.
2. Política de uso del correo electrónico.
3. Uso de las TICs propiedad de las personas vinculadas en las instalaciones del Club (BYOD.).
4. Uso de las TICs por terceros que presten servicios en las instalaciones del Club o que asistan a retransmisión de eventos, charlas, conferencias, ruedas de prensa, etc.
5. Acceso a redes WIFI o cable.

1.2. Uso de las TICs propiedad del Club y la Fundación entregadas a las personas vinculadas

El Club asigna al personal que lo requiera unos determinados equipos informáticos, medios electrónicos, teléfono y una cuenta de correo electrónica corporativa; en cuyos equipos se almacenan datos, debiendo estar vinculados con el Plan de Protección de Datos de carácter Personal.

A este respecto, se define "dato de carácter personal" como cualquier información que pueda identificarte o hacerte identificable (p. ej. el domicilio, retribuciones, fiscalidad, circunstancias personales y familiares, datos bancarios, aptitudes profesionales, reconocimientos médicos, afiliaciones sindicales, etc.) y, en general, cualquier otro dato o información que sea facilitada u obtenida por el GCF vinculado con cada persona.

La máxima de esta política es la protección de los datos de los empleados y miembros del Club y la Fundación y la información de los propios, razón por la cual el GCF prohíbe a sus empleados realizar las siguientes acciones:

- Apoderamiento, utilización, comunicación, o modificación de datos reservados de carácter personal o familiar que se encuentren registrados o archivados. Por ejemplo, acceder a información reservada de carácter personal a la que no se tenga autorización en función del perfil de acceso del empleado.
- Apoderarse de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales, así como interceptar comunicaciones de



cualquier modo con el fin de descubrir los secretos o vulnerar la intimidad de otro.

- Utilizar los datos obtenidos de terceros para finalidades ajenas a aquellas por las que estos han sido recabados. Los datos no pueden ser cedidos a otras empresas o terceros ni utilizados con una finalidad diferente de aquella para la que se pidieron salvo que se cuente con la oportuna autorización.
- Acceder por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo (por ejemplo, sistema de claves de ordenador o contraseñas) a datos o programas contenidos en un sistema informático.

Consecuentemente, este Reglamento tiene como finalidad regular:

- i. El uso de dispositivos propiedad del Club y la Fundación, entregados a las personas vinculadas (miembros del Consejo de Administración, apoderados, representantes, directivos, jugadores, técnicos y empleados) con fines profesionales, así como el uso de los dispositivos privados de los empleados para uso profesional.
- ii. La política de uso del correo electrónico corporativo por los destinatarios, con el fin de garantizar un uso correcto.
- iii. Informar de las obligaciones que asumen los destinatarios como las consecuencias de dicho uso.
- iv. Informar de la existencia de controles por parte del Club con la intervención mínima necesaria y solo para aquellos casos especificados.

Las personas vinculadas, respecto de las TIC propiedad del Club, asumen los siguientes compromisos:

- a. El uso de los dispositivos deberá destinarse únicamente a los fines profesionales para los que son entregados.
- b. Deberán autorizar la monitorización de estos dispositivos por el Club.
- c. Deberán responsabilizarse del uso y custodia del dispositivo, con el fin de impedir el acceso por parte de terceros no autorizados.
- d. Deberán configurar un sistema de identificación/autenticación para el acceso al dispositivo mediante la utilización de una contraseña, código PIN o mecanismo equivalente; el cual deberá ser modificado con cierta periodicidad siendo responsable de la custodia de contraseñas y claves de acceso. Cada 4 meses desde el Área de Informática se recordará a cada usuario el cambio de claves de acceso.



- e. Deberán bloquear el dispositivo cuando no esté siendo utilizado y configurar el bloqueo inmediato por inactividad.
- f. No facilitarán a otras personas los códigos y/o contraseñas de acceso y/o desbloqueo del terminal, ni las claves de acceso a los sistemas de información corporativa integrados en su dispositivo personal.
- g. No almacenarán información corporativa sensible en el dispositivo salvo que por razones de trabajo estén autorizados a almacenarlo.
- h. Deberán realizar copias de seguridad de la información corporativa que se almacene en el servidor, en su caso, con una periodicidad mínima semanal.
- i. Deberán seguir las instrucciones que facilite el Área de TI en relación a programas antimalware y/o antivirus y actualizaciones requeridas en el software.
- j. No instalarán ni reproducirán en el dispositivo programas informáticos o cualquier otro tipo de obra o material que infrinja derechos de propiedad intelectual o industrial. No instalarán software que promueva o permita, directa o indirectamente, la infracción de tales derechos.
- k. Comunicarán inmediatamente cualquier incidencia que pudiera afectar la información integrada en el dispositivo, tales como pérdida o sustracción del terminal, pérdida o borrado de información corporativa, etc.
- l. El uso de la red inalámbrica del Club únicamente puede utilizarse para aquellos servicios que estén autorizados. Sin la debida autorización, no se permite tener acceso directo a los servidores, copiar software o modificar los archivos que se encuentren allí.
- m. El uso que se dé a los servicios de Red estará circunscrito a fines exclusivamente propios del club para los que le han sido entregados los dispositivos.
- n. Está prohibido usar los dispositivos y servicios de Red para jugar, entrar en redes sociales personales, enviar o recibir información pornográfica o que tengan propósito comercial ajeno a la actividad del club.

