SGSI02 – Normativa de Seguridad

Clasificación de la Información:

Nivel del Documento	Normativa
Nombre del Fichero	SGSI02-NormativaDeSeguridad.docx
Tipo	RESTRINGIDO
Ámbito de Difusión	Todos los empleados y colaboradores externos
Responsable	Responsable de Seguridad de la Información

CONTROL DE MODIFICACIONES		
Descripción	**Versión**	**Fecha**
Versión preliminar del documento.	1.0	19/11/2019
Versión revisada y primera publicación.	1.1	23/02/2021

ÍNDICE DE CONTENIDO

1. Introducción

Conforme a lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), este documento contiene la Normativa General de Utilización de los Recursos y Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la FUNDACIÓ LLUÍS ALCANYÍS que se encuentren afectados por el alcance del ENS para el desempeño de su trabajo, y en su caso el personal externo vinculado a prestaciones de servicios.

Por ello, cada uno de ellos debe cumplir los requerimientos de la Normativa de Seguridad de la Información y su documentación asociada. Quienes deliberadamente o por negligencia incumplan la Normativa de Seguridad podrían estar sujetos a responsabilidad.

La presente Normativa ha sido aprobada por la Dirección de la FUNDACIÓ LLUÍS ALCANYÍS, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la FUNDACIÓ LLUÍS ALCANYÍS pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

La Normativa de Seguridad será mantenida, actualizada y adecuada a los fines de la FUNDACIÓ LLUÍS ALCANYÍS, alineándose con el contexto de gestión de riesgos estratégica de la entidad.

Este documento se considera de uso interno para la FUNDACIÓ LLUÍS ALCANYÍS y, por consiguiente, no podrá ser divulgado salvo autorización del Comité de Gestión y Coordinación de la Seguridad de la Información (en adelante, Comité de Seguridad).

2. Objetivo

El buen funcionamiento de la FUNDACIÓ LLUÍS ALCANYÍS depende en gran medida de los Sistemas de Información[1] y de la Información que en ellos se almacena. La utilización de recursos tecnológicos para el tratamiento de la información es esencial y cumple con una doble finalidad para la organización:

- Facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión, y

  (DISPONIBILIDAD)

- Proporcionar información completa, homogénea, actualizada y fiable.

  (INTEGRIDAD)

Por ello, la utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier entidad pública y privada. Estos medios y recursos se ponen

[1] Siguiendo la definición dada por el ENS, en el ámbito de esta Normativa General se entiende por Sistema de Información todo conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. (RD 3/2010, ENS – Anexo IV – Glosario.)

a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la FUNDACIÓ LLUÍS ALCANYÍS determinar las normas, condiciones y responsabilidades bajo las cuales deben utilizarse.

La Normativa de Seguridad tiene como misión establecer objetivos de FUNDACIÓ LLUÍS ALCANYÍS, así como proteger los activos de información y alcanzar la mayor eficacia y seguridad en su uso. Estos objetivos incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento con la finalidad de proteger la información de FUNDACIÓ LLUÍS ALCANYÍS. El objetivo principal del desarrollo de esta Normativa de Seguridad por parte del Comité de Seguridad es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiere para el desempeño del trabajo, así como evitar pérdidas de información y accesos no autorizados a la misma.

Para lograr los objetivos en materia de seguridad resulta necesario definir obligaciones integradas por un conjunto de acciones positivas (deber de hacer algo) u omisivas (deber de abstenerse de hacer). Estas obligaciones derivan directamente de la naturaleza de las tecnologías de la información que constituyen nuestra herramienta natural de trabajo y no son otra cosa que la actualización del deber de secreto y de preservar la información administrativa que incumbe a todo empleado.

La seguridad es un instrumento al servicio de la organización y de todos los usuarios, capaz de proporcionar confianza en los sistemas, preservar el ejercicio de las funciones y responsabilidades propias de cada usuario y garantizar la calidad y veracidad de la información objeto de tratamiento.

La seguridad se articula en torno a cinco grandes objetivos-principios:

- **Confidencialidad**: La información perteneciente a la entidad debe ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- **Integridad**: La información de la FUNDACIÓ LLUÍS ALCANYÍS debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- **Autenticidad**: La información de la FUNDACIÓ LLUÍS ALCANYÍS es generada por un autor identificado que es imposible de suplantar, lo que incluye el no repudio de la información introducida pues se garantiza que el emisor de la información es quien dice ser.
- **Disponibilidad**: La información de la FUNDACIÓ LLUÍS ALCANYÍS está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad.
- **Trazabilidad**. Supone que las actuaciones de usuarios autorizados e identificados se pueden rastrear a posteriori para definir quién ha accedido o modificado una cierta información, de modo que puedan ser imputadas exclusivamente a su autor.

