Normativa interna de seguridad de la información para el correcto uso de equipos, servicios e instalaciones

HISTÓRICO DE VERSIONES		
Versión	**Fecha**	**Resumen de los cambios producidos**
1	20/02/2026	Inicial

Elaborado y/o revisado:	Aprobado:
Responsable de Seguridad **TOMAS RAMOS SUAREZ**	Gerente **FRANCISCO JAVIER PESCADOR PEREZ**

Contenido

1. INTRODUCCIÓN Y OBJETO DE LA NORMATIVA

El objetivo de este documento es proporcionar a SPORT STUDIO un catálogo normativo interno, que satisfaga el ámbito de aplicación del Esquema Nacional de Seguridad, es decir, una relación de Normas internas de seguridad, recogiendo lo exigido por dicha regulación. La necesidad de completar este marco normativo se establece en varios artículos del ENS y en concreto, en el Anexo II del ENS (Medidas de Seguridad), en la medida [org.2], "Normativa de seguridad".

La publicación y el cumplimiento de estas normas contribuirá a:

- Mejorar los servicios que SPORT STUDIO presta, propiciando una gestión eficiente y segura de los procesos incluidos en los sistemas de información con los que opera.
- Facilitar el máximo aprovechamiento de los recursos y sistemas de información en la actuación de SPORT STUDIO.
- Proteger los sistemas de información de SPORT STUDIO y los datos que tratan, de los riesgos que puedan deberse a la acción humana, especialmente en lo referente a conductas incorrectas, inadecuadas o ilegales.
- Asegurar la protección de los derechos de terceros en sus relaciones con SPORT STUDIO y el desenvolvimiento profesional de los empleados y usuarios que tienen acceso a los recursos y sistemas de información de SPORT STUDIO.

Con el objetivo de profundizar en las medidas de seguridad requeridas por los sistemas de información del ámbito de aplicación del ENS, dicho Esquema insta a desarrollar, publicar y hacer valer normas de carácter interno en las organizaciones, tendentes a mejorar el nivel de seguridad de las informaciones que manejan y los servicios que prestan.

2. NORMATIVA INTERNA DE SEGURIDAD

Este apartado recoge las normas que rigen internamente el uso correcto de equipos, servicios e instalaciones, de SPORT STUDIO, junto con todo aquello que se considerará uso indebido y, por último, la responsabilidad del personal con respecto al cumplimiento de dichas normas.

2.1 DEBERES Y OBLIGACIONES DEL PERSONAL

Las obligaciones que afectarán a cada persona en su puesto de trabajo de cada Departamento/Área de SPORT STUDIO son las siguientes:

- Conocer y cumplir **lo dispuesto en la normativa interna en materia de seguridad de la información, y de protección de datos personales**.
- Conocer las **consecuencias que se pudieran derivar y las responsabilidades** en que pudiera incurrir en caso de incumplimiento de la normativa, que podrían derivar en sanciones.
- **Guardar secreto** sobre los datos e informaciones que pueda conocer, así como sobre controles y posibles debilidades, incluso después de haber causado baja en la empresa.
- **Usar de forma adecuada** según la normativa los mecanismos de identificación y autenticación ante los sistemas de información. En el caso de contraseñas, cumplir lo recogido en la normativa, especialmente en cuanto a asignación, sintaxis, distribución, custodia y almacenamiento de las mismas, así como el cambio con la periodicidad que se determine.
- Cumplir la normativa en cuanto a gestión de soportes informáticos, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia. En el caso de averías que requieran su transporte fuera de las instalaciones se intentará proteger (cifrar) o borrar (salvo que sea copia única) previamente su contenido o se exigirán garantías escritas de que se respetará la confidencialidad y la integridad de la información.

- La documentación en papel deberá ser guardada y custodiada en sus archivos correspondientes.

- Se seguirá una política de puesto de trabajo despejado y mesas limpias, no dejando información confidencial o privada a la vista. De modo que cuando concluya la jornada laboral, el usuario deberá evitar dejar documentación encima de las mesas o fuera de sus lugares de archivo, que deberán permanecer cerrados con llave.