No obstante lo anterior, el Área de Comunicación y Contenidos está autorizado a usar las redes sociales personales para la difusión de mensajes de interés para el Club. Igualmente, los responsables de cada Área están autorizados al uso de redes sociales personales para difundir noticias e información oficial del Club.

De igual manera, los jugadores y familiares están autorizados a utilizar sus dispositivos para jugar en la zona reservada para ello en Ciudad Deportiva.



- o. Queda prohibido capturar material audiovisual de personal del Club y sus instalaciones, quedando totalmente prohibido su difusión a través de internet, mensajería, correo electrónico, redes sociales, y similares, sin previa autorización. Cuando sea requerido para alguna actividad deberá autorizarse por el director del área correspondiente, quien deberá consultar al responsable de los servicios jurídicos.
- p. Queda prohibido borrar, dañar, deteriorar, suprimir o hacer inaccesibles, datos, programas informáticos o documentos electrónicos ajenos o de terceros (como por ejemplo, enviar virus informáticos a terceros a través de los sistemas del Granada CF o destruir por cualquier medio informático las bases de datos de un tercero).
- q. Obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno.
- r. Se deberá informar inmediatamente del mal funcionamiento de los dispositivos o red inalámbrica.
- s. Deberán asegurarse del debido orden, limpieza y cuidado de los equipos al terminar de usarlos, incluyendo apagarlos adecuadamente y dejar el puesto de trabajo limpio y ordenado.
- t. En horario laboral, así como en aquellos momentos en los que se atienda a medios de comunicación o durante el trascurso de los entrenamientos, queda prohibido el uso de los dispositivos y TIC para utilización personal, como puede ser redes sociales, mensajería, reproducciones, descargas, etc. que impidan el correcto desempeño de la labor encomendada.

No obstante lo anterior, los jugadores y técnicos podrán hacer uso de sus redes sociales una vez finalizado el entrenamiento o partido.

- u. La utilización de los recursos fuera del horario laboral se registrará por las mismas reglas y deben estar debidamente autorizados.
- v. Como norma general, el Trabajador respetará siempre las normas del Club en lo referente a las nuevas tecnologías y específicamente en cuanto a cuestiones de seguridad informática; para ello seguirá las directrices que el Área de IT tenga establecidas y cualquiera otras que se consideren necesarias por parte del Club, siendo responsabilidad del Trabajador cualquier trasgresión de las citadas normas.
- w. Cuando el usuario de un número telefónico del Club cree una cuenta de WhatsApp siempre utilizará una imagen corporativa y no personal.

1.3. Cuidado y protección de los elementos TICs propiedad del Club.



El trabajador o trabajadora que tenga asignado unos determinados equipos informáticos, medios electrónicos o teléfono propiedad del Club, es responsables del buen uso, conservación y cuidado de los mismos.

Para el supuesto que estos equipos sufran algún desperfecto, daño o alteración de su estructura original, el destinatario deberá informar inmediatamente del hecho al departamento TIC del Club. En esta información deberá recoger con todo detalle el lugar, hora, fecha, daños observados, detalle de cómo se han producido los daños y testigos del incidente.

En función de la información facilitada, el Club valorará la situación sobre dolo, negligencia o culpa del trabajador en los hechos y determinará, el carácter fortuito o voluntario del incidente que ocasiona los daños.

Para el supuesto que el trabajador o trabajadora provoque daños intencionadamente en los equipos informáticos, medios electrónicos, y teléfonos propiedad del Club, el trabajador será responsable de la reparación de los daños o la restitución de los mismos.

De igual manera, la sustracción, pérdida o robo de los equipos informáticos, medios electrónicos, y teléfonos de propiedad del Club, será responsabilidad del trabajador, siempre que las circunstancias en las que ocurra sean debidas a una negligencia, descuido o distracción del mismo.

En todo caso, la negativa del trabajador o trabajadora a emitir un informe explicativo de los daños observados y los daños producidos, será considerada como una negligencia e intencionalidad en la provocación de los daños y, por tanto, serán el trabajador responsable de los mismos.

Los equipos informáticos, medios electrónicos, teléfono y cualquier dispositivo que sea propiedad del Club, serán entregados inmediatamente al Club en el momento en que la relación laboral sea extinguida por cualquier causa.

