PROTOCOLO DE USO TIC

El uso de los recursos de tecnologías de la información y las comunicaciones (recursos TIC) de la FFIB, incluyendo equipos telemáticos e informáticos con sus aplicaciones ofimáticas y herramientas en ellos instaladas, así como la manera de acceder a la red corporativa y sus servicios asociados (almacenamiento de datos e impresión de los mismos), exige definir unas políticas sobre su utilización y sobre el control a ejercer por parte de la FFIB, para garantizar el uso adecuado de dichos recursos, limitar los riesgos que dicha utilización comporta para los propios activos informáticos, y proteger la información.

En este sentido, la presente política pretende dar respuesta a las siguientes necesidades:

- Garantizar que solo el personal autorizado accede a la red de datos de la FFIB

- Proteger los sistemas informáticos de la FFIB

- Prevenir responsabilidades administrativas, civiles y penales que pudieran derivarse para la FFIB por el uso ilícito de los recursos TIC.

- Preservar la integridad, disponibilidad y confidencialidad de la información propiedad de la FFIB o de cualquier tercero vinculado a ésta.

El presente documento tiene por objeto definir las obligaciones de los usuarios respecto al acceso a la red de datos corporativa de la FFIB y las medidas de seguridad a aplicar en el uso de los recursos TIC, así como establecer las directrices para el buen uso de dichos recursos.

Esta política vincula y es de aplicación a los empleados y colaboradores, sin excepción y cualquiera que sea su cargo, responsabilidad o ubicación geográfica, a todo el personal que preste sus servicios en cualquiera de los centros de trabajo de la FFIB.

Asimismo, el presente documento es igualmente de aplicación al personal de cualquier proveedor externo que preste sus servicios en los referidos centros de trabajo, y que de algún modo utilice o tenga acceso a la red de datos corporativa de la FFIB.

A todos ellos, denominados en adelante, «usuarios», les serán de aplicación las normas contenidas en el presente título.

ACCESO A LOS SISTEMAS INFORMÁTICOS Y A LA RED CORPORATIVA (INTRANET)

El acceso a los sistemas informáticos y a la red corporativa de la FFIB se concederá a los empleados que lo requieran para el desempeño de su trabajo, previa solicitud por los responsables a los que dichos empleados estén adscritos, mediante una petición formal al Secretario General explicando los motivos.

Y el mismo procedimiento se habrá de seguir para conceder el acceso al personal externo que lo requiera.

Será responsabilidad del Secretario General, la petición de derechos de acceso a los sistemas informáticos y a la red corporativa de la FFIB, de cambios en los derechos de acceso (por cambio de funciones u ocupación), así como la comunicación del cese de actividad del empleado, dentro del mismo día en el que el cese tiene lugar, con el objeto de dar de baja al usuario. El mismo periodo de tiempo se aplicará para la comunicación del cese de actividad de cualquier externo que tuviera acceso a la red corporativa.

ACCESO A LOS ACTIVOS INFORMÁTICOS FÍSICOS.

Se entiende como activos informáticos físicos todos aquellos activos informáticos que, por su naturaleza, requieren disponer de una fuente de energía eléctrica para su adecuada utilización, y que disponen de funcionalidad en sí mismos, como por ejemplo un ordenador de sobremesa, un ordenador portátil, un dispositivo móvil, una impresora, tablets, relojes digitales, etc.

En función de las necesidades laborales de los usuarios, se definirán los activos físicos a proveer. Estas peticiones se realizarán igualmente por los empleados a los que los usuarios estén adscritos, mediante una petición formal al Secretario General.

Todos los recursos TIC que se utilicen en el ámbito profesional, serán adquiridos por la FFIB y seguirán el protocolo de compras establecido.
Aquellos supuestos excepcionales en los que se adquiera un dispositivo TIC fuera del cauce internamente establecido, deberán estar justificados, y se deberá informar de ello con carácter previo a la Comisión Económica, con el fin de darlo de alta en el inventario y registrarlo.
Los recursos TIC puestos a disposición de los usuarios de la FFIB, son de titularidad de la FFIB y cumplen con la finalidad principal de asegurar la prestación de servicios por parte de dichos usuarios.
Por ello, los recursos TIC serán utilizados por los usuarios para fines estrictamente profesionales y atendiendo en todo momento a las siguientes condiciones generales de uso.