- Respecto a la documentación que se imprima, el usuario será responsable de su recogida, que deberá efectuarse con carácter inmediato, evitando el acceso a la documentación por usuarios no autorizados. La documentación que no sea de utilidad para el usuario, deberá ser destruida utilizando para ello las destructoras de papel existentes.

- Se debe bloquear el equipo cuando no vaya a ser usado, o usar mecanismos automáticos, no dejándolo nunca desatendido sin bloquearlo previamente.

- Se informará al personal de SPORT STUDIO, mediante la difusión de esta normativa, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, en concreto:
  - Se especificarán las medidas disciplinarias a que haya lugar.
  - Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
  - Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.

- Cuando los documentos electrónicos vayan a ser difundidos ampliamente (a través de la Web, o por correo electrónico a numerosos destinatarios), sus autores o quienes los envíen, deben realizar la limpieza de los metadatos que dichos documentos contengan, antes de la difusión.

2.2 CONCIENCIACIÓN Y FORMACIÓN DE EMPLEADOS

Todo el personal de la organización, y cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la misma, podrán acceder a una adecuada **formación** sobre aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

- Configuración de sistemas que les afecten directamente, según sus competencias.
- Detección y reacción a incidentes.
- Gestión de la información en cualquier soporte en el que se encuentre.

Asimismo, se realizarán las acciones necesarias para **concienciar** regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.
En particular, se recordará como mínimo una vez al año y por escrito (mediante correo electrónico):

- La presente normativa de seguridad relativa al buen uso de los sistemas.
- El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

2.3 NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

La finalidad de la gestión de incidentes es asegurar que los eventos y debilidades en la seguridad de la información sean comunicados y gestionados de una manera que permita tomar una acción correctiva oportuna. Asimismo, se establecen las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
Se entiende por "incidencia" o "incidente", cualquier evento que pueda afectar o que afecte a la seguridad de la información (dimensiones: integridad, disponibilidad, confidencialidad y autenticidad). Por consiguiente, se clasificará como "incidencia" o "incidente" cualquier evento de este tipo.

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de SPORT STUDIO, deberá informar inmediatamente al Jefe de Departamento/Área o al Responsable de Seguridad, quien gestionará dicha incidencia.

Los signos de un incidente pueden ser de dos tipos:

Técnicos:

- Alertas de sensores de un servidor.
- Una alerta del antivirus.
- La caída de un servidor o sistema.
- Accesos lentos.
- La detección de un escáner de puertos.
- El resultado del análisis de vulnerabilidades.
- Las amenazas de ataque por parte de hackers.

Organizativos o de usuario:

- Pérdida del certificado digital (o del soporte que lo contiene).
- Apertura no intencionada de un fichero infectado.
- Intento de robo de credenciales/phishing por correo electrónico.
- Intento de perjudicar a la entidad mediante ingeniería social desde el exterior (Hacerse pasar por otra persona).

2.4 USO EFICIENTE DE EQUIPOS Y RECURSOS

Dentro de las medidas de mejora de la eficiencia energética, y de austeridad y reducción del gasto en SPORT STUDIO, se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios y que además contribuyen a mejorar la seguridad de la información.

- Apagar el PC (y la impresora local, en su caso), al finalizar la jornada laboral .

- 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.

- Se optará por usar las impresoras en red antes que las locales.
- Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.

2.5 COMPROMISOS DE LOS USUARIOS

Es responsabilidad directa del usuario:

- Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore el Comité de Seguridad de la Información, para garantizar que aquellas no puedan ser utilizadas por terceros.
- Cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.
- En el caso de que su equipo contenga información privada y/o confidencial, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa de SPORT STUDIO establece al respecto.

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

- El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
- La degradación de los servicios.
- 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.
- El uso de los sistemas de información para fines ajenos a los fines del servicio.

- Dañar intencionadamente los recursos informáticos de SPORT STUDIO o de otras empresas o instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

2.6 USOS ESPECÍFICAMENTE PROHIBIDOS

Están terminantemente prohibidos los siguientes comportamientos:

- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por SPORT STUDIO, sin la previa autorización del Responsable del Sistema (responsable informático).
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por SPORT STUDIO, a través del Responsable del Sistema (responsable informático).
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa de SPORT STUDIO, a través del Responsable del Sistema (responsable informático).
- Instalación y/o 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.
- Instalar voluntariamente cualquier producto informático en el sistema de información de la organización. Todas aquellas aplicaciones necesarias para el desempeño de su trabajo serán instaladas únicamente por personal debidamente autorizado de la organización o empresa prestadora de los servicios informáticos.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).

- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos, sin estar autorizado.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema, sin estar autorizado para hacerlo.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la organización o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento de la organización.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus establecidos por la organización y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la organización, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los corporativos.
- Borrar cualquiera de los programas instalados legalmente sin autorización de la organización.
- Utilizar los recursos telemáticos de la organización, incluido el acceso a la red Internet, para actividades que no se hallen directamente relacionadas con el

puesto de trabajo del usuario.

- Utilizar los recursos del sistema de información a los que tenga acceso para uso privado o para cualquier otra finalidad diferente de las estrictamente laborales.
- Realizar cualquier actividad privada o diferente de las estrictamente laborales, utilizando recursos de la empresa o propios del empleado.
- Facilitar a persona alguna ajena a la organización ningún soporte conteniendo datos, a los que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.
- Utilizar cualquier información que hubiese podido obtener por su condición de empleado de la organización y que no sea necesaria para el desempeño de sus funciones.
- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para las finalidades propias de la empresa, en la red corporativa de la misma.
- Intentar eludir o vulnerar los mecanismos y dispositivos de seguridad, intentar cualquier acceso no autorizado a datos o recursos, y poner en peligro la disponibilidad de los datos, la confidencialidad o la integridad de los mismos. El usuario informará al Responsable de Seguridad, sobre posibles debilidades en los controles que pudiera detectar.
- Ceder o comunicar a otros las contraseñas, que son personales, las cuales no estarán almacenadas en claro, y que serán transmitidas por canales seguros; los usuarios serán responsables ante la entidad de todos los accesos y actividades que se puedan haber realizado utilizando su código de usuario y contraseña.
- Sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido.

2.7 USO DEL CORREO ELECTRÓNICO

A continuación, se incluye un conjunto de normas que tienen como objetivo reducir el riesgo en el uso del correo electrónico; por ello, el usuario está obligado a:

- Utilizar el correo electrónico exclusivamente para propósitos profesionales. [Gran parte de los mensajes de correo electrónico no deseados que llegan a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo. Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de ataque.]
- Usar contraseñas seguras para limitar la posibilidad de un acceso no autorizado a las cuentas de correo electrónico, es conveniente utilizar contraseñas robustas.
- No ceder el uso de las cuentas de correo. Las cuentas de correo son personales e intransferibles.
- Además de ello, es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios.
- Revisar la barra de direcciones antes de enviar un mensaje. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información (es un incidente).
- Cuando se responda a un mensaje, es esencial revisar las direcciones que aparecen en el campo Con Copia (CC). Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.
- No se deben enviar o reenviar correos de forma masiva. Si se envía por necesidad un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO o BCC), evitando su visibilidad a todos los receptores del mensaje.
- No enviar mensajes en cadena. [Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe notificar la incidencia al Responsable de Seguridad.]

- No responder a mensajes de Spam. [La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envían a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a SPORT STUDIO.]
- Utilizar mecanismos de cifrado de la información. Los mensajes que contengan información sensible, confidencial o privada deben cifrarse. [Se pondrá a disposición de los usuarios que lo precisen el acceso a la aplicación necesaria para el cifrado de información.]
- Asegurarse de la identidad del remitente antes de abrir un mensaje. [Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) del usuario atacado. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación virtual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información sensible, confidencial o protegida a petición de un correo del que no se puede asegurar la identidad del remitente debe rechazarse. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso.]
- Desactivar la vista previa de mensajes. [Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos.]
- Limitar el uso de HTML en los mensajes. [El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.]
- Utilizar herramientas de análisis contra código dañino. [La utilización de herramientas tales como antivirus y cortafuegos ayuda a detectar el código malicioso y a mitigar sus efectos. Por ello, debe configurarse el antivirus con la opción de analizar el correo electrónico entrante.]