2. COMPROMISO CON EL RESPETO DE LOS DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL

Con el fin de promover el respeto a los derechos de Propiedad Intelectual e Industrial, tanto de la propia marca del Club, escudos y demás derechos como el respeto al derecho de terceros. Por ello, está prohibida la realización, entre otras, de las siguientes conductas:

- Distribución, plagio, reproducción o comunicación pública de obras literarias, artística o científica, es decir, cualquier tipo de documento, material gráfico, programa informático, etc. protegido sin la autorización del titular del derecho correspondiente. Por ejemplo, no se pueden copiar ni reutilizar informes de análisis de terceros, programas informáticos, o utilizar para incluir en



presentaciones o conferencias cualquier tipo de material (imágenes, textos, dibujos, etc.) sin la previa constancia de que el Granada CF ha obtenido los correspondientes derechos o licencias.

- Instalar o utilizar en los equipos informáticos que pone a disposición el Grupo, programas o aplicaciones sin contar con las oportunas licencias.
- Reproducir, imitar, modificar o usurpar de cualquier otro modo un signo distintivo idéntico o confundible de una tercera entidad, sin la autorización del titular del mismo, por ejemplo, incluir en presentaciones u otros documentos logos, imágenes o signos distintivos sobre los que el Granada CF no haya adquirido los correspondientes derechos.

3. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

3.1. Instrucciones generales de uso del correo electrónico.

El sistema de correo electrónico y de internet del Club, son propiedad de la Entidad y deberá ser utilizado por los usuarios conforme a la política interna de e-mail vigente en cada momento. El personal al servicio del tendrá la obligación de hacer un buen uso del correo electrónico.

Cada empleado que disponga asignada una cuenta de correo electrónico es usuario de los sistemas del Club y, por tanto, responsable de la cuenta de correo electrónico y las acciones que se realicen a través de la misma.

La cuenta de e-mail se facilita al empleado para el desempeño de las funciones laborales, por lo que la misma puede ser controlada y monitorizada –con la intervención mínima necesaria- en aquellos casos en los que sea necesario coordinar y garantizar la actividad laboral en los supuestos de ausencias laborales o bajas, la protección del sistema informático del Club y para la prevención de responsabilidades por un mal uso de este medio. Este control se realizará por el usuario y limitado a dos personas exclusivamente.

3.2. Usos permitidos y no permitidos del correo electrónico.

La cuenta de correo electrónico facilitada por el Club no puede emplearse con fines privados.

(Si la cuenta de correo electrónico profesional es utilizada por el usuario para fines privados, es consciente que el Club puede acceder a su información. No puede utilizarse la cuenta de correo electrónico para actividades profesionales ajenas a las tareas encomendadas por el Club).



El proveedor de correo web asegurará al Club que dispone y tiene establecidas políticas de privacidad y seguridad adecuadas, a través de las correspondientes cláusulas contractuales según recoge su contrato.

3.3. Usos no permitidos:

- El envío de correos masivos (spam) utilizando la dirección de correo electrónico corporativo, salvo las cuentas genéricas para el desarrollo de funciones comerciales y las destinadas a envío de información para abonados.
- El uso del correo electrónico corporativo vulnerando los derechos de terceros o del Club así como para la realización de actos de carácter ilícito.
- El uso del correo electrónico para el envío de información del Club, quedando únicamente autorizado el envío de información cuando sea necesario para el desempeño de las funciones. Cuando la información sea especialmente sensible, se enviará siempre encriptado.
- El uso de programas chat, redes sociales, mensajería instantánea, etc., durante la jornada laboral, salvo aquellas personas que por sus funciones requieran hacer uso de las mismas, en concreto los Responsables de Área y el personal del Área de Comunicación.

3.4 Gestión del buzón de correo electrónico.

Corresponde a cada usuario velar por una correcta y adecuada gestión de la información contenida en su correo electrónico. Para ello, el usuario tiene que revisar periódicamente la bandeja de entrada y, si procede, la de salida, como mínimo dos veces al día. En este sentido, se recomienda eliminar los mensajes que no deban conservarse y archivar el resto en la carpeta o subcarpeta apropiada, especialmente los que pueden tener un contenido personal o privado.

Los mensajes que formen parte de un procedimiento, u otros que deban conservarse, tienen que estar debidamente archivados en el expediente correspondiente, puesto que es previsible que se borren al cabo de un tiempo o se llegue a un tope de capacidad. El Área de IT enviará un recordatorio anual de limpieza de las máquinas.

Los correos electrónicos con fines privados deben ser borrados o movidos cada día por si es necesario hacer un traspaso o eliminación de la cuenta por motivos profesionales.

3.5 Adicionalmente, se fijan las siguientes normas:

- a) Utilizar la opción de reenviar solo en los casos en que la persona destinataria pueda acceder tanto al emisor del mensaje como a su contenido, y a toda la información de la cadena de correos que formen parte de él.