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a la FUNDACIÓ LLUÍS ALCANYÍS, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Estas dimensiones de la seguridad alcanzan no sólo al personal de la FUNDACIÓ LLUÍS ALCANYÍS sino también a los usuarios integrados en las organizaciones externas que se relacionan con la misma o prestan en ella sus servicios.

3. Ámbito de aplicación

Esta normativa es de aplicación y obligado cumplimiento para todo el personal que desempeñe sus funciones en los sistemas de información de la FUNDACIÓ LLUÍS ALCANYÍS, bajo el alcance del ENS. Se entiende por usuario de los Sistemas de Información:

1. Cualquier empleado perteneciente a la organización.
2. El personal de prestadores de servicios, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la FUNDACIÓ LLUÍS ALCANYÍS cuando utilice o posea acceso a sus Sistemas de Información.

Sus contenidos se basan en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

Bajo el alcance del ENS se entienden incluidos tanto los recursos informáticos como la información que puede ser tratada o extraída por ellos y cualquier soporte que la contenga.

4. Aprobación y vigencia

Esta normativa se difundirá a todo el personal mediante su publicación y entrará en vigor transcurrido un mes natural desde la fecha de aprobación por la Dirección de FUNDACIÓ LLUÍS ALCANYÍS.

La Normativa de Seguridad será mantenida, actualizada y adecuada a los fines de la empresa. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación.

5. Revisión y Evaluación

La gestión de esta Normativa General corresponde al Comité de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Proponer su revisión.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa General. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la

información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

6. Entorno de Gestión de la Seguridad

La FUNDACIÓ LLUÍS ALCANYÍS dispone de un Sistema de Gestión de Seguridad de la Información integrado con el cumplimiento de las obligaciones del Esquema Nacional de Seguridad. Todas las políticas y procedimientos a los que se hace referencia en este documento y en el Sistema han sido revisados, aprobados e impulsados por el Comité de Seguridad de la FUNDACIÓ LLUÍS ALCANYÍS.

El conjunto de obligaciones que derivan de esta Normativa se definen en directa relación con los activos protegidos y la sensibilidad de la información objeto de protección.

6.1. Utilización del Equipo Informático y de comunicaciones

La FUNDACIÓ LLUÍS ALCANYÍS facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional.

Así pues, los datos, dispositivos, programas y servicios informáticos que la organización pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y Servicios Informáticos de la entidad, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

6.2. Clasificación de la información

La información de la FUNDACIÓ LLUÍS ALCANYÍS está clasificada en 3 categorías dependiendo de su grado de confidencialidad. Todo empleado debe ser consciente de esta clasificación:

- **NO CLASIFICADA** (PÚBLICA): Esta información puede ser compartida sin restricciones.

- **RESTRINGIDA** (USO INTERNO Y DE DIFUSION LIMITADA): La información Restringida puede ser compartida entre el personal afectado por la presente normativa con competencia en su tratamiento y además con terceros interesados como administrados o proveedores vinculados con algún tipo de contrato si fuere necesario.

- **CONFIDENCIAL**: Esta información debe ser únicamente compartida entre personal que en virtud de sus funciones deba ser conocedor de la misma.

Corresponde al Comité de Seguridad la clasificación del conjunto del Sistema de información. Como principio general la información se clasifica como RESTRINGIDA.

En aquellos supuestos en los que resulte necesaria la reclasificación de alguna información o documento con motivo del desempeño de las funciones propias del servicio ésta será decidida por el correspondiente Responsable de la Información teniendo en cuenta las directrices fijadas por el Comité de Seguridad.

6.3. Manejo de la información

Las reglas de manejo y custodia de la Información Clasificada son las siguientes:

1. Toda persona que tenga conocimiento de cualquier Información Clasificada, voluntaria o involuntariamente, deberá mantener la oportuna reserva sobre la misma. Dicho deber de reserva no expira mientras la información afectada no sea desclasificada.

2. Los soportes físicos con información restringida o confidencial a desechar deberán ser físicamente destruidos de manera que se imposibilite la reconstrucción total o parcial de la información clasificada almacenada en estos.