PROPIEDAD, CONFIDENCIALIDAD Y USO PROFESIONAL DE LA INFORMACIÓN ALMACENADA EN LOS SISTEMAS CORPORATIVOS.

La información relacionada con la actividad laboral de la FFIB, deberá ser obligatoriamente almacenada en los sistemas de

red puestos a disposición de los usuarios (carpetas de red para el almacenamiento de datos departamentales, gestores documentales, así como espacios de trabajo en red), y dado que se trata de información profesional, la FFIB podrá tener acceso a la misma respetando en cualquier caso la legalidad vigente. En el momento que se produzca un relevo en un puesto de trabajo, es de obligado cumplimiento la cesión de toda la información y datos relacionados con la actividad laboral en los diferentes soportes a la persona entrante.

La mencionada información tendrá como mínimo la categoría de restringida, y en ningún caso podrá ser objeto de comunicación a terceros cuando la remisión no quede justificada por motivos profesionales. Asimismo, la documentación que deban analizar auditores, consultores u otros externos contratados por la FFIB para cualquier proyecto, deberá analizarse en la medida de lo posible en las instalaciones de la FFIB (sin la entrega de copias digitales o impresas), y en todo caso, previa autorización expresa del Órgano de Cumplimiento y la firma de una cláusula de confidencialidad.

Los usuarios guardarán especial diligencia en relación a la confidencialidad de aquellos ficheros que contengan datos cuya naturaleza esté afectada por las leyes de protección de datos vigentes en cada momento. Aquellos usuarios que tengan acceso a dichos ficheros deberán respetar, en todo momento, las medidas de seguridad establecidas para cada caso y extremarán las precauciones a fin de evitar la exposición de información y preservar su confidencialidad frente a terceros no autorizados.

El ordenador es vulnerable, por lo que cada vez que un usuario deje su ordenador, ya sea en su escritorio o en cualquier otro lugar, se recomienda cerrar la sesión o bloquear el ordenador antes de salir. Se recomienda cerrar la sesión en lugar de bloquear si se deja de utilizar el ordenador para largos periodos de tiempo, como durante la noche o los

fines de semana, excepto si es de aplicación el uso del control remoto para teletrabajo.

Asimismo, al objeto de preservar la seguridad de la información, las mesas de trabajo deberán mantenerse despejadas y libres de documentos, especialmente en las salas de reuniones y lugares de paso. Los expedientes confidenciales y los documentos de trabajo especialmente sensibles –tales como aquellos que contengan datos relativos a la salud-, deberán ser guardados en un lugar seguro (tales como armarios y cajones bajo llave), cuando no se estén utilizando, evitando así cualquier acceso no autorizado.

Las obligaciones de confidencialidad a las que se hace referencia en el presente documento se entienden por tiempo indefinido, debiendo los usuarios guardar la máxima reserva de la información a la que tenga acceso en el ejercicio de sus funciones profesionales en la FFIB, incluso hasta después de finalizar la relación laboral con ésta, no pudiendo en ningún caso divulgar ni utilizar, directa o indirectamente, los datos, documentos, metodologías, claves y demás información perteneciente a la FFIB o a terceros a ésta vinculada.

RESTRICCIONES EN CUANTO A LA NATURALEZA DE LOS DATOS.

En ningún caso se admitirá el almacenamiento en los recursos TIC de la FFIB de:

- Archivos con contenidos de naturaleza ofensiva, intimidatoria u hostil en relación con la raza, sexo, religión, nacionalidad, orientación sexual, discapacidad o cualquier otra condición de la persona, así como los que realicen proselitismo religioso, político o de cualquier otro carácter.