- b) Eliminar el pie de firma si se manda un mensaje privado desde el correo profesional.
- c) Revisar las direcciones de los destinatarios antes de enviar el mensaje.
- d) Valorar la utilización de la opción de copia oculta para enviar un correo electrónico a múltiples destinatarios.
- e) Con objeto de no difundir injustificadamente direcciones de correo de terceros al reenviar un correo electrónico, deberán eliminarse las direcciones de los destinatarios anteriores.
- f) Identificar de forma clara y concisa el asunto.
- g) No incluir datos personales en el asunto.
- h) Evitar palabras o expresiones que puedan activar los programas “anti-spam”.
- i) Revisar la posibilidad de revelar el contenido del mensaje antes de enviarlo.
- j) Emplear el pie de firma automático de los mensajes de correo electrónico, con arreglo al modelo corporativo establecido, que incluye la cláusula de confidencialidad. Cuando se trate de mensajes con fines personales, deberá suprimirse el pie de la firma.
- k) Organizar los mensajes enviados y recibidos en carpetas.
- l) Mantener la bandeja de entrada actualizada.
- m) Revisar la posibilidad de revelar el contenido de los archivos adjuntos antes de enviarlos.
- n) Evitar enviar archivos superiores a 30 Mb.

3.6. Medidas de seguridad

Los usuarios cumplirán las siguientes medidas de seguridad:

- i. Guardar el usuario y la contraseña de acceso a la cuenta de correo de forma segura y no facilitarlos a otras personas, ni siquiera a efectos de mantenimiento del sistema.
- ii. La contraseña es entregada por el Área de Sistemas al usuario y se solicitarán para su almacenamiento encriptados.
- iii. No utilizar una contraseña fácilmente deducible, debiendo tener un número mínimo de 8 caracteres con mayúsculas, minúsculas, caracteres y números.



- iv. Bloquear el acceso a la cuenta de correo y el equipamiento informático, en caso de ausentarse del puesto de trabajo durante la jornada.
- v. No seguir cadenas de mensajes piramidales.
- vi. No abrir mensajes sospechosos que puedan provocar daños en el sistema o en el equipo informático.
- vii. No enviar, reenviar o responder a mensajes de correo que contengan datos sensibles sin la autorización del responsable.
- viii. En caso de detectar una incidencia durante el uso del correo electrónico, el usuario debe ponerlo en conocimiento del responsable de seguridad de manera inmediata.
- ix. Cuando se adjunten datos que contengan información protegida (datos personales sobre ideología, afiliación, raza, sexo, vida laboral o médicos, bancarios, etc, será necesario utilizar las herramientas de cifrado de mensajes, enviando los archivos encriptados, según el método de encriptación.

3.7. Ausencias del usuario

En caso de ausencia programada superior a 3 días, el titular de la cuenta de correo deberá activar el mensaje de ausencia de oficina para facilitar otra dirección de contacto que garantice la continuidad de la actividad.

3.8. Extinción de la relación laboral

El Club suspenderá la cuenta de e-mail asignada al trabajador en el momento de finalizar la relación contractual con el empleado.

En estos casos, el trabajador tiene derecho a recuperar los mensajes personales de su cuenta de correo electrónico que se encuentran debidamente almacenados en la carpeta de mensajes personales que designe o que puedan identificarse como tales.

En todo caso, todos los mensajes del trabajador pueden analizarse con el fin de valorar si son necesarios para la continuidad de la actividad o su eliminación definitiva.

3.9. Desarrollo del trabajo fuera del puesto de trabajo

Cuando se utilice el correo electrónico facilitado por el Club fuera del puesto de trabajo, debe tenerse en cuenta lo siguiente:

- a) No guardar la contraseña de la cuenta de correo cuando se utilicen ordenadores de uso compartido.



- b) Borrar el historial de navegación y cerrar la sesión, al terminar, siempre que se utilice un ordenador de uso compartido para acceder al correo vía web.
- c) Utilizar programas antivirus.
- d) Utilizar usuario y contraseña para bloquear los dispositivos móviles desde donde pueda utilizarse el correo electrónico profesional.

3.10. Monitorización de la cuenta de correo electrónico y de los equipos informáticos por parte del club.

El Club puede hacer controles automatizados sobre el uso del correo electrónico para velar por el normal funcionamiento del sistema, pudiendo inspeccionar todos los e-mails enviados y recibidos, siempre y cuando sea necesario para preservar el interés del Club.

Solo se accederá al contenido de los mensajes o de los documentos adjuntos cuando no puedan utilizarse otros mecanismos menos intrusivos, concretamente en los siguientes casos:

- a) Para llevar a cabo tareas de mantenimiento o vinculadas a la seguridad del sistema. En tales casos, se informará a la persona trabajadora de las tareas que deben llevarse a cabo y se le ofrecerá la posibilidad de estar presente.
- b) Para comprobar, en relación con una información reservada o un procedimiento disciplinario, el uso del correo electrónico, en aquellos casos en los que haya indicios de que la persona trabajadora ha hecho un mal uso. El acceso debe hacerse en presencia de la persona trabajadora o de un representante del personal.
- c) En caso de ausencia del trabajador, el Club tomará las medidas necesarias respecto a los correos electrónicos entrantes, con el fin de garantizar la continuidad de las actividades.