3. En caso de transporte de equipos fuera de las instalaciones autorizadas se debe solicitar autorización al Responsable de Seguridad de la Información.

4. Para la información clasificada como restringida que se intercambia con determinadas partes interesadas externas (empresas, miembros de la entidad o proveedores, p.e.) debe realizarse a través de medios seguros y fiables y con una clara referencia a la distribución exclusiva del documento entre las personas autorizadas.

5. Para la información clasificada como confidencial en caso de transportar la información en soporte removible, este deberá ser adecuadamente cifrado y etiquetado. En el caso de transmitir este tipo de información por correo electrónico deberá ser cifrada.

7. Normas de Seguridad

A continuación, se detallan las Normas de Seguridad que todos los usuarios deben conocer y aplicar en su caso.

7.1. Normas Generales

1. Los equipos informáticos (PCs, dispositivos móviles, portátiles…), serán asignados por el departamento de informática.

2. Existirá un inventario actualizado de los equipos informáticos. El departamento de informática será la unidad encargada de gestionar dicho inventario.

3. A cada nuevo usuario que se incorpore a la organización y así lo precise, se le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales.

4. Para dar de alta nuevos usuarios en el sistema, RRHH comunicará la información necesaria para el alta de usuarios al departamento de informática mediante el formulario preparado para este fin. (TICKET ALTA DE EMPLEADO).

5. Los ordenadores personales deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

6. Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad. Cuando se precise instalar dispositivos no provistos por la entidad, se deberá solicitarse autorización previa al Responsable de Sistemas.

7. Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.

8. Salvo autorización expresa del Responsable de Sistemas, los usuarios no tendrán privilegio de administración sobre los equipos.

9. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.

10. Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo escalará y se tomaran las oportunas medidas correctoras y dará traslado de la incidencia.

11. Cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su correcto uso.

12. Dentro de las medidas de austeridad y reducción del gasto, se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios.
    - Apagar el PC (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
    - 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.

13. El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren de la participación de los usuarios para propagarse, ya sea a través de CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.

14. El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los

mismos, especialmente cuando se trate información sensible, confidencial o protegida.

15. El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al departamento de informática por RRHH, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por la FUNDACIÓ LLUÍS ALCANYÍS estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente cuando finalice su vinculación con dicho puesto o función.

16. No está permitido la conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la FUNDACIÓ LLUÍS ALCANYÍS, sin la previa autorización.

7.2. Normas específicas para el almacenamiento de información

1. Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. La entidad pondrá a disposición de los usuarios el espacio en red necesarios para el desempeño de su trabajo. (disco UV)

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

3. 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, siendo obligación del usuario la limpieza y optimización del espacio del disco asignado.

7.3. Normas específicas para equipos portátiles y móviles

1. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. Se deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.

2. Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales y autorizados, especialmente cuando se usen fuera de las instalaciones de la FUNDACIÓ LLUÍS ALCANYÍS.

3. Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la entidad o no autorizadas para ello.

7.4. Normas específicas para para memorias USB

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

2. La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento el departamento de Informática de forma inmediata.

3. Siempre que el contenido esté clasificado como confidencial o existan datos sensibles, las memorias USB deberán ir cifradas.

4. Sistemas de Información pondrá a disposición de los usuarios unidades de almacenamiento en red (personal, grupal y común), que podrán usarse para tal propósito o indicará que espacio en la nube está autorizado. (Disco UV)

7.5. Copias de Seguridad

1. Los datos generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, en una unidad de red compartida, evitando los duplicados y documentos innecesarios.

2. De forma periódica, se realizarán copias de seguridad de las unidades de red compartidas donde se almacene la información del usuario.

3. La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse al departamento de informática, mediante la generación de un ticket a través de la correspondiente herramienta.

7.6. Borrado y eliminación de soportes informáticos

1. Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información. En este sentido, el usuario deberá:

    - Asegurarse del contenido de cualquier soporte antes de su eliminación.
    - Cuando contenga información sensible, confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por la FUNDACIÓ LLUÍS ALCANYÍS. PR08.

7.7. Impresoras en red, fotocopiadoras y faxes

1. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras

locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la entidad y, en su consecuencia, estén debidamente inventariados.

2. Cuando se imprima documentación o se envíe un fax, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

3. Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del departamento de informática.

7.8. Digitalización de documentos

1. Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarlos, especialmente si contienen información sensible, confidencial o protegida.

2. Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del departamento de informática.