- No abrir correos basura ni correos sospechosos. Aun cuando un mensaje no deseado hubiera traspasado el filtro contra spam, no debe abrirse, debiendo reportarse el correspondiente incidente de seguridad. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.
- No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso.
- Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de archivos ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).
- Informar de correos con virus, sin reenviarlos. Si el usuario detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente de seguridad al Responsable de Seguridad y no reenviarlo, para evitar su posible propagación.
- No utilizar el sistema de correo electrónico como espacio de almacenamiento.

2.8 USO Y ACCESO DE INTERNET

Para minimizar los riesgos derivados del uso de Internet, resulta necesario adoptar un conjunto mínimo de medidas de seguridad dirigidas a propiciar su correcto uso. El usuario está obligado a:

- Usar Internet para fines profesionales. Internet es una herramienta más de las utilizadas por los usuarios de SPORT STUDIO. Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales.
- No visitar páginas de contenido poco ético, ofensivo o ilegal. No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o atentar contra la dignidad humana. Análogamente, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.

- No visitar páginas no fiables o sospechosas. Para evitar posibles incidentes de seguridad, es aconsejable no visitar páginas que se consideren sospechosas de contener código malicioso.

- Cuidar la información que se publica en Internet. No se debe proporcionar información sobre la organización en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta. En este sentido, está prohibido difundir sin autorización cualquier tipo de información no pública sobre el funcionamiento interno de SPORT STUDIO, sus recursos, estructura, etc.

- Observar las restricciones legales que sean de aplicación. Antes de utilizar una información obtenida de Internet, los usuarios deberán comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial.

- Realizar descargas sólo si se tiene autorización. Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso. Aunque SPORT STUDIO decida no limitar técnicamente la capacidad para descargar archivos de audio o vídeo, los usuarios deberán tener en consideración que la descarga de estos archivos puede ir en detrimento del rendimiento de los recursos informáticos y, por ello, limitarán su descarga y reproducción al ámbito estrictamente profesional.

- No descargar código o programas no confiables. Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas.

- Asegurar la autenticidad de la página visitada. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones. Cuando la página web se encuentre autenticada mediante

certificado digital, el usuario verificará su autenticidad.

- Comprobar la seguridad de la conexión. En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o privada es importante asegurar su cifrado. Una manera de asegurar la confidencialidad es comprobar que se utiliza protocolo HTTPS en la comunicación en vez del protocolo estándar http (examinando la barra de direcciones).

- Cerrar las sesiones al terminar la conexión. Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información, ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador.

- Utilizar herramientas contra código dañino. El volumen de código dañino que circula en el ciberespacio es muy elevado y presenta multitud de aspectos diferentes. Por tanto, es necesario disponer del adecuado abanico de herramientas que permitan una adecuada protección.

- Mantener actualizado el navegador y las herramientas de seguridad.

- Utilizar los niveles de seguridad del navegador. Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.

- Bloquear las cookies, permitiéndolas únicamente en aquellas páginas que ofrezcan garantías de privacidad. Las cookies son pequeños programas que emplean los servidores Web para almacenar y recuperar información acerca de sus visitantes. (Por ejemplo, quién, cuándo y desde dónde se ha conectado un usuario).

- Eliminar la información privada. Los navegadores Web almacenan información privada durante su utilización, tal como el historial de navegación, cookies aceptadas, contraseñas, etc.; información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable

borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.

- No instalar complementos desconocidos. Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador del usuario un complemento (plug-in, add-on, etc.) para poder acceder al contenido.

- Limitar y vigilar la ejecución de Applets y Scripts.

2.9 USO DE LA FIRMA ELECTRÓNICA Y CERTIFICADOS

A raíz de la implementación de la administración electrónica, se han impuesto mecanismos para firmar y garantizar la autenticidad, integridad y no repudio de la documentación, por lo que son una herramienta básica de trabajo para el personal de SPORT STUDIO, y como tal, deberán aplicárseles una serie de medidas y recomendaciones para un correcto uso de certificados digitales.