3.11. Consecuencias del incumplimiento de la política de uso del correo electrónico.

El incumplimiento de las normas establecidas para el uso del correo electrónico con las cuentas de dominio establecido, será advertido por escrito al usuario, sin perjuicio de la aplicación, si procede del régimen disciplinario correspondiente y el cierre de la cuenta de correo por un mal uso de dicho servicio o cambio de contraseña provisionalmente o temporalmente.

4. USO DE LAS TICS PROPIEDAD DE LAS PERSONAS VINCULADAS EN LAS INSTALACIONES DEL CLUB (BYOD)

El Club permite que las personas vinculadas puedan utilizar sus propios dispositivos personales para fines profesionales a excepción del uso de ordenadores para fines



profesionales por cuestiones de seguridad y protección de las políticas de privacidad, protección de datos y confidencialidad, no se autoriza el uso de ordenadores personales para fines profesionales. Teniendo en cuenta esta excepción, se permite que el resto de dispositivos puedan conectarse a las redes corporativas.

Las siguientes normas tienen la finalidad de regular la política para el uso de los dispositivos personales con fines profesionales y establecen las reglas y los procedimientos necesarios de las personas vinculadas al Club para el uso de dispositivos personales como herramienta de trabajo, actualmente conocido como "Bring Your Own Device" o su acrónimo BYOD.

Una política BYOD es un conjunto de reglas que gobiernan los aspectos relacionados con el uso de dispositivos personales para acceder y utilizar recursos de la organización.

Las personas vinculadas durante el horario de trabajo:

- Deberán autorizar la monitorización de sus dispositivos por el Club sobre la parte de su dispositivo destinada a uso profesional.
- No entrar en páginas web que comporten un riesgo para la seguridad TIC de la entidad.
- Se realizará un uso responsable de los dispositivos personales cuando se utilicen en las instalaciones de la entidad para fines laborales.
- Deberán responsabilizarse del uso y custodia del dispositivo, con el fin de impedir el acceso por parte de los terceros no autorizados.
- Deberán configurar un sistema de identificación/autenticación para el acceso al dispositivo mediante la utilización de una contraseña, código PIN o mecanismo equivalente; el cual deberá ser modificado con cierta periodicidad.
- Deberán bloquear el dispositivo cuando no esté siendo utilizado y configurar el bloqueo inmediato por inactividad cuando el equipo se encuentre inactivo durante más de 2 minutos.
- No facilitarán a otras personas los códigos y/o contraseñas de acceso y/o desbloqueo del terminal, ni las claves de acceso a los sistemas de información corporativa integrados en su dispositivo personal.
- No almacenarán información corporativa no autorizada en el dispositivo, permitiendo realizar una copia de seguridad en los servicios contratados por el Club.
- El dispositivo deberá tener instalado versiones oficiales y preferiblemente actualizadas de programas antimalware y/o antivirus.



- No instalarán, ni reproducirán en el dispositivo programas informáticos o cualquier otro tipo de obra o material que infrinja derechos de propiedad intelectual o industrial. No instalarán software que promueva o permita, directa o indirectamente, la infracción de tales derechos.
- Comunicar inmediatamente cualquier incidencia que pudiera afectar la información integrada en su dispositivo, tales como pérdida o sustracción del terminal, pérdida o borrado de información corporativa, etc.
- El uso de la red inalámbrica del centro únicamente puede utilizarse para aquellos servicios que estén autorizados. Sin la debida autorización, no se permite tener acceso directo a los servidores, copiar software o modificar los archivos que se encuentren allí.
- El uso que se dé a los servicios de Red estará circunscrito a fines exclusivamente laborales o comprometidos contractualmente o a los medios de comunicación. Está tajantemente prohibido entrar a páginas web o servicios en red de contenido pornográfico o sensible.
- Está prohibido usar los dispositivos en la entidad y los servicios de Red de la entidad para jugar, entrar en redes sociales, enviar o recibir información pornográfica o que tengan propósito comercial ajeno a la actividad de la entidad. Los posibles usos personales del dispositivo (redes sociales, chats, etc) deberán realizarse en periodos de descanso.

Sólo se permite el acceso a redes sociales, chats, etc. aquellos trabajadores que por motivos profesionales tengan que divulgar información por estos medios, en concreto a los trabajadores destinados al Área de Comunicación y Contenidos.

- La utilización de los recursos de la entidad fuera del horario laboral se registrará por las mismas reglas y deben estar debidamente autorizados por el Club.
- Está prohibido capturar material audiovisual (fotos, audio, vídeos...), quedando totalmente prohibido su difusión a través de internet, mensajería, correo electrónico, redes sociales, y similares, sin previa autorización, pudiendo en caso contrario, ser constitutivo de delito. Cuando sea requerido para alguna actividad profesional será autorizada por el responsable del Área, previa consulta al responsable de servicios jurídicos.
- En horario laboral, así como en aquellos momentos en los que se atienda a medios de comunicación o durante el transcurso de los entrenamientos, queda prohibido el uso de los dispositivos y TIC para utilización personal, como puede ser redes sociales, mensajería, reproducciones, descargas, etc. que impidan el correcto desempeño de la labor encomendada.