7.9. Cuidado y protección de la documentación impresa

1. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, utilizando la opción de impresión con código seguro, y debiendo ser recogida rápidamente de las impresoras para ser custodiada en armarios bajo llave.

2. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las maquinas destructoras, de forma que no sea recuperable la información que pudieran contener.

3. Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

7.10. Pizarras y flipcharts

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

7.11. Protección de la propiedad intelectual

1. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS sin la correspondiente licencia de uso.

2. Los programas informáticos propiedad están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa del departamento de informática.

3. 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.

7.12. Instalación de software

1. Únicamente el personal de soporte técnico autorizado por el departamento de informática podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

2. No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.

3. Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la entidad de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

4. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el departamento de informática, especialmente aquellas relacionadas con la seguridad.

7.13. Acceso a los sistemas de información y a los datos tratados

1. Los datos gestionados por la FUNDACIÓ LLUÍS ALCANYÍS y tratados por cualquier Sistema de Información deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

2. Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar en caso de mala utilización.

3. Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

4. Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar las salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 15 minutos.

5. La baja de los usuarios será comunicada por el departamento de RRHH, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

7.14. Identificación y autenticación

1. Los usuarios dispondrán de un código de usuario (user-id) y una contraseña (password), para el acceso a los Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

2. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

3. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

4. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar la correspondiente incidencia de seguridad.

5. El usuario deberá utilizar contraseñas robustas siguiendo las indicaciones siguientes:

    - La contraseña no deberá contener el nombre de la cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
    - Deberá tener una longitud mínima de siete (6) caracteres.
    - Deberá incluir caracteres de tres de las siguientes categorías:
        - Mayúsculas (de la A a la Z)
        - Minúsculas (de la a a la z)

- Dígitos de base 10 (del 0 al 9)
- Caracteres no alfanuméricos (por ejemplo, !, $, #, %)

6. Si, en un momento dado, un usuario recibiera una llamada telefónica solicitándole su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar este hecho al departamento de informática, de forma inmediata.

7. El acceso remoto a los sistemas de información deberá realizarse a través de red privada virtual (VPN).

7.15. Acceso de terceros a las instalaciones de la Fundació Lluís Alcanyís

1. Los terceros ajenos a la entidad que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, y tengan que acceder a las “Zonas Seguras” deberán cumplir la normativa de seguridad física publicada en el documento PR06-ControldeAccesoFisico.

7.16. Protección de datos de carácter personal y deber de secreto

1. Todo usuario que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la FUNDACIÓ LLUÍS ALCANYÍS, de conformidad con el documento “Contrato de Confidencialidad”.

2. La información contenida en las bases de datos de la entidad que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos de Carácter Personal. Los Tratamientos de datos de carácter personal gestionados por la misma han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

7.17. Tratamiento de la información

1. Toda la información contenida en los Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a su personal.

2. Cualquier tratamiento en los Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos.

3. Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia de la FUNDACIÓ LLUÍS ALCANYÍS en servidores externos (en la nube) a la entidad salvo autorización expresa del responsable, que

comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la entidad y la empresa responsable de la prestación del servicio "Encargado del Tratamiento", incluyendo el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

4. La salida de datos sensibles, confidenciales o protegidos, requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la normativa vigente en materia de Protección de Datos.

7.18. Uso del correo electrónico corporativo

1. El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la FUNDACIÓ LLUÍS ALCANYÍS, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

2. Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.

3. Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.

4. El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal.

5. Se deberá notificar al departamento de informática cualquier tipo de anomalía detectada en el uso del correo electrónico.

6. Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia al departamento de informática.

7. No está permitido el acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio, sin la debida autorización.

8. No se debe responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.

9. Se recomienda asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

10. Es recomendable evitar, en la medida de lo posible, el uso ineficiente en los envíos de correo: agrupar los envíos a múltiples destinatarios en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de los mismos), envíos innecesarios, etc.

11. No se permite el envío de contraseñas en plano a través del correo electrónico.

7.19. Acceso a internet y otras herramientas de colaboración

1. El acceso corporativo a Internet es un recurso centralizado que la FUNDACIÓ LLUÍS ALCANYÍS pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

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

3. Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos.

4. Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por la FUNDACIÓ LLUÍS ALCANYÍS en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del departamento de informática.

5. Se debe de evitar la descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.

6. No está autorizada la descarga de programas informáticos sin la autorización previa del departamento de informática. En todo caso debe asegurarse que el sitio Web visitado es confiable.