En el ámbito profesional: el certificado digital de firma o firma digital es el documento electrónico que identifica a la persona como autorizada por SPORT STUDIO. El uso de este certificado implica que todas las obligaciones, declaraciones, solicitudes y demás gestiones que se realicen, vincularán a dicha persona o a SPORT STUDIO a la hora de formalizar contratos con terceros, realizar trámites, etc., con plena validez jurídica, por ello, se deben mantener unas medidas de custodia y uso excepcionales, en concreto:

- El certificado digital de firma personal es intransferible por lo que sólo el titular del mismo deberá tener acceso a él.
- Si el certificado está en formato de tarjeta, o pendrive, debe guardarlo en un lugar seguro bajo llave, asegurándose de que terceros no puedan acceder.
- No comunicar a nadie el PIN del certificado digital, es la garantía de que si el certificado digital cae en manos ajenas no pueda ser usado.
- No guardar nunca juntos, en el mismo lugar, el certificado digital y el PIN.
- Si se tiene instalado el certificado digital en el equipo informático del usuario, evitar que terceras personas tengan acceso al mismo; para ello se

debe bloquear el equipo con contraseña siempre que vaya a abandonarse el puesto de trabajo.

- En el equipo que use el certificado digital tener antivirus y firewall para evitar accesos no deseados.
- Antes de utilizar el certificado, en la firma de cualquier trámite, asegurarse de que ese es el trámite que se desea realizar por lo que hay que leer detenidamente todas las partes del mismo ya que una vez firmado tendrá validez legal.

2.10 GESTIÓN DE SOPORTES: MEMORIAS USB, DISPOSITIVOS EXTERNOS E IMPRESORAS.

Con carácter general, **el uso de memorias USB debe ser previamente autorizado en SPORT STUDIO**, en su caso, la autorización deberá proporcionarla el Responsable de Sistemas siguiendo el procedimiento de autorización.

Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento.

En el caso de que el personal de SPORT STUDIO necesitara enviar datos sensibles por medios inseguros, como el correo electrónico, o mediante protocolos IP que no soporten cifrado, o bien si se necesitara sacar dispositivos con información fuera de las instalaciones, se deben usar herramientas de cifrado.

A la hora de reutilizar o destruir un soporte o dispositivo se deben aplicar medidas que garanticen que tras el proceso no se pueda acceder a la información.

<u>Impresoras en red, fotocopiadoras y faxes</u>

En ningún caso el usuario podrá hacer uso de impresoras, escáneres o fotocopiadoras que no hayan sido proporcionadas por SPORT STUDIO y, que, por tanto, estarán previamente inventariadas, asimismo:

- Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras.
- Conviene no olvidar recoger los originales del dispositivo de copia, una vez

finalizado el proceso de copia.

- Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo.

2.11 PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de SPORT STUDIO sin la correspondiente licencia de uso.

Los programas informáticos propiedad de SPORT STUDIO o usados bajo licencia, 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 todo ello se realice con la autorización previa.

Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización.

2.12 MEDIDAS DE SEGURIDAD CON TERCEROS Y PRESTADORES DE SERVICIOS

A continuación, se relacionan las medidas de seguridad que conforman la base normativa que regirá en la relación con terceros prestando servicios a SPORT STUDIO, y que podrá completarse con medidas más restrictivas en el caso de servicios que así lo requieran.

- SPORT STUDIO tratará de operar con terceros que posean certificación de conformidad con el ENS.
- Los contratos firmados con las entidades que prestarán servicios a SPORT STUDIO deberán recoger en su clausulado la OBLIGACIÓN DE CONFIDENCIALIDAD en el marco de la relación contractual.
- Las empresas que prestan servicios a SPORT STUDIO que requieran de acceso a sus sistemas de información deberán seguir las directrices establecidas en la presente NORMATIVA.
- Se prohíbe el empleo de soportes de información extraíbles (CD's, DVD's, memorias USB, etc.), por parte del personal de terceros que presten servicios a

SPORT STUDIO, para el almacenamiento de información de la empresa, sin autorización previa.

- SPORT STUDIO podrá exigir, en aplicación del clausulado de los contratos de prestación de servicios firmados con terceros, cualesquiera EVIDENCIAS DE CUMPLIMIENTO de la legislación vigente.

2.13 INCUMPLIMIENTO DE LA NORMATIVA

Todos los usuarios de SPORT STUDIO están obligados a cumplir lo prescrito en la presente *Normativa Interna de Seguridad para el correcto uso de Equipos, Servicios e Instalaciones*.

En el supuesto de que un usuario no cumpla alguna de las obligaciones establecidas en la presente Normativa, sin perjuicio de las acciones disciplinarias que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.