5. USO DE LAS TICS POR TERCEROS QUE PRESTEN SERVICIOS EN LAS INSTALACIONES DEL CLUB O QUE ASISTAN A RETRASMISIÓN DE EVENTOS, CHARLAS, CONFERENCIAS, RUEDAS DE PRENSA, ETC. COMO PONENTES.

- a) Queda prohibido la función de cámara para capturar, grabar o transmitir audio, vídeo o fotos de los jugadores, técnicos o empleados aún con el permiso del sujeto de la foto o vídeo, así como su difusión, sin previa autorización del Club.
- b) Los asistentes como ponentes a charlas, conferencias, etc. deberán facilitar el contenido de su trabajo previamente a su exposición mediante dispositivo USB, DVD o similar, debiendo utilizar los ordenadores y dispositivos facilitados o autorizados por el Club, donde introducirán los referidos dispositivos previamente examinados para detectar virus o malware por personal de la entidad.
- c) Deberán responsabilizarse del uso y custodia de sus dispositivos, con el fin de impedir el acceso por parte de terceros no autorizados.
- d) Deberán configurar un sistema de identificación/autenticación para el acceso al dispositivo mediante la utilización de una contraseña, código PIN o mecanismo equivalente.
- e) Deberán bloquear el dispositivo cuando no esté siendo utilizado y configurar el bloqueo inmediato por inactividad.
- f) No facilitarán a otras personas los códigos y/o contraseñas de acceso y/o desbloqueo del terminal, ni las claves de acceso a los sistemas de información corporativa integrados en el dispositivo.
- g) No copiarán, moverán o almacenarán información corporativa en sus dispositivos o enviarán a dispositivos externos.
- h) Deberán garantizar que el dispositivo es seguro y limpio de riesgos o virus que puedan afectar a la TIC del Club.
- i) No instalarán, ni difundirán mediante sus dispositivos programas informáticos o cualquier otro tipo de obra o material que infrinja derechos de propiedad intelectual o industrial. No instalarán software que promueva o permita, directa o indirectamente, la infracción de tales derechos.
- j) El uso de las redes inalámbricas únicamente puede utilizarse para aquellos servicios que estén autorizados. Sin la debida autorización, no se permite tener acceso directo a los servidores, copiar software o modificar los archivos que se encuentren allí.



- k) El uso que se dé a los servicios de TIC en la entidad estarán circunscritos a fines exclusivamente autorizados. Está tajantemente prohibido entrar a páginas web o servicios en red para mayores de dieciocho años o de contenido pornográfico o sensible.
- l) Está prohibido usar los dispositivos en la entidad y los servicios de Red de la entidad para jugar, entrar en redes sociales, enviar o recibir información pornográfica o que tengan propósito comercial.
- m) Está prohibido capturar material audiovisual (fotos, audio, vídeos...) del Club, jugadores y empleados, quedando totalmente prohibido su difusión a través de internet, mensajería, correo electrónico, redes sociales, y similares, sin previa autorización.

6. ACCESO A REDES WIFI

Existen 3 redes WIFI desplegadas en El Estadio Nuevos los Cármenes y 2 en la Ciudad Deportiva. Las redes identificadas son seguras. y requieren las siguientes condiciones o autorizaciones para acceder:

Hay redes que surgen por la necesidad de facilitar servicios inalámbricos a los medios de comunicación y/o visitantes de las instalaciones, eliminando la necesidad de configurar certificados, usuarios o contraseñas y con ello la pérdida de algunas medidas de seguridad, permitiendo, únicamente, el acceso a internet.

6.1. Condiciones de uso

Las redes inalámbricas de acceso WIFI catalogadas como seguras, están únicamente al servicio del Club y sus empleados, no permitiendo las claves de acceso a personas ajenas al mismo. Las redes inalámbricas de acceso WIFI no seguras, están destinadas a facilitar servicio de internet a los visitantes y medios de comunicación.

6.2. Condiciones de acceso

El uso de las redes WIFI sólo está autorizado para el desarrollo de la actividad profesional, siendo responsabilidad del usuario realizar un uso lícito de la red.

No se puede realizar un uso de las redes para fines privados, ni está permitido su utilización para infringir la legislación vigente en cada momento, siendo responsabilidad exclusiva del usuario la utilización ilícita de las redes.

6.3. Monitorización y control

El Club se reserva el derecho a monitorizar y registrar la actividad que se realice a través de sus redes WIFI. Además, el acceso a internet podrá ser filtrado y controlado por el Área de informática del Club, no estando autorizado el uso de técnicas, sistemas o aplicaciones que permitan evitar dicho control.



7. MEDIDAS “ANTI-PHISHING”

7.1 Definición

“Phishing” es una forma de engaño mediante la cual los atacantes envían un mensaje (anzuelo) a una o a varias personas, con el propósito de convencerlas de que revelen sus datos personales. Generalmente, esta información es utilizada luego para realizar acciones fraudulentas como transferencias de fondos, compras u otros comportamientos delictivos que requieren el empleo de tales datos.