7.20. Incidencias de seguridad

1. Los usuarios deberán notificar al departamento de informática, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

2. Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS o su imagen, deberá informar inmediatamente al departamento de informática, que lo registrará debidamente y elevará, en su caso.

3. Deberá notificarse al departamento de informática cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

4. Todas estas notificaciones, se realizarán mediante la creación de un ticket a través la herramienta correspondiente.

7.21. Compromisos de los usuarios

1. Es responsabilidad directa del usuario:
   - Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore el departamento de informática, para garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.

   - En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa establezca al respecto.

7.22. Control de actuaciones sobre las bases de datos

1. La FUNDACIÓ LLUÍS ALCANYÍS podrán habilitar Sistemas de Información cuyo acceso y/o modificación de la información contenida quedarán registrados en una Base de Datos, lo que permitirá su ulterior auditoría.

2. Se prohíbe realizar cualquier tipo de actualización en Bases de Datos corporativas, masiva o puntual, desde fuera de las aplicaciones de la FUNDACIÓ LLUÍS ALCANYÍS sin la autorización previa del departamento de informática.

7.23. Monitorización y aplicación de esta normativa

1. La FUNDACIÓ LLUÍS ALCANYÍS, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente puede:

   a) Revisar periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

   b) Monitorizar los accesos a la información contenida en sus sistemas.

   c) Auditara la seguridad de las credenciales y aplicaciones.

   d) Monitorizar los servicios de internet, correo electrónico y otras herramientas de colaboración.

2. La FUNDACIÓ LLUÍS ALCANYÍS llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las

señaladas en la jurisprudencia y con observancia de los derechos de los usuarios

3. Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente, previo aviso del usuario. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El departamento de informática, con la colaboración de las restantes unidades de la FUNDACIÓ LLUÍS ALCANYÍS, velarán por el cumplimiento de la presente Normativa General.

4. El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

7.24. Modelo de aceptación y compromiso de cumplimiento

1. Todos los usuarios de los recursos informáticos y/o Sistemas de Información de la FUNDACIÓ LLUÍS ALCANYÍS deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa.

7.25. Publicación en web.

1. La publicación de contenidos en la web de la FUNDACIÓ LLUÍS ALCANYÍS se limitará a los documentos o informaciones con clasificación pública.

5. Se retirará de estos documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente.

6. La información publicada debe garantizar los principios de autenticidad e integridad.

7. Los gestores y editores de páginas web asegurarán la disponibilidad de la información durante el periodo previsto de vigencia de la misma procediendo a su retirada cuando se produzca el vencimiento.

7.26. Publicación de información en redes sociales

1. El usuario respetará el buen nombre, marca comercial, identidad corporativa e identidad digital y marca personal de la FUNDACIÓ LLUÍS ALCANYÍS en todos los medios de comunicación incluidas las redes sociales. En particular, el usuario no podrá llevar a cabo ninguna de las siguientes actuaciones:

   a) Revelar información interna de la empresa.

b) Revelar información sobre sus compañeros de trabajo ni trabajos desarrollados en la entidad, ni de sus clientes y/o proveedores u otras personas con quienes la organización mantenga relaciones jurídicas.

c) Utilizar los medios de comunicación y redes sociales para desprestigiar a la empresa.

d) Crear páginas oficiales de la FUNDACIÓ LLUÍS ALCANYÍS en redes sociales sin autorización.

e) Publicar información en medios de comunicación y redes sociales en nombre y representación de la FUNDACIÓ LLUÍS ALCANYÍS sin autorización.

f) Utilizar los logos, nombres, marcas, gráficos, iconos y en general, simbologías identificativas en medios de comunicación y redes sociales sin autorización.

7.27. Directrices de puesto de trabajo despejado

1. La documentación que no se está utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando dejamos nuestro puesto de trabajo y al finalizar la jornada.

2. La información se destruirá de manera segura, haciendo uso de las destructoras de papel.

3. No se conservarán contraseñas en lugares visibles alrededor del puesto de trabajo (apuntadas en post-it o similares).

4. El puesto de trabajo estará limpio y ordenado.

5. El usuario bloqueará el ordenador cuando este quede desatendido.

8. Incumplimiento de la Normativa

Todos los usuarios de los sistemas de información están obligados a cumplir la presente Normativa de Seguridad. Su incumplimiento genera responsabilidad que se sustanciará conforme al procedimiento establecido al efecto en cada caso.