- Archivos de contenido protegido por derechos de propiedad intelectual, como música, obras científicas o literarias, juegos y programas informáticos no autorizados, etc., sin el consentimiento expreso del titular de dichos derechos.

- Archivos con datos personales de terceros, sin cumplir con las disposiciones legales en materia de protección de datos de carácter personal.

USO DE LAS CARPETAS EN RED.

Para asegurar el mejor aprovechamiento de los servicios de impresión y digitalización en red, se hace necesario establecer unas normas de uso que garanticen el uso racional de dichos dispositivos y la contención del gasto de los consumibles necesarios para la operación de este servicio. La política a seguir es la eliminación progresiva de las impresiones personales (locales), potenciando la compartición de las impresoras basadas en servidor (en red), que darán servicio a un conjunto de usuarios. Asimismo, las impresoras deberán garantizar la confidencialidad y seguridad de las impresiones o digitalizaciones, así como la autoría de las impresiones realizadas; todo ello mediante un sistema de impresión segura.

USO DE CONTRASEÑAS O CLAVES DE ACCESO Y ACCESO REMOTO.

El usuario no podrá comunicar ni compartir con otra persona el identificador de usuario y la clave de acceso al sistema. Salvo prueba en contrario, se presumirá que la actividad desarrollada con dicho identificador y clave de acceso ha sido realizada por el titular de los mismos, asumiendo éste la responsabilidad laboral, civil o penal que pueda derivarse de su uso.

Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso, deberá ponerlo en conocimiento de la empresa informática, y crear una nueva clave de acceso.
En la gestión y uso de las contraseñas, se han de seguir las siguientes pautas:

- La contraseña deberá tener la extensión y complejidad que establezca en cada momento el responsable de seguridad.

- Deberán evitarse contraseñas de fácil intuición, que incluyan la utilización de palabras comunes, nombre del usuario, familiares, teléfonos, fechas de aniversario, matrículas de coche, repeticiones de un único carácter o cualquier otra palabra fácilmente deducible.

- No se deben conservar anotaciones de contraseñas en ningún documento en papel, agendas personales, etc.

- El empleado deberá facilitar a la empresa toda contraseña y acceso a cualquier tipo de plataforma, programa o soporte corporativo.

- En el caso de vacaciones, baja laboral o ausencia temporal del trabajador, incluidos los periodos fuera del horario laboral, el Secretario General o departamento al que esté adscrito el usuario ausente, podrá adoptar excepcionalmente y siempre que esté justificado por motivos profesionales las siguientes medidas:

  - Solicitar al responsable de seguridad la creación de una clave o acceso temporal que permita el acceso a los documentos de trabajo, al ordenador, directorios del servidor y al correo electrónico del trabajador ausente. El uso de esta clave se limitará a garantizar la continuidad del trabajo iniciado por el usuario ausente,

y en todo caso, cuando éste se reincorpore, la clave temporal deberá ser anulada.

- Solicitar al usuario ausente o al administrador de sistemas la configuración de un mensaje de respuesta automática en el correo electrónico, comunicando los datos de la persona que sustituya al usuario ausente.
- Solicitar al administrador de sistemas el desvío de los mensajes entrantes hacia otra/s cuenta/s de correo electrónico.
- Las claves de acceso de los usuarios que por cualquier motivo causen baja en la FFIB, quedarán sin efecto el mismo día en que se produzca la baja.

USO DEL CORREO ELECTRÓNICO.

El correo electrónico constituye una herramienta estandarizada en el mundo de las comunicaciones entre personas, pero también, uno de los riesgos más corrientes de obtener nuevos virus, códigos destructivos (spyware, troyanos, programas auto ejecutables, etc.), correos electrónicos no solicitados (spam), o cualquier material no autorizado.

Por ello, la FFIB se ha dotado de los medios técnicos necesarios para prestar este servicio con las debidas garantías tanto del servicio en sí mismo como de protección contra las posibles amenazas de seguridad que provengan del exterior. Asimismo, al objeto de mitigar dichos riesgos y regular el correcto uso de esta herramienta, es necesario que los usuarios cumplan obligatoriamente con las siguientes normas:

- El correo electrónico corporativo debe ser utilizado única y exclusivamente para fines profesionales de la FFIB.

- Archivos adjuntos a correos electrónicos sospechosos de remitente desconocido no se deben abrir. Asimismo, si el escáner antivirus del ordenador informa de una infección o si se sospecha de una posible infección, se debe comunicar al responsable de seguridad.

- Está estrictamente prohibido el envío o reenvío de correos electrónicos con contenidos de naturaleza ofensiva, inapropiada, intimidatoria u hostil, discriminatoria por razón de raza, sexo, religión, nacionalidad, orientación sexual, discapacidad o cualquier otra circunstancia personal o social, así como aquellos que realicen proselitismo religioso, político o de cualquier otro carácter no relacionado con la FFIB.

- Está igualmente prohibida la utilización del correo electrónico para ocasionar o favorecer situaciones de acoso sexual o laboral.

- El envío o almacenamiento de contenidos protegidos por derechos de propiedad intelectual, tales como música, obras científicas o literarias, juegos y programas informáticos no autorizados, etc., sin el consentimiento expreso de su titular, está absolutamente prohibido.

- En ningún caso se podrá llevar a cabo ninguna actuación que pretenda falsificar los encabezados de correo electrónico con el objeto de confundir a los destinatarios en cuanto a remitente, fechas u horas de remisión.

- Antes de enviar un correo electrónico a cualquier externo, el usuario deberá tener en cuenta y ser consciente, de que el contenido de dicho correo electrónico puede ser utilizado como prueba por el destinatario del mismo, en un eventual conflicto judicial o extrajudicial.

- No se deben reenviar correos electrónicos ni documentos corporativos a cuentas privadas del usuario, de sus familiares o amigos, ya que éstas no gozan del mismo

nivel de seguridad. Tampoco se puede configurar la cuenta de correo corporativo para reenviar los correos recibidos a una cuenta de correo personal.

- El formato de los correos electrónicos (tipos de letra, contenido de la firma, etc.) será el establecido en todo momento por la FFIB, para contribuir al mejor funcionamiento general del servicio, mediante el correspondiente libro de estilo.

USO Y ACCESO A INTERNET.

La importancia de los servicios basados en la conexión a internet está creciendo continuamente y el uso del correo electrónico y la navegación web son de vital importancia para el desarrollo de nuestra actividad. No obstante, la FFIB es consciente de los riesgos que implica el acceso a contenidos externos no controlados o previstos por la organización, focalizando el uso de internet únicamente a los intereses profesionales de la Federación.

Asimismo, para minimizar los riesgos derivados del uso de internet, los usuarios ser conscientes de los siguientes extremos:

- El uso de internet debe realizarse con fines lícitos, con arreglo a los valores éticos y profesionales establecidos en el código ético de la FFIB, y siempre con el máximo respeto a la Ley.

CONTROL Y MONITORIZACIÓN POR PARTE DE LA FFIB

La FFIB ostenta un derecho legítimo a controlar el uso adecuado de las herramientas y medios técnicos de su

propiedad, salvaguardando en todo momento los derechos fundamentales de los profesionales.

Todos los recursos TIC puestos a disposición de los usuarios, incluida la red de conexión a internet y el correo electrónico, son medios corporativos que se deben utilizar únicamente para llevar a cabo las funciones profesionales que cada usuario tenga asignadas en la FFIB.

A este respecto, se comunica que la FFIB vigilará el cumplimiento de la presente política, registrando la actividad de la red corporativa, manteniendo estadísticas y patrones de uso, y efectuando rastreos ocasionales del uso de internet y del tráfico de correos electrónicos, con el fin de evitar cualquier perjuicio derivado del incumplimiento de esta política.

La actividad de control y monitorización de recursos TIC se realizará en todo momento cumpliendo la legalidad vigente y respetando los derechos fundamentales de los profesionales.