El medio más utilizado actualmente por los atacantes para realizar una acometida de “phishing” es el correo electrónico. Sus mensajes suelen ser muy convincentes, ya que simulan haber sido enviados por una entidad conocida y confiable para el usuario con la cual éste opera habitualmente.

En el mensaje se alegan motivos diversos, como problemas técnicos, actualización o revisión de los datos de una cuenta. A continuación, para –supuestamente- verificar o modificar sus datos personales, se le solicita que ingrese a un determinado sitio web: su nombre completo, DNI, claves de acceso, etc.

Son también usuales los casos en los que el usuario recibe un mensaje SMS en su teléfono celular o una comunicación en su contestador automático y hasta una llamada telefónica.

7.2 Medidas de prevención

1. Si algún trabajador o trabajadora del Club, miembro de la Fundación o persona relacionada recibe un correo electrónico, SMS o llamada telefónica que le pide información personal o financiera, no se debe responder salvo los casos contrastados. Si el mensaje además le invita a acceder a un sitio web a través de un enlace incluido en su contenido, queda prohibido el acceso al mismo, debiendo comunicarse directamente con la entidad o persona que, supuestamente le ha contactado.
2. No enviar información personal usando mensajes de correo electrónico sin utilizar técnicas de cifrado y/o firma digital, no es un medio seguro para enviar información personal o confidencial.
3. Evitar ingresar al sitio web de entidades financieras o comercio electrónico desde un cyber-café, locutorio u otro lugar público.
4. Verificar los indicadores de seguridad del sitio web en el cual ingresará información personal.
5. Los ordenadores del Club deben tener al día las actualizaciones de seguridad en el sistema operativo.



6. Los encargados de áreas financieras deberán revisar los resúmenes bancarios y de tarjeta de crédito tan pronto como los reciban y, en caso de detectar cargos u operaciones no autorizadas, comunicarse de inmediato con la organización emisora.
7. Los usuarios no deberán descargar ni abrir archivos de fuentes no confiables en los ordenadores propiedad del Club.

8. RESUMEN DE CONTROLES

Consecuencia de lo anterior, las medidas adoptadas para evitar, prevenir y erradicar las actuaciones delictivas relacionadas contra la intimidad personal y familiar, prostitución, explotación sexual y corrupción de menores, delitos contra la dignidad de las personas, delitos informáticos y delitos contra la propiedad intelectual, son:

1. Existencia de un responsable de seguridad a efectos de la LOPD.
2. Centralización de reclamaciones de terceros sobre LOPD en el departamento de Cumplimiento Normativo.
3. Procedimiento para el ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición al tratamiento de datos de carácter personal).
4. Documento de funciones y obligaciones del personal.
5. Política Corporativa de Seguridad de la Información, incluyendo la información y formación a los empleados de la entidad para el uso de la información.
6. Política de uso del correo electrónico, elaborada conforme al R.D. 1720/2007, de medidas de seguridad sobre el tratamiento de los datos de carácter personal, y a la norma de estándares de seguridad de la información ISO 27002:2005.
7. Descripción detallada de aquellos usos no autorizados en relación con el correo electrónico, de obligado seguimiento por todos los usuarios. Entre los usos prohibidos destacan conductas tales como el envío de comunicaciones comerciales en vulneración de la LOPD, el reenvío de contenidos no relacionados con actividades propias de la entidad, entre otros.
8. Descripción de buenas prácticas en relación al uso del correo electrónico, tales como la prohibición de abrir o ejecutar correos de remitente desconocido, o la de transmitir mensajes que contengan determinados datos de carácter personal, entre otras.
9. Herramienta informática que permite tanto el examen del contenido de los correos electrónicos y archivos LOG del servidor como su filtración y bloqueo de acuerdo a determinados parámetros preestablecidos.



10. Política de backup que asegura la realización diaria de una copia de seguridad de los entornos críticos.
11. Política de almacenamiento de la información sensible de forma confidencial y ordenada.
12. Política de uso de dispositivos móviles para empleados.
13. Informar y formar a los visitantes y aficionados en los controles de acceso sobre el uso de dispositivos móviles de captación de imágenes.
14. La inclusión de cláusula de confidencialidad en los contratos de los empleados sobre la información de carácter personal que se tenga acceso en el desarrollo de su actividad.
15. La inclusión de cláusulas contractuales en los contratos con los proveedores relativas al tratamiento de datos de terceros.
16. Existencia de claves de acceso de los empleados a sistemas informáticos.
17. La obligación de informar de anomalías de los sistemas de información.
18. Formación en materia de protección de datos de carácter personal.
19. Medidas de protección del fax y sus comunicaciones.
20. Trazabilidad y límites en acceso a bases de datos de clientes/abonados/socios/simpatizantes para detectar accesos anómalos.
21. Plan de continuidad de negocio ante desastres.
22. Descripción de buenas prácticas en relación al uso del correo electrónico, tales como la prohibición de abrir o ejecutar correos de remitente desconocido, o la de transmitir mensajes que contengan determinados datos de carácter personal, entre otras.
23. Vigilancia, control y auditoría del buen uso de correo electrónico corporativo.
24. Herramienta informática que permite tanto el examen del contenido de los correos electrónicos y archivos LOG del servidor como su filtración y bloqueo de acuerdo a determinados parámetros preestablecidos.
25. Procedimiento específico para realizar la contratación de servicios de Tecnología para el mantenimiento y soporte de la infraestructura tecnológica.
26. La obligación de informar de anomalías de los sistemas de información.



27. La existencia de claves acceso de los empleados a sistemas informáticos.
28. Auditoría de sistemas por profesionales externos a la entidad deportiva
29. Servicios externos de control, entre los que se incluyen: Servicio Temprano Anti-phising.
30. Monitorización y análisis troyanos.
31. Monitorización de aplicaciones móviles maliciosas.
32. Monitorización reputación redes sociales.
33. Monitorización registros dominios, barras de navegadores, buscadores, correos basura.
34. Monitorización perimetral de sistemas.

DISPOSICIÓN DE ENTRADA EN VIGOR

El Presente Reglamento, aprobado por el Consejo de Administración del Club el día 12 de mayo de 2023, deroga cualquier otra versión anterior, y mantendrá su vigencia desde el día siguiente a su publicación en la web corporativa (granadacf.es).

DISPOSICIÓN FINAL

El presente Reglamento será entregado a cada uno de los integrantes del club, empleados, jugadores, y directivos, que habrán de firmar la entrega del mismo a los efectos de recibí y conocimiento. El mismo estará igualmente disponible en la web corporativa de la entidad (granadacf.es).

Todas las dudas y/o incidencias que plantee la aplicación de la presente normativa serán resueltas por el Departamento de Cumplimiento del Club.



ANEXO I
SOLICITUD DE ACCESO DE ORDENADORES Y
TABLETS PERSONALES A LOS RECURSOS
INFORMÁTICOS DEL CLUB



**ANEXO I. SOLICITUD DE ACCESO DE ORDENADORES Y TABLETS
PERSONALES A LOS RECURSOS INFORMÁTICOS DEL CLUB**

Por la presente solicito el acceso de mi dispositivo privado que consiste en a los recursos informáticos del GRANADA CD, SAD (en adelante “el Club”), manifestando mi compromiso de cumplir con la normativa de la entidad para tener acceso a dichos recursos a través de mis dispositivos móviles personales.

Entiendo y autorizo que, durante el uso de los recursos, el Club, por causa justificada, pueda monitorizar mi uso para cuestiones de seguridad y debidamente justificada.

Entiendo además que, si cometo alguna violación en el uso de estos recursos, mi acceso puede ser revocado y el Club puede tomar medidas disciplinarias.

En relación al uso de los recursos informáticos del Club eximo a la entidad de cualquier reclamación y/o daños que provenga por mi uso inadecuado y contrario a las políticas de la entidad.

Acepto y entiendo que el uso de los recursos informáticos del Club con dispositivos personales no incluye mantenimiento, soporte informático ni actualización de mis dispositivos para que sean compatibles con los recursos informáticos del Club y eximo al Club de cualquier responsabilidad sobre el mal funcionamiento de mis dispositivos una vez conectados a los recursos informáticos del Club.

FIRMA:

NOMBRE:

DNI:

FECHA:

Esta autorización debe ser enviada al Área de



ANEXO II
ACEPTACIÓN PROTOCOLO DE
TECNOLOGÍA DE LA INFORMACIÓN



ANEXO II. ACEPTACIÓN PROTOCOLO DE TECNOLOGÍA DE LA INFORMACIÓN

El protocolo Tecnología de la Información regula el uso de los dispositivos electrónicos y digitales y en general las nuevas tecnologías que el Club pone a disposición de los trabajadores y usuarios en general, bien sean propios del Club o del trabajador, con el fin de proteger la seguridad del Club, la privacidad, los derechos fundamentales de nuestros trabajadores y las leyes de propiedad intelectual y la revelación de secretos, entre otras normas.

Esta política establece que los trabajadores sujetos a su aplicación, deben confirmar la recepción y aceptación, circunstancias que confirmo con la firma del presente documento.

ENTIENDO QUE EL INCUMPLIMIENTO, INTENCIONADAMENTE O POR NEGLIGENCIA, DE CUALESQUIERA DE LAS OBLIGACIONES Y COMPROMISOS ADQUIRIDOS CON EL PROTOCOLO, PODRÁN IMPLICAR, EN SU CASO, LAS SANCIONES DISCIPLINARIAS CORRESPONDIENTES POR PARTE DE GRANADA CF SAD Y LA POSIBLE RECLAMACIÓN POR PARTE DE LA MISMA DE LOS DAÑOS Y PERJUICIOS ECONÓMICOS CAUSADOS.

EL TRABAJADOR

Fdo: D/D^a

DNI

Fecha:

