DOCUMENTO DE SEGURIDAD

Reglamento de desarrollo de la Ley Orgánica de Protección de Datos

Fecha de Elaboración

05/11/15

Fecha de Revisión

23/11/16

Elaborado por:

GUADALTEL, S.L

Versión

1

Contenido

1. Introducción.

La Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) dispone, en su artículo 9, la obligación del Responsable del Fichero de adaptar las medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciendo asimismo en el artículo 44.3 letra h) que constituye una infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen."

La obligación de seguridad dispuesta en el artículo 9 de la LOPD viene desarrollada en el Reglamento de Desarrollo de la misma, aprobado por Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RLOPD).

El Título VIII del RLOPD tiene por objeto el desarrollo de las medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad, confidencialidad e integridad de los ficheros de datos personales, con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales, frente a su alteración, pérdida, tratamiento o acceso no autorizado.

El artículo 88 del RLOPD, establece la obligación de elaborar e implantar la normativa de seguridad mediante un documento de obligado cumplimiento para todo el personal con acceso a los sistemas de información. El presente Documento de Seguridad responde a esa obligación legal recogiendo las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los ficheros que contienen datos de carácter personal de ICEX.

Al conjunto de ficheros, programas, soportes, sistemas y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal, se hará referencia de forma indistinta a sistemas de información.

El RLOPD establece tres niveles de seguridad, básico, medio, alto, atendiendo a la naturaleza de la información tratada, en relación con mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información. Estas medidas y procedimientos deberán ser acatadas por todos los usuarios de los sistemas de información pertenecientes a ICEX.

2. Objeto y finalidad del documento.

De conformidad con el artículo 88 del RLOPD, el Documento de Seguridad recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para todo el personal que tenga acceso a datos de carácter personal, así como a los sistemas de información. Es obligación del responsable del fichero la elaboración e implantación de la normativa de seguridad, mediante el presente documento.

El Documento de Seguridad tiene por objeto establecer en ICEX, de acuerdo con la LOPD y el RLOPD las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

El Documento de Seguridad deberá mantenerse actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

3. Ámbito de aplicación y recursos protegidos.

El ámbito de aplicación del presente Documento de Seguridad comprende los ficheros que contienen datos de carácter personal, los sistemas de información, soportes y equipos empleados, instalaciones y personal propio o ajeno que intervienen en el tratamiento y los locales donde se ubican.

Todas las personas que tienen acceso a los datos del Fichero, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento.

Una copia de este documento será entregada o puesta a disposición, para su conocimiento, a cada persona autorizada a acceder a los datos de los ficheros que contengan datos de carácter personal, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

Las medidas de seguridad se clasifican en tres niveles acumulativos, con carácter de mínimos exigibles atendiendo a la naturaleza de los datos que contienen los ficheros, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información. Estos niveles son:

- **Nivel Básico:** Cualquier fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

    1. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros.

    2. Se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero.

    3. En los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

- **Nivel Medio:** Ficheros o tratamiento de datos:

    1. Relativos a la comisión de infracciones administrativas o penales, que se rijan por el artículo 29 de la LOPD de servicios de información sobre solvencia patrimonial y crédito.

    2. De Administraciones Tributarias y que se relacionen con el ejercicio de sus potestades tributarias.

    3. De entidades financieras para las finalidades relacionadas con la prestación de servicios financieros.

    4. De entidades gestoras y servicios comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias.

    5. De mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

    6. Que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas.

7. De los operadores de telecomunicaciones o comunicaciones electrónicas, respecto de los datos del tráfico y localización.

- **Nivel Alto**: Ficheros o tratamiento relativos a datos:

1. De ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, respecto de los cuales no se prevea la posibilidad de adoptar nivel básico.

2. Recabado con fines policiales sin consentimiento de las personas afectadas.

3. Derivados de actos de violencia de género.

3.1. Alcance y glosario de términos

El presente Documento de Seguridad tiene por objeto establecer en ICEX España Exportación e Inversiones (en adelante, indistintamente ICEX o la Entidad) las medidas técnicas y organizativas necesarias para garantizar la seguridad y buen uso que deben reunir los ficheros automatizados y no automatizados con datos de carácter personal, los centros de tratamiento, locales, equipos, sistemas, programas y las personas, sujetos al régimen de la LOPD y el RLOPD, y cualquier otra disposición legal al respecto o norma interna.

El presente documento es de aplicación a ICEX como entidad ubicada en territorio español, de acuerdo con los artículos 2 y 3 de la LOPD y del RLOPD, respectivamente.

De acuerdo con la Ley, ICEX como responsable de los ficheros de datos de carácter personal registrados a su instancia, así como de los tratamientos de los mismos debe implantar las medidas de seguridad con arreglo a lo dispuesto en el Título VIII del RLOPD, con independencia de cuál sea su sistema de tratamiento. En este sentido, ICEX se compromete a implantar y garantizar la efectiva aplicación de la normativa de seguridad contenida en el presente documento, cuyo incumplimiento podría suponer una infracción de la normativa vigente en materia de protección de datos.

A través de cursos, seminarios, comunicaciones, etc. que se realizarán con, al menos, una periodicidad anual, se garantiza la divulgación de esta normativa a todo el personal de ICEX.
Los ficheros afectados por esta normativa son los dados de alta por ICEX, registrados en la Agencia Española de Protección de Datos (en adelante, AEPD), y a su vez incluidos en los sistemas de control interno de ICEX entendiéndose que todos y cada uno de los ficheros con datos personales existentes en ICEX han sido registrados en la misma.

Una vez el interesado ha sido informado de que sus datos van a ser incorporados a un fichero registrado en la AEPD, para unos fines determinados, el tratamiento de éstos datos estará legitimado, pero únicamente podrán tratarse dichos datos de carácter personal para esa finalidad para la que hayan sido recogidos.

El Documento de Seguridad es de obligado cumplimiento para todo el personal de ICEX que trate o acceda a datos personales responsabilidad de ICEX. Todas las personas que tengan acceso a los datos de los ficheros a los que hace referencia el presente Documento de Seguridad, bien a través de los sistemas informáticos existentes para estos efectos, o bien a través de cualquier otro medio automatizado o no de acceso, se encuentran obligadas por Ley a cumplir lo establecido en el mismo, y sujetas a las consecuencias que pudieran derivarse en caso de incumplimiento.

El personal de ICEX tendrá acceso a las partes de este documento que necesite para realizar sus funciones, así como a la Política de Seguridad para Usuarios recogida en el mismo, a través de distintos medios tales como: curso o manual de bienvenida, publicación del documento en la red corporativa, u otros medios de formación que se consideren adecuados.

Para garantizar una mayor comprensión de este documento a todos los destinatarios del mismo se incluye a continuación un glosario con las definiciones y términos utilizados a lo largo de mismo.

TÉRMINO	DEFINICIÓN
Accesos autorizados	Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.
Administradores	Deberán disponer de una relación actualizada de todo su personal que tenga acceso a datos de carácter personal o procesos que los administren, indicando las funciones asignadas a cada colaborador.
Afectado o interesado	Persona física titular de los datos personales que se incluyan en ficheros automatizados o manuales.
Autenticación	Procedimiento de comprobación de la identidad de un usuario (Contraseña de cada usuario).
Bloqueo de datos	La identificación y reserva de los datos (un registro o varios registros) con el fin de impedir su tratamiento. El bloqueo puede producirse por iniciativa propia o a instancias del afectado.
Código de usuario	Información no confidencial, frecuentemente constituida por una cadena de caracteres previamente establecida, que se usa para identificar al usuario
Comunicación, cesión o transferencia de datos	Toda revelación de datos realizada por el Responsable del Fichero a una persona física o jurídica distinta del afectado, tanto dentro como fuera del territorio nacional pudiendo hacer uso de los mismos para fines propios.
Consentimiento del interesado	Manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el afectado o interesado consiente el tratamiento de datos personales que le conciernen. Tipos de consentimiento: • Tácito: derivado de una información aportado al afectado/interesado relativa a que sus datos van a formar parte de un fichero de datos personales, sin que dicho afectado haya comunicado expresamente su negativa. Se aplica a los ficheros de seguridad básica y media. • Expreso: lo da por escrito el afectado, considerando como negativa del mismo a formar parte del fichero de datos personales la no existencia de dicho consentimiento expreso. Se aplica a los ficheros de seguridad alta. El consentimiento podrá otorgarse en cualquiera de las formas admisibles en Derecho, siendo requisito imprescindible para su validez que no se recabe por medios fraudulentos desleales o ilícitos. Teniendo en cuenta que el consentimiento tácito no tiene valor de prueba a favor en caso de demanda judicial, se debe ir progresivamente hacia el consentimiento expreso en todos los casos.
Contraseña	Información confidencial, frecuentemente constituida por una cadena de caracteres, que es usada para la autenticación de un usuario.
Control de acceso	Mecanismo que en función de la identificación y la autenticación permite conocer los accesos a datos o recursos.
Copia de respaldo	Copia de los datos de un fichero automatizado en un soporte que posibilite su almacenamiento, identificación y recuperación (back-up).

Datos de carácter personal	Cualquier información concerniente a personas físicas identificadas e identificables, con independencia de número de campos. En principio cualquier agrupamiento de datos personales partiendo de un solo identificador (p.ej. nombre, DNI, NIF, número de pasaporte o Seguridad Social, número de matrícula dentro de iCEX, número de proveedor, número de cliente, etc.) junto con otro u otros identificadores de carácter personal, incluidos los referidos, está sujeto a la aplicación de la legislación de protección de datos de carácter personal y consecuentemente a los procedimientos indicados en este Documento y en cualquier otra normativa interna.
Fichero	Todo conjunto organizado de datos de carácter personal, implementado de manera automatizada o manual, que nos permita su almacenamiento, acceso y gestión.
Fuentes accesibles al público	Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Exclusivamente tienen la consideración de fuentes de acceso público el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.
Identificación del afectado	Cualquier elemento que permita determinar directa o indirectamente la identidad física o antropométrica, fisiológica, psíquica, económica, cultural o social de la persona afectada.
Identificación del usuario	Procedimiento de reconocimiento de la identidad de un usuario (Código de usuario).
Incidencia	Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos
Procedimiento de disociación	Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
Transporte de datos	El trasiego de datos entre sistemas informáticos por cualquier medio de transmisión, así como el envío físico de datos por correo o por cualquier otro medio convencional.
Tratamiento de datos	Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, impresión, conservación, elaboración, evaluación, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Recurso	Cualquier parte componente de un sistema de información (Hardware y Software).
Responsable del fichero	El responsable del fichero es, a todos los efectos, ICEX, como entidad jurídica de naturaleza pública, que decide sobre su finalidad, contenido y uso. El responsable del fichero es el encargado jurídicamente de la seguridad de los ficheros y de las medidas de seguridad establecidas en el presente documento, y se responsabiliza de implantar las medidas de seguridad establecidas en él y adoptar las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Funciones y obligaciones del Responsable del Fichero	Notificar a la AEPD los ficheros con datos personales de la Entidad. Velar por el cumplimiento de todos los requisitos establecidos en la LOPD y en el RLOPD, así como de otra legislación que pudiera afectar. Redactar, implantar y comprobar la aplicación y el cumplimiento del presente Documento de Seguridad. Garantizar la difusión de los datos necesarios de este documento entre todo el personal que vaya a utilizarla, sobre todo en cuanto a las obligaciones derivadas del mismo, e informar acerca de las consecuencias en que pudiera incurrir en caso de incumplimiento. Mantener actualizado este documento siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo, según el artículo 88.7 del RLOPD. Adecuar en todo momento el contenido del mismo a las disposiciones vigentes en materia de seguridad de datos. Describir los sistemas de información que gestionan el tratamiento de los datos personales de ICEX. Describir la estructura del fichero de datos. Establecer los criterios que el Responsable de Seguridad debe seguir al conceder, alterar o anular el acceso autorizado a los datos y recursos. Establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos/perfiles distintos de los autorizados. Autorizar la salida de soportes informáticos que contengan datos del fichero fuera de los locales donde esté ubicado. Aprobar o designar al administrador que se responsabilizará del sistema operativo y de comunicaciones. Verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos. Cualesquiera otras que se mencionen en este Documento de Seguridad.
Responsable de Seguridad	Actúa como responsable del establecimiento, coordinación y control de las medidas técnicas necesarias, de seguridad informática y de comunicaciones, para el desarrollo específico del RLOPD o de cualquier otra normativa externa o interna sobre este tema. Mantendrá una relación actualizada de su personal administrador autorizado que maneje datos de carácter personal o procesos que los administren, realicen copias de seguridad y back-up o tengan acceso a locales donde se encuentra ubicados los sistemas de información y comunicación. En esta relación estarán descritas las funciones asignadas a cada colaborador. De igual forma figurarán en la referida relación las personas que tengan potestad para autorizar el acceso a los locales restringidos a personas que no dispongan de una autorización permanente.

Funciones y obligaciones del Responsable de Seguridad	Coordinar la puesta en marcha de las medidas de seguridad. Colaborar con el Responsable del Fichero en la necesaria difusión del presente Documento de Seguridad. Coopera con el Responsable del fichero controlando el cumplimiento del mismo. Habilitar un Registro de Incidencias a disposición de todos los usuarios y administradores de los ficheros, con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad del mismo. Analizar las incidencias registradas, tomando las medidas oportunas en colaboración con el Responsable del Fichero. En el caso de que los datos de los ficheros sean de nivel medio o alto, al menos cada dos (2) años, se realizará una auditoría externa prevista en el RLOPD, que dictamine el correcto cumplimiento y la adecuación de las medidas del presente Documento de Seguridad o las exigencias del Reglamento, identificando las deficiencias y proponiendo las medidas correctoras necesarias. En tal caso, los informes de auditoría serán analizados por el Responsable de Seguridad, quien propondrá la Responsable del Fichero las medidas correctoras correspondientes. Los resultados de las referidas auditorías y de los controles periódicos serán adjuntados al presente Documento de Seguridad.
Sistema de Comunicaciones	Procedimientos electrónicos de redes de comunicaciones que realizan el envío/recepción de datos, tanto local como externamente.
Sistema de Información	Conjunto de ficheros automatizados, programas, soportes y equipos empleados en el almacenamiento y tratamiento de datos de carácter personal.
Soporte	Objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se puede grabar o recuperar datos (cintas, discos, CD, disquetes, Pen-drive, etc.).
Tratamiento en terceros	Actividades fuera de la compañía por externalización de tareas, con prohibición expresa a esos terceros del uso de los datos para fines propios.
Usuario	Cualquier persona interna o externa que acceda a datos personales. La relación de usuarios autorizados para el acceso y utilización de datos personales, quedará recogida por cada fichero.

3.2 Recursos protegidos.

El RLOPD establece que en el Documento de Seguridad se deberá incluir la especificación detallada de los recursos protegidos a los que les son de aplicación las medidas de seguridad contenidas en dicho documento.

3.2.1 Relación de ficheros.

Los ficheros que contienen datos de carácter personal sujetos a las medidas de seguridad recogidas en este documento constan relacionados en el Anexo I: Relación de Ficheros

El contenido de los ficheros, así como la confirmación de su inscripción en el Registro General de Protección de Datos, se conservará indefinidamente en la Dirección Adjunta de Asesoría Jurídica y Ayudas.

La inscripción de un fichero se puede consultar en el Catálogo de ficheros inscritos en el Registro General de Protección de Datos en la sección de Ficheros inscritos de la página web de la AEPD en el siguiente enlace Consulta de Ficheros Inscritos.

La información que se hace pública en el citado catálogo se corresponde con la información que el responsable del fichero, ICEX, ha notificado al Registro General de Protección de Datos (en adelante, RGPD) en los apartados siguientes:

- Responsable del fichero.
- Servicio o unidad ante el que pueden ejercitarse los derechos de oposición, acceso, rectificación y cancelación.
- Identificación y finalidad.
- Usos previstos del fichero, origen y procedencia de los datos
- Colectivo de personas sobre el que se obtienen los datos de carácter personal
- Tipos de datos, estructura y organización del fichero
- Destinatarios de cesiones y/o transferencias internacionales de datos
- Datos relativos a la disposición general de creación, modificación o supresión del fichero.

También la persona que haya presentado la última notificación relacionada con la inscripción del fichero o la persona que haya sido debidamente autorizada por el responsable del mismo podrá identificarse mediante su certificado electrónico de firma, para consultar la información relativa al código de inscripción, nivel de medidas de seguridad declarado, así como los datos consignados en el apartado de encargado de tratamiento solicitando una copia de la Inscripción de los Ficheros en la página web de la AEPD mediante el siguiente enlace :Solicitud de Copia de la Inscripción de Ficheros, o bien mediante escrito dirigido a la Agencia Española de Protección de Datos, C/Jorge Juan, 6, 28001-MADRID, firmado por la persona que represente al responsable del fichero

3.2.2 Centro de tratamientos.

Los locales donde residen los sistemas de información involucrados en el tratamiento están ubicados en los centros de ICEX afectados por el ámbito de este Documento de Seguridad, los cuales son los siguientes:

- Paseo de la Castellana nº 278, Madrid.
- Avda. Cardenal Herrera Oria nº 378, Madrid.
- Informática El Corte Inglés, S.A. (IECISA) en Murcia C/ Santiago Navarro, 8.

El presente Documento de Seguridad es de aplicación a todos los Locales y Centros de tratamiento de datos personales responsabilidad de ICEX. La actualización de los mismos es responsabilidad del Departamento de Secretaría General.

3.2.3 Inventario de recursos.

La relación del software y hardware empleados en el tratamiento, la descripción del sistema de información y los soportes utilizados, se recogen en los siguientes anexos:

Anexo II: Inventario de Equipos:

1. Servidores y Centros de Proceso de Datos

El presente Documento de Seguridad es de aplicación a todos los Servidores y Centros de Proceso de Datos (en lo sucesivo, CPD) que den soporte al sistema de información destinado al tratamiento de datos personales responsabilidad de ICEX.

El ANEXO II contiene la relación de dichos servidores y CPD's. Su actualización es responsabilidad del Departamento de Tecnologías de la Información.

2. Equipos Informáticos

El presente Documento de Seguridad es de aplicación a todos los equipos informáticos destinados al tratamiento de datos personales responsabilidad de ICEX.

El ANEXO III contiene la relación de equipos informáticos u ordenadores personales destinados al tratamiento de datos personales. Su actualización es responsabilidad de la Dirección de Tecnología de la Información.

Anexo III: Inventario de Software

1. Aplicaciones informáticas

El presente Documento de Seguridad es de aplicación a todas las aplicaciones informáticas destinadas al tratamiento de datos personales responsabilidad de ICEX.

El ANEXO III contiene la relación de aplicaciones informáticas que se emplean para el tratamiento de datos personales. Su actualización es responsabilidad del Departamento de Tecnologías de la Información.

2. Armarios y Dispositivos de Almacenamiento de Datos en Soporte Papel.

El presente Documento de Seguridad es de aplicación a todos los Armarios y Dispositivos de Almacenamiento de datos personales responsabilidad de ICEX.

El Anexo IV contiene la relación de armarios y dispositivos de almacenamiento. Su actualización es responsabilidad del Departamento de Servicios Generales de ICEX.

Anexo IV: Inventario de Soportes.

1. Soportes y Dispositivos de Almacenamiento Digital que contienen datos de carácter personal

El presente Documento de Seguridad es de aplicación a todos los soportes (CD, DVD, HDD interno/externo, SSD, pendrive, tarjeta de memoria flash, etc.) que contengan de datos personales responsabilidad de ICEX.

Cada departamento llevará un inventario de estos dispositivos y será responsabilidad de los mismos la actualización del Anexo IV en este apartado.

2. Gestión de soportes

En el presente apartado del Anexo IV relativo a la Gestión de soportes se debe llevar un control y registro tanto de entrada como de salida.

Cada departamento llevará el control de entrada y salida de soportes y será responsabilidad de los mismos la actualización del Anexo IV en este apartado.

3.3 Personal.

Todo el personal que trate datos de carácter personal u otros datos propiedad de ICEX, entendiéndose como tratamiento cualquier tipo de operación o procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, impresión, conservación, elaboración, evaluación, modificación, bloqueo y cancelación, en una o varias de estas fases, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias y tratamiento en terceros, está obligado a observar las medidas de seguridad contenidas en el presente Documento de Seguridad.

3.3.1 Consideraciones para el personal en general

Todos los usuarios internos y externos del sistema de información de ICEX deberán conocer y respetar sus funciones y obligaciones en materia de protección de datos y de seguridad de la información.

El incumplimiento por parte del usuario del sistema de información de las siguientes funciones y obligaciones, podrá ser considerado como una falta grave en el trabajo (en atención al catálogo recogido en el Convenio

Colectivo de ICEX), que constituye una de las causas de despido disciplinario de acuerdo con la legislación laboral que resulte de aplicación al personal de la Entidad.

3.3.1.1 Funciones.

- Tratar únicamente datos adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, siempre de acuerdo con las instrucciones que reciba del Responsable de Seguridad del Departamento.

- Actualizar los datos personales cuando tenga conocimiento efectivo de que han sufrido cambios, siempre previa información al Responsable de Seguridad del Departamento.

- Informar y solicitar el consentimiento de los afectados según las instrucciones del Responsable de Seguridad de su Departamento cuando se recaben datos personales, así como teniendo en cuenta lo indicado en la Circular Interna recogida en el Anexo V: Circular personal LOPD relativa a “Adaptación de formularios de recogida de datos a la normativa de protección de datos de carácter personal”.

- Acceder únicamente a los datos que necesite para el ejercicio de las funciones que le hayan sido encomendadas por cualquiera de sus responsables.

- Tratar los datos personales a los que tenga acceso con el máximo respeto y confidencialidad y únicamente para las tareas que le hayan sido encomendadas por cualquiera de sus responsables.

- Informar a cualquier persona que lo solicite del procedimiento definido por ICEX para ejercer los derechos de acceso, rectificación, cancelación y oposición (en adelante, Derechos ARCO), según lo establecido en el apartado 8 de este documento donde se define el Protocolo a seguir para el ejercicio de los Derechos ARCO.

- Como parte afectada por el tratamiento de datos, el personal de ICEX también puede ejercitar los Derechos ARCO a sus propios datos personales, siempre y cuando no sean incompatibles con la propia relación contractual.

- En caso de reclamaciones o consultas realizadas por personas afectadas por el tratamiento de sus datos personales, observaremos los procedimientos y límites de fechas recogidos establecido en el apartado 8 de este documento donde se define el Protocolo a seguir para el ejercicio de los Derechos ARCO.

3.3.1.2 Obligaciones.

- Obligación de guardar secreto profesional y de confidencialidad en el tratamiento de datos a los que tengamos acceso. Esta obligación subsistirá aun después de finalizar la asignación de las tareas o incluso después de finalizar las relaciones contractuales de trabajo con ICEX. El incumplimiento de las obligaciones descritas podrá ser constitutivo de las acciones que se deriven de la ley.

- Queda prohibido hacer uso personal de los datos de los ficheros, soportes y documentos y otros datos propiedad de ICEX.

- La existencia de bases de datos de carácter personal que incumplan las leyes, las instrucciones o las normas internas debe ser comunicada de inmediato al Responsable de Seguridad del Departamento, para que éste actúe en consecuencia y tome las medidas que estime oportunas.

- Conocer y respetar el presente Documento de Seguridad.

- Guardar el secreto profesional respecto de los datos personales responsabilidad de ICEX a los que acceda, incluso después de finalizar su relación con ICEX.

- Informar al Responsable de Seguridad del Departamento acerca de la creación de cualquier fichero o base de datos de carácter personal conforme al procedimiento descrito en el presente Documento de Seguridad.
- Notificar cualquier incidencia que afecte a la seguridad de la información a través del procedimiento descrito en el presente Documento de Seguridad.

- Utilizar de forma adecuada los mecanismos de control de acceso implantados por ICEX conforme a lo descrito en el presente Documento de Seguridad, teniendo especial cuidado en la confidencialidad de sus claves y contraseñas de acceso al sistema operativo o a las aplicaciones destinadas al tratamiento de datos personales responsabilidad de ICEX.

- Solicitar autorización para sacar equipos o soportes que contengan datos personales, así como para el envío de información fuera de la Entidad conforme al procedimiento descrito en el presente Documento de Seguridad.

- Trabajar en el entorno seguro descrito por ICEX para garantizar la seguridad de la información y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

- Archivar los documentos que contengan datos personales conforme a los criterios definidos por el Responsable de Seguridad del Departamento, o persona en la que éste hubiese delegado.

- Utilizar correctamente los armarios y dispositivos de almacenamiento de documentos, empleando los mecanismos de cierre de que disponga dicho dispositivo y respetando los procedimientos establecidos por el Responsable de Seguridad del Departamento para la conservación de dichos mecanismos.

- Custodiar la documentación con la que esté trabajando conforme a lo descrito en el presente Documento de Seguridad, especialmente cuando se haya impreso, fotocopiado, escaneado o enviado por fax desde dispositivos comunes a uno o varios departamentos.

- Destruir las fotocopias de documentos a través de medios que impidan su recuperación posterior, según las instrucciones del Responsable de Seguridad del Departamento.

- Devolver todas las llaves, claves, tarjetas de identificación, material, documentación, equipos, contraseñas y cuantos activos sean propiedad de ICEX cuando le sea requerido y en todo caso, cuando abandone la Entidad.

- Conocer el procedimiento establecido por ICEX para el ejercicio de los Derechos ARCO.

- En el traslado físico de la documentación, adoptar medidas dirigidas a impedir el acceso no autorizado a la información, según las instrucciones del Responsable de Seguridad del Departamento.

- Utilizar de forma adecuada y responsable los recursos que le hayan sido facilitados por ICEX para el desarrollo de su actividad laboral de acuerdo con lo dispuesto en el Anexo VI: Política de Seguridad para Usuarios del presente Documento de Seguridad.

3.3.2 Funciones y obligaciones del responsable del fichero.

El responsable de un fichero o tratamiento es la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales.

3.3.2.1 Funciones.

- Decidir sobre la finalidad, contenido y uso del tratamiento.
- Autorizar:
  - La ejecución de tratamientos de datos de carácter personal fuera de los locales de la ubicación el fichero
  - Salida de soportes informáticos que contengan datos de carácter personal fuera de los locales de la ubicación el fichero
- Realizar el control del tratamiento, calidad y seguridad de los datos.
- Controlar la gestión de soportes informáticos que contengan datos de carácter personal
- Gestionar y dirigir los procedimientos de acceso, rectificación, cancelación y oposición de los afectados y resolver:
  - La petición de acceso en el plazo de un (1) mes.
  - La petición de rectificación, cancelación y oposición en el plazo de diez (10) días
- Proceder al bloqueo de datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa de procedimiento o soporte utilizados.
- Elaborar el Documento de Seguridad
- Encargarse de la existencia de una relación actualizada de usuarios con acceso autorizado a los sistemas de información
- Establecer procedimiento de autenticación e identificación para dichos procesos.
- Establecer los mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Establecer los procedimientos de realización de copias de respaldo y recuperación de datos.
- Encargarse de forma directa o por delegación, del cumplimento efectivo de la normativa sobre protección de datos en ICEX, garantizando la difusión y conocimiento de este documento entre todo el personal.
- Implantación de las medidas de seguridad establecidas en el RLOPD.
- Mantener el Documento de Seguridad actualizado en todo momento, debiendo revisarse siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo y adecuar su contenido a las disposiciones vigentes en materia de seguridad de datos.

- Garantizar los bienes jurídicos y recursos protegidos.
- Designar a uno o varios responsables de seguridad.
- Cumplir en cada momento con el ordenamiento jurídico vigente en relación a los datos de carácter personal.

3.3.2.2 Obligaciones.

- Legalización de ficheros.
- Legitimación para el tratamiento de los datos.
- Control de las entradas en el fichero.
- Mantenimiento actualizado de los datos.
- Controlar a encargados de tratamiento externos.
- Gestión de entorno de sistema operativo y de comunicaciones.
- Gestión del Sistema informático o aplicaciones de acceso al fichero.
- Salvaguarda y protección de las contraseñas personales.
- Gestión de incidencias.
- Gestión de soportes.
- Procedimientos de respaldo y recuperación
- Auditoría.

ICEX nombrará los siguientes responsables, pudiendo recaer sobre una misma persona varias responsabilidades distintas

- Comité de Seguridad.
- Responsable de Seguridad de cada Departamento.
- Responsable ARCO.
- Responsable NOTA.
- Responsable de la Dirección de Tecnologías de la Información.

Cada uno de estos Responsables deberá suscribir sus respectivas FUNCIONES Y OBLIGACIONES específicas para su cargo a través de lo definido la hoja de su nombramientos.

Anexo X: Nombramiento Responsable de Seguridad

ICEX podrá adoptar medidas de vigilancia y control para verificar el cumplimiento de estas funciones y obligaciones, informando previamente a los afectados de dichas medidas adoptadas.

El Comité de Seguridad LOPD trimestralmente analizará el estado del cumplimiento de la normativa en ICEX y tomará las medidas oportunas para corregir las deficiencias que se detecten.

3.3.3 Comité de Seguridad.

Además de las Funciones y Obligaciones Generales, asumidas en su condición de Usuario, el Comité de Seguridad deberá cumplir con las siguientes:

3.3.3.1 Funciones.

- Detectar posibles deficiencias en la seguridad de ICEX y analizar las posibles soluciones de forma conjunta con el Responsable de la Dirección de Tecnologías de la Información.
- Planificar y ejecutar las auditorías de verificación del cumplimiento de las medidas de seguridad conforme a lo dispuesto en el presente Documento de Seguridad.
- Analizar los informes de auditoría.

3.3.3.2 Obligaciones.

- Mantener los anexos del presente Documento de Seguridad de forma conjunta con el Responsable de la Dirección de Tecnologías de la Información.
- Coordinar y controlar las medidas definidas en el presente Documento de Seguridad.
- Conocer la normativa vigente en materia de protección de datos.
- Actualizar el Documento de Seguridad en caso de cambios normativos.
- Elevar al máximo responsable de ICEX las conclusiones del análisis del informe de auditoría.

3.3.4 Responsable de Seguridad de cada Departamento.

Además de las Funciones y Obligaciones Generales, asumidas en su condición de Usuario, el Responsable de Departamento deberá cumplir con las recogidas en el apartado de éste Documento de Seguridad dedicado al Responsable de Seguridad de cada Departamento.

En ICEX se constituye a un Responsable de Seguridad por cada departamento, el cual tendrá las siguientes funciones:

- En el caso del Responsable de Seguridad por Departamento de Recursos Humanos, se adoptarán las medidas necesarias para que el personal interno y externo conozca sus funciones y obligaciones en materia de protección de datos, ya sea a través de la firma del contrato laboral, o a través de la

firma de un documento que recoja las Funciones y Obligaciones Generales recogidas en el presente Documento de Seguridad. En cualquier caso, se conservará acreditación del cumplimiento de esta función.

- Decidir sobre la finalidad, contenido y uso de un fichero cuando algún empleado a su cargo le haya expresado la necesidad de crearlo, y seguir el procedimiento descrito en el presente Documento de Seguridad para la notificación de ficheros.
- Decidir sobre la modificación o eliminación de ficheros de su departamento, y seguir el procedimiento descrito en el presente Documento de Seguridad para la notificación de ficheros.
- Autorizar la creación de nuevos formularios de recogida de datos dentro de su departamento de forma que lleven incorporada las cláusulas informativas pertinentes.
- Autorizar la concesión, modificación y supresión de permisos de acceso a ficheros y recursos de la Entidad para los empleados a su cargo.
- Autorizar la salida de equipos portátiles y soportes fuera de los locales de ICEX.
- Autorizar la salida de ficheros fuera de los locales de ICEX, incluidos los adjuntos a un correo electrónico.
- Solicitar el alta, baja o modificación de usuarios y contraseñas para los empleados a su cargo.
- Autorizar los procedimientos de restauración de los ficheros de Nivel Medio y Alto de su departamento.
- Autorizar la copia o reproducción de documentos que contengan información clasificada de Nivel Alto.
- Autorizar el acceso a la documentación de su departamento clasificada de Nivel Alto.
- Controlar directamente los mecanismos que registren el acceso a los ficheros de Nivel Alto que sean responsabilidad de su departamento.

De otra parte, las obligaciones del Responsable de Seguridad de cada Departamento serán:

- Colaborar con el Responsable ARCO cuando se reciba una solicitud de ejercicio de Derechos ARCO.
- Definir los criterios de archivo de la documentación dentro de su departamento.
- Controlar el buen uso de los dispositivos de almacenamiento de la documentación dentro de su departamento.
- Controlar que el personal a su cargo custodia debidamente la documentación del departamento.
- Controlar el acceso a las áreas donde se encuentren los dispositivos de almacenamiento de ficheros de nivel alto de su departamento.
- Colaborar en el mantenimiento de los anexos del presente Documento de Seguridad.
- Conocer y aplicar los procedimientos establecidos en el presente Documento de Seguridad para su difusión entre el personal a su cargo.

- Controlar directamente los mecanismos que registren el acceso a los ficheros de Nivel Alto que sean responsabilidad de su departamento.
- Revisar mensualmente el registro de accesos a los ficheros de Nivel Alto que sean responsabilidad de su departamento.
- Elaborar mensualmente un informe del registro de accesos de los ficheros de Nivel Alto que sean responsabilidad de su departamento.

3.3.5 Responsable ARCO.

Además de las Funciones y Obligaciones Generales, asumidas en su condición de Usuario, el Responsable ARCO deberá cumplir con las siguientes:

3.3.5.1 Funciones.

- Validar formalmente las solicitudes de ejercicio de derechos conforme al procedimiento establecido en el presente Documento de Seguridad.
- Solicitar subsanación de los defectos subsanables que contenga la solicitud, conforme al procedimiento establecido en el presente Documento de Seguridad.
- Coordinar las acciones necesarias para, en su caso, hacer efectivos y otorgar los derechos solicitados.
- Contestar a los solicitantes de los derechos conforme al procedimiento establecido en el presente Documento de Seguridad.

3.3.5.2 Obligaciones.

- Asegurar el correcto otorgamiento de los Derechos ARCO, conforme al procedimiento establecido en el presente Documento de Seguridad.
- Comunicar las rectificaciones o cancelaciones efectuadas a los posibles cesionarios de la información conforme al procedimiento establecido en el presente Documento de Seguridad.
- Conocer y aplicar el procedimiento establecido en el presente Documento de Seguridad para la atención de las solicitudes de derechos de los afectados.

3.3.6 Responsable NOTA.

Además de las Funciones y Obligaciones Generales, asumidas en su condición de Usuario, el Responsable de Notificaciones Telemáticas a la AEPD (en adelante, Responsable NOTA) deberá cumplir con las siguientes:

3.3.6.1 Funciones.

- Concienciar a los distintos departamentos sobre la necesidad de comunicar la creación, modificación y supresión de ficheros conforme al procedimiento establecido en el presente Documento de Seguridad.
- Asesorar y orientar a los distintos departamentos sobre la creación, modificación y supresión de ficheros.

- Analizar las solicitudes de los distintos departamentos para la creación, modificación o supresión de ficheros.

3.3.6.2 Obligaciones.

- Notificar a la AEPD la creación, modificación o supresión de los ficheros.
- Conservar todas las notificaciones efectuadas.
- Conservar las contestaciones de la AEPD con respecto a los ficheros notificados.
- Conocer y aplicar el procedimiento establecido en el presente Documento de Seguridad para la notificación de ficheros.

3.3.7 Responsable de la Dirección de Tecnologías de la Información.

Además de las Funciones y Obligaciones Generales, asumidas en su condición de Usuario, el Responsable de la Dirección de Tecnologías de la Información deberá cumplir con las siguientes:

3.3.7.1 Funciones.

- Colaborar en la elaboración y mantenimiento del Documento de Seguridad.
- Mantener el registro de incidencias según el procedimiento descrito en el presente Documento de seguridad.
- Mantener una relación actualizada de usuarios que tengan acceso autorizado al Sistema de Información.
- Mantener los mecanismos de control de acceso definidos en el presente Documento de Seguridad.
- Mantener los mecanismos de identificación y autenticación definidos en el presente Documento de Seguridad.
- Conceder, modificar o suprimir el acceso a los ficheros que contengan datos de carácter personal, así como a los recursos de la Entidad, bajo las instrucciones del Responsable de Departamento.
- Verificar semestralmente la correcta definición y funcionamiento de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Administrar y monitorizar el correcto funcionamiento del sistema incluyendo cambios de versiones, administración de acceso y realización de copias de respaldo.
- Analizar posibles transgresiones e irregularidades en los accesos, e informar en su caso al Comité de Seguridad.
- Evaluar la seguridad de paquetes, aplicaciones, productos y dispositivos, antes de su adquisición o implantación.

- Coordinar aspectos de seguridad con administradores/técnicos de sistemas, comunicaciones, bases de datos y usuarios en general.

- Definir la arquitectura de sistemas de información más adecuada para la organización, teniendo en cuenta la evolución tecnológica y la introducción de nuevos productos y servicios.

- Dirigir las actividades de desarrollo, mantenimiento y soporte técnico para garantizar el servicio a los usuarios.

- Participar en los planes de protección de datos y seguridad de la información no automatizada en sus diferentes soportes, y tanto en transmisión como en proceso y almacenamiento.

3.3.7.2 Obligaciones.

- Mantener los anexos del presente Documento de Seguridad de forma conjunta con el Comité de Seguridad y los Responsables de Seguridad de los Distintos Departamentos.

- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.

- Implantar y mantener los controles y medios que se hayan establecido para proteger tanto los datos de carácter personal como los propios sistemas de información y sus componentes: los ficheros automatizados, los programas, los soportes y los equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

- Cumplir la normativa en cuanto a gestión de soportes informáticos que contengan datos de carácter personal, 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 borrar previamente su contenido o se exigirán garantías escritas de que se hará así.

- Conocer y aplicar los procedimientos establecidos en el presente Documento de Seguridad.

4. Medidas, normas, procedimientos, reglas y estándares de seguridad.

4.1 Centros de tratamientos y locales.

Los locales donde se encuentran los equipos informáticos que contienen los ficheros objeto de tratamiento debe disponer de las medidas de seguridad mínimas al objeto de garantizar la confidencialidad de los datos de carácter personal y su disponibilidad.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Anexo VII: Centros de tratamiento y locales:

- CPDs y elementos principales de comunicación
- Estructura LAN de C278
- Esquema de Conexiones en C278
- Mapa de Red en Santiago Navarro, 8 (Murcia) – IECISA.
- Diseño físico LAN por plantas

4.1.1. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o un perfil de usuarios determinando y un periodo de validez para las mismas. Las políticas, normas y procedimientos que ICEX posee en relación con este apartado pueden encontrarse a lo largo de este documento.

En la relación de personal autorizado se recogen las autorizaciones y el periodo de validez de las misma, en el Anexo VIII: Relación del personal autorizado.

4.1.2. Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los Sistemas de Información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que previamente se haya realizado una copia de seguridad y se asegure el nivel de seguridad correspondiente al tratamiento realizado, y se anote su realización en el presente Documento de seguridad.

De las pruebas realizadas conforme al párrafo anterior deberá quedar constancia en el Registro de Incidencias.

ICEX dispone de entornos separados para Desarrollo, Preproducción y Producción.

4.2. Puestos de trabajo.

4.2.1. Concepto y características.

Las medidas de seguridad que afectan a los puestos de trabajo son de aplicación a todos los ficheros existentes en ICEX con independencia del nivel de seguridad que precisen por la tipología de datos que contengan.

A los efectos del presente documento, se define como puesto de trabajo a todo aquel dispositivo desde el cual resulte posible acceder a los datos contenidos en los ficheros.

Cada puesto de trabajo estará bajo la responsabilidad de cada una de las personas autorizadas en la red de ICEX, quien garantizará que la información a la que tiene acceso no pueda ser visualizada por personas no autorizadas. Esto supone que:

- Se prohíbe la grabación de datos corporativos en los discos duros de los puestos locales, salvo en los casos específicos y autorizados por el Responsable del Fichero.

- Los monitores de los ordenadores deben estar colocados de forma estratégica a fin de evitar la visualización de la información por parte de personas no autorizadas. Asimismo, cuando el responsable de un puesto lo abandone temporal o definitivamente, deberá arbitrar los medios adecuados para impedir la visualización de la información visualizada en las pantallas y el acceso al equipo.

- Cualquier dispositivo físico (tales como impresoras, módem, fotocopiadoras, escáner y demás periféricos), conectado o no al ordenador, deberá estar situado de forma que se impida el acceso a la información a personas que no cuentan con la autorización necesaria para ello. Los responsables de cada uno de los puestos de trabajo utilizarán dichos dispositivos con la diligencia debida y asegurarán durante su uso la confidencialidad e integridad de la información.

- Cualquier documento o soporte que contenga datos de carácter personal deberá ser custodiado de forma que se evite el acceso por personal no autorizado.

- Los dispositivos de almacenamiento de documentos (cajoneras, archivadores etc) contengan datos de carácter personal, que esté bajo la responsabilidad del usuario, deberá garantizar disponer de mecanismo que obstaculicen el acceso a la información que contienen a las personas no autorizadas.

La utilización de ordenadores portátiles reviste un peligro adicional ya que, además de los riesgos inherentes a todo puesto de trabajo cuenta con los derivados de su portabilidad, debiendo extremarse las medidas de seguridad sobre estos dispositivos

Los ordenadores portátiles pertenecientes a ICEX estarán bajo el control del Responsable de Seguridad, el cual los almacenará bajo llave y autorizará la disposición de los mismos al personal que deba servirse de ellos para la realización de las funciones que les hayan sido encomendadas.

- En los desplazamientos fuera del centro habitual de trabajo, deberán observarse las siguientes precauciones de seguridad:

- Evitar su depósito en lugares visibles y/o fácilmente accesibles por personal no autorizado.

- Evitar su depósito en habitáculos o depósitos que carezcan de cerradura.

- Evitar facturarlos en medios de locomoción.

- Evitar dejarlos encendidos, sin los correspondientes mecanismos de protección.
- Evitar la revelación de las identificaciones de acceso asignadas.
- Impedir manipulaciones técnicas del mismo por parte de personal no autorizado.
- Como medida adicional, la Dirección de Tecnologías de la Información de ICEX mantiene un registro de asignación de equipos portátiles, en el que se apuntan:
    - Fecha de retiro del equipo.
    - Persona que lo solicita.

Al momento de retirarlos, los sujetos a cargo deben firmar un recibo en el que se detallen las características básicas del ordenador, la fecha de solicitud, tiempo por el que se solicita y usos previstos en relación con datos de carácter personal.

Una vez reintegrado, el personal de sistemas debe efectuar una comprobación del estado y contenido del disco duro, eliminando previo aviso la información que hubiera quedado registrada y no fuera de utilidad.

El RLOPD exige que las funciones y obligaciones del personal estén claramente definidas y documentadas, siendo obligación del responsable del fichero adoptar las medidas necesarias para que el personal conozca las normas que afectan al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.

4.2.2. Política de uso de los recursos físicos y lógicos.

Además de la aceptación y cumplimiento de la Política de Seguridad Corporativa de ICEX en general, establecida en el su propio reglamento interno, los usuarios deberán cumplir la siguiente norma relativas al buen uso de los recursos informáticos:

Normas de uso del Correo Electrónico Corporativo de ICEX

- Los usuarios son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la empresa ICEX.
- Es una falta grave facilitar y/o permitir la utilización de la cuenta y/o el correspondiente buzón a personas no autorizadas.
- Los usuarios deben ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por ICEX. Los mensajes de correo transmiten información en sus cabeceras (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como daños a la imagen institucional) que podría acarrear una mala utilización de este recurso.
- Los servicios de correo electrónico suministrados deben ser destinados a uso estrictamente laboral. Excepcionalmente pueden ser utilizados para temas personales siempre que no interfieran con el rendimiento del propio servicio, la actividad laboral, los gestores del servicio o que supongan un alto coste para ICEX.
- Está prohibida la utilización en los equipos informáticos provistos por ICEX, de buzones de correo electrónico de otros proveedores Internet. Especialmente se prohíbe la utilización como encaminador

de correo de otras máquinas que no sean las puestas a disposición por ICEX, el envío de mensajes con direcciones no asignadas por los responsables de la institución y la manipulación de las cabeceras de correo electrónico saliente.

- El correo electrónico es una herramienta para el intercambio de información entre personas y no debe ser utilizada como herramienta de difusión de información. Para ello existen otros canales más adecuados y efectivos, para cuyos propósitos debe contactarse con los responsables del servicio.

- La violación de la seguridad de los sistemas puede generar responsabilidades civiles y/o criminales. ICEX colaborará al máximo de sus posibilidades en cualquier eventual investigación contra este tipo de actos o cualquier otra utilización ilegal, incluyendo la cooperación con la Justicia.

- El sistema informático de ICEX se encuentra protegido contra virus informáticos por un antivirus. La responsabilidad sobre la comunicación a los responsables del sistema de cualquier anomalía suscitada en este sentido depende de cada usuario, así como la apertura de un correo sobre el que se tengan dudas o la emisión de un mensaje de virus por parte del antivirus.

- No es correcto enviar correos electrónicos a personas que no desean recibirlo. En caso de reunir determinadas características, estos envíos podrían llegar a enrolarse dentro del concepto de *spam*, lo que configura una conducta prohibida por la legislación vigente en nuestro país. Si ICEX llegara a recibir reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.

- Está completamente prohibido realizar cualquiera de las siguientes actividades:

    - Utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno a las actividades laborales autorizadas por la empresa.

    - Participar en la propagación de cartas encadenadas, esquemas piramidales o similares.
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para ICEX.

    - Falsificar las cabeceras de correo electrónico.

    - Recoger correo de buzones de otro proveedor de Internet.

    - Difundir contenido ilegal o contrario a la moral (como apología del terrorismo, piratería, pornografía, amenazas, estafas, virus, códigos maliciosos o hacking).

    - Enviar correo propio a través de cuentas ajenas sin consentimiento de su titular.

    - Efectuar ataques con objeto de imposibilitar u obstruir sistemas informáticos (ataques de denegación de servicio), dirigido a un usuario o al propio sistema de correo, así como el envío de un número alto de mensajes por segundo (mail *bombing*), o cualquier variante, que tenga por objeto la paralización del servicio por saturación de las líneas, de la capacidad de CPU del servidor, del espacio en disco de servidores o terminales o cualquier otra práctica similar.

    - Enviar mensajes que comprometan la reputación de ICEX a foros de discusión, listas de distribución y/o *newsgroups*.

Normas de acceso a Internet

- Los usuarios son únicos responsables de las sesiones iniciadas en la red Internet desde sus terminales de trabajo. En la empresa, la red Internet tiene carácter laboral, sin perjuicio del uso de la misma para fines informativos.

- En ningún caso se pueden modificar las configuraciones de los navegadores (opciones de Internet) del equipo ni la activación de servidores o puertos sin autorización de los responsables de seguridad.

- Debe evitarse la utilización de imágenes (como los formatos GIF, JPG, BMP o TIFF entre otros), sonido (formatos WAV y MP3 principalmente) y vídeo (MPG, DivX), AVI, RAW o similares) para fines ajenos a la actividad laboral de la empresa, debido a que el tamaño de estos archivos satura los canales de comunicación y disminuye la velocidad de transmisión perjudicando al funcionamiento de la red en su conjunto.

- Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres; de los formatos de imágenes, sonidos o vídeo que a modo de ejemplo se enumeran en la norma anterior; de virus y códigos maliciosos y, en general, de todo tipo de programas y/o *plug in* sin la expresa autorización del coordinador de seguridad. ICEX colaborará al máximo de sus posibilidades en cualquier eventual investigación contra este tipo de actos o cualquier otra utilización ilegal, incluyendo la cooperación con la Justicia.

- Queda vedada toda utilización ajena a las actividades de la empresa de los servicios de IRC (canales de chat) ya sea mediante el acceso a páginas que los brinden como desde aplicaciones instaladas en los equipos (como MS Messenger, TOM, Yahoo, ICQ o similares). Tampoco se permite el acceso a páginas de juegos en línea o la descarga de cualquier dispositivo similar.

Normas sobre el uso de los programas de ordenador

- No se permite la instalación de ningún producto informático en el sistema de información de ICEX. Todas las aplicaciones necesarias para el desempeño de su trabajo serán instaladas únicamente por el personal especializado del Departamento de Sistemas o bajo su supervisión, tras su conocimiento y aprobación.

- No deberán utilizarse los recursos del sistema de información de ICEX para uso privado ni para cualquier otra finalidad diferente a las estrictamente laborales.

- Se prohíbe la revelación a cualquier persona ajena a la organización, de información a la que se haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.

- No se facilitarán a persona alguna ajena a la organización, soportes que contengan datos a los que se haya tenido acceso en el desempeño de sus funciones sin la debida autorización.

- La información referida en el párrafo anterior deberá utilizarse únicamente en la forma exigida para el desempeño de sus funciones, absteniéndose los usuarios de disponer de ella de ninguna otra forma o para finalidad diferente.

- No se permite el acceso ni ningún otro tipo de tratamiento informatizado, de datos que no sean necesarios para el normal desempeño de sus funciones en la propia organización.

- Todo usuario del sistema de ICEX, se encuentra obligado a cumplir la normativa vigente en el desarrollo de sus funciones en la Entidad, así como los extremos vertidos en el documento de seguridad, en relación a la protección de datos de carácter personal.

- Deberá darse cumplimiento a los compromisos anteriores, incluso después de extinguida la relación laboral con ICEX.

- El trabajador será responsable frente a ICEX y frente a terceros, de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores, debiendo resarcir a ICEX por las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Incumplimiento de las Obligaciones

El incumplimiento de las obligaciones anteriormente descritas dará lugar a la imposición de las correspondientes sanciones disciplinarias por parte de ICEX atendiendo a la naturaleza de la infracción cometida, así como a los daños y perjuicios ocasionados tanto a la propia empresa como a los titulares de los datos de carácter personal o afectados.

Podrán imponerse, de acuerdo con el principio de proporcionalidad y atendiendo a la gravedad del incumplimiento, las sanciones correspondientes.

No obstante, y, sin perjuicio de la sanción que pudiese imponerse en el seno de la relación laboral, ICEX podrá reservarse contra el trabajador las acciones civiles y/o penales que de acuerdo con la legislación vigente procedan.

4.3. Identificación y autenticación del personal autorizado.

El responsable del fichero o tratamiento establecerá un procedimiento que garantice la correcta identificación y autenticación de los usuarios autorizados para acceder a los sistemas de información.

Los accesos a los sistemas de información se realizarán mediante un sistema que permita la autenticación de forma inequívoca y personalizad del usuario. Cada identificación deberá pertenecer a un único usuario. La política de identificación y autenticación se implanta con el objeto de evitar accesos no autorizados al sistema que contiene datos personales automatizados.

A tal fin, deberá identificarse a la totalidad de los operarios y terminales que efectúen peticiones contra los sistemas que contienen los ficheros, de manera que sea posible determinar ante cada acceso, la identidad tanto del gestor como del equipo gestionado.

Cada usuario deberá vincularse a una clave única, que deberá introducir para obtener los permisos correspondientes a sus funciones dentro de cada sesión mantenida en un equipo.

Los sistemas de identificación y autenticación de los usuarios con acceso a los sistemas de ICEX que contienen ficheros con datos de carácter personal se encuentran establecidos.

El sistema establecido permite la identificación de forma inequívoca y personalizada, de todo aquel usuario que intenta acceder al sistema de información y verifica que está autorizado.

A continuación se especifican las características del procedimiento establecido:

4.3.1. Procedimiento de identificación y autenticación.

Cualquier acceso a los sistemas de información de ICEX se realiza utilizando un código de usuario, sujeto a las normas de nomenclatura existentes en la propia Entidad, provisto por personal de la Dirección de Tecnologías de la Información. Cualquier excepción a la normativa de asignación de usuarios deberá ser notificada a la Dirección de Tecnologías de la Información quién autorizará, en caso de estar justificado, la definición del usuario.

No se permite el acceso a los sistemas de información con un identificador de usuario que no sea el propio, así como comunicarlo y/o cederlo con su contraseña a cualquier otra persona perteneciente o no a ICEX. Las altas o restauraciones de usuarios son realizadas por la Dirección de Tecnologías de la Información que asignan contraseñas estándar. El sistema operativo obliga al cambio de contraseñas cuando ésta es la estándar.

Asimismo, la identificación de los usuarios se realiza mediante tarjetas inteligentes o Smart Card, que se autentican contra el Directorio Activo. No obstante, actualmente no todos los empleados de ICEX disponen de este método de identificación, si bien lo utilizan ya más de la mitad de los mismos.

Existen tres perfiles para las tarjetas inteligentes:

- Empleados de ICEX
- Personal externo
- Estudiantes en prácticas

La gestión y administración de los permisos de usuarios es responsabilidad del Departamento de Informática de ICEX. No obstante, en el momento en que el administrador va a dar acceso a un nuevo usuario al sistema, le informa convenientemente de que es responsabilidad del propio usuario, el cumplimiento de las políticas existentes en ICEX en materia de autenticación de usuarios.

4.3.2. Calidad de las contraseñas.

Las contraseñas de ICEX deben mantener un estándar mínimo de seguridad. Estos estándares ayudan a proteger su información privada haciendo más difícil que terceros desautorizados tengan acceso a las cuentas de usuarios autorizados. La política indica los siguientes niveles de seguridad para Windows:

LONGITUD: La longitud mínima de la contraseña debe ser de ocho (8) caracteres alfanuméricos.

EXPIRACIÓN: La contraseña expirará a los noventa (90) días como máximo.

REPETICIÓN: No puede renovarse la contraseña con su contraseña actual, recordándose de hecho las tres (3) últimas contraseñas.

PRIVACIDAD: No puede compartirse la contraseña con ninguna persona. Cada usuario es responsable de cualquier acción que ocurra en su cuenta cuando ha entrado a con su contraseña.

RECOMENDACIONES:

- Seleccionar una contraseña difícil de adivinar.

- Incluir caracteres especiales o números.

- No utilizar ninguno de estos parámetros:

  - Nombre del usuario.
  - Nombre de familiares: esposo, novia, novio, o de cualquier otro pariente.
  - Nombre del perro, gato u otro animal doméstico.
  - Teléfono del hogar u oficina

Se recomienda no seleccionar como contraseña del sistema por parte de los usuarios palabras en cualquier idioma, códigos con valores asociables al usuario (nombres de personas, matrículas, teléfonos, fechas, etc.), ni utilizar secuencias lógicas deducibles en los cambios de contraseñas, permutaciones sencillas, secuencias de teclado, etc.

Se recomienda la utilización de cadenas de caracteres en las que se mezclen caracteres alfabéticos y numéricos sin ningún tipo de significado.

4.3.3. Reemplazo de contraseñas.

No obstante, los miembros del personal con acceso autorizado a los recursos del sistema podrán reemplazar en todo momento su contraseña o solicitarlo a la Dirección de Tecnologías de la Información.

4.3.4. Reglas de nomenclatura.

La nomenclatura utilizada en la definición del código de usuario en los sistemas informáticos de ICEX, sigue las normas descritas a continuación.

Cualquier excepción a la nomenclatura identificada deberá ser notificada a la Dirección de Tecnologías de la Información quién autorizará, caso de estar justificado, la utilización de una nomenclatura diferente.

El identificador de cada usuario con acceso al sistema se compone de la letra “P” seguida del número de matrícula del empleado.

No obstante, ICEX dispone de contraseñas no solo a nivel de sistema operativo, sino también de correo y aplicaciones.

4.3.5. Confidencialidad de las contraseñas.

La contraseña del usuario no resulta visible en pantalla durante su introducción por teclado. Los sistemas informáticos de ICEX están configurados de manera que bajo cualquiera de los entornos existentes en el sistema, al introducir la contraseña en la pantalla de acceso al sistema o aplicaciones se visualicen asteriscos o espacios en blanco en lugar de los caracteres introducidos, evitando de esta manera que terceras personas que se encuentren cercanas al puesto de trabajo puedan ver los caracteres que integran el código mientras es introducido por su propietario.

Los usuarios dados de alta en los sistemas y aquellos que solicitan cambio por olvido o bloqueo de usuario, son informados por el administrador del sistema correspondiente de la contraseña inicial que les ha sido asignada.

Los cauces establecidos para la comunicación al usuario de su contraseña inicial, están diseñados de manera que se garantiza la confidencialidad de la misma.

Cuando se informa sobre el olvido de la password o bloqueo de la cuenta de usuario (por superarse el límite de tres (3) intentos erróneos reiterados de acceso al sistema) el administrador del sistema está obligado a comprobar la identidad del solicitante.

Los sistemas informáticos permiten efectuar el cambio voluntario de la contraseña de un usuario tanto por parte del propietario de la misma como por parte del administrador de usuarios.

Es obligatorio por parte del usuario, en su primer acceso al sistema o a una aplicación, el cambio de la contraseña asignada al ser dado de alta o en el procedimiento de asignación por olvido de contraseña. Los sistemas de la Entidad están preparados para obligar a este cambio de manera automatizada.

Las contraseñas son codificadas y almacenadas de manera que resulten ininteligibles. En particular, en ICEX, las contraseñas se almacenan encriptadas bajo los mecanismos del sistema operativo Windows.

Las contraseñas deben viajar cifradas por las líneas de comunicación.

4.3.6. Autenticación de usuarios.

Todos los usuarios de los sistemas de información de ICEX, disponen de contraseñas asociadas a sus identificadores de usuario para permitirles el acceso a los sistemas informáticos de la compañía.

La administración de los usuarios es responsabilidad de la Dirección de Tecnologías de la Información de ICEX. No obstante, en el momento en que el administrador va a dar acceso a un nuevo usuario al sistema, le informa convenientemente de que es responsabilidad del propio usuario el cumplimiento de las políticas existentes en ICEX en materia de autenticación de usuarios.

Las consecuencias que se deriven del incumplimiento de estas políticas, serán de exclusiva responsabilidad del propietario del identificador y contraseña del usuario. Los responsables de cada departamento deberán velar por el cumplimiento de esta norma en el ámbito de su responsabilidad, exigiendo a sus subordinados el acatamiento de la misma y comunicando los incumplimientos al Responsable de Seguridad como incidencias de seguridad.

4.3.7. Relación de usuarios.

ICEX, con objeto de cumplir los puntos 1 y 2 del artículo 93 del RLOPD, podría extraer del Directorio Activo el listado de usuarios con acceso a los sistemas de información. Además, esta relación contiene el tipo de acceso permitido para cada uno de ellos, cumpliendo de esta manera el artículo 91.2 del RLOPD en relación con el Control de Acceso.
Siempre que se realizan altas, bajas y modificaciones de usuarios, dicha lista se actualiza automáticamente.

Dicha relación deberá solicitarse a la Dirección de Tecnologías de la Información de ICEX, en caso de ser requerida en cumplimiento de lo establecido en la normativa vigente en materia de protección de datos. La relación de usuarios con acceso al sistema, así como los grupos a los que pertenece cada uno de ellos, se puede obtener siguiendo los siguientes puntos:

- El responsable del sistema entra como Administrador.
- Mediante la utilidad de administración de usuarios se obtiene el listado con los usuarios dados de alta en el dominio y los grupos a los que tienen acceso.

Cada usuario es responsable de la confidencialidad de la contraseña, debiendo actuar con la diligencia debida. En caso de que tuviera conocimiento de que la misma pudiera resultar conocida fortuita o fraudulentamente por personas no autorizadas, deberá informar al Responsable de Seguridad, quien procederá inmediatamente a su cambio a través del procedimiento establecido al efecto.

4.4. Control de acceso.

4.4.1. Control de acceso lógico.

ICEX, en su condición de Responsable del Fichero puede conceder, alterar o anular el acceso a datos y recursos referidos al fichero o ficheros de su competencia.

1. Introducción

Se entiende por control de acceso al mecanismo que en función a la identificación ya autenticada, permite acceder a datos, recursos, soportes y/o documentos.

El acceso lógico y operativo de los usuarios a los datos, recursos, soportes y/o documentos de ICEX estará permitido exclusivamente en función de las necesidades derivadas de la actividad profesional que realizan.

Se habilitarán los mecanismos técnicos pertinentes a fin de garantizar un nivel de acceso adecuado al perfil de cada usuario.

Las altas, bajas, o modificaciones de los diferentes perfiles asignados a los usuarios, se realizarán a través del responsable del área al que pertenezca el nuevo usuario, el cual tramitará la solicitud a la Dirección de Tecnologías de la Información siguiendo el procedimiento establecido. Única y exclusivamente el personal de la Dirección de Tecnologías de la Información poseerá la facultad fáctica de conceder, alterar o anular el acceso autorizado sobre los datos, recursos, soportes y/o documentos, conforme a los criterios establecidos por el responsable o encargado de tratamiento de cada uno de los ficheros de carácter personal.

Las personas que tengan acceso a información sensible, o bien reciban información de clientes en cualquier tipo de soporte, tendrán la obligación de cumplir las normas y procedimientos de seguridad y confidencialidad que se establezcan en cada momento.

El control de acceso se efectuará mediante código de usuario y contraseña de acuerdo con las disposiciones establecidas en el apartado Identificación y Autenticación. Accesoriamente podrán implantarse sistemas de autenticación de equipos (autenticación por IP). Se recuerda que el uso de las claves de acceso a los sistemas y aplicaciones es estrictamente personal estando prohibido su uso por cualquier otra persona distinta del titular de la misma.

El acceso no autorizado a ficheros por parte de los usuarios implica una transgresión a las medidas de seguridad pudiendo producirse sanciones a la Entidad por parte de AEPD.

Los usuarios están obligados a poner en conocimiento de su Responsable o del Responsable de Seguridad cualquier incidencia que afecte a la confidencialidad e integridad de los datos de un fichero, conforme se indica en el apartado relativo a gestión de incidencias.

2. Procedimientos de Administración de Usuarios

El Departamento de Informática de ICEX tiene definidos perfiles de usuarios, de forma que sólo los empleados autorizados acceden a los ficheros. Dichos accesos son efectuados con los privilegios otorgados al personal en virtud de sus funciones y obligaciones.

Las peticiones de altas de los accesos de los usuarios a los sistemas de información de ICEX, se realizan a través del Responsable del departamento correspondiente mediante solicitud al Departamento de Informática, que procede a enviar al nuevo usuario sus datos de usuario y contraseña por email.

En el sistema se han creado grupos y subgrupos en relación a los departamentos y áreas existentes en la organización. Las autorizaciones a los ficheros y/o aplicaciones se realizan a través de los grupos y subgrupos en relación al departamento / área a la que pertenece el usuario.

Únicamente el personal de la Dirección de Tecnologías de la Información puede gestionar el control de acceso al sistema informático de ICEX. Los únicos usuarios con permisos de administración son los especificados en el Documento de Seguridad.

Como regla, los usuarios tendrán restricciones de acceso a la totalidad de los recursos existentes en el sistema de información de ICEX, a excepción de los permisos que se otorguen específicamente a cada factor en razón de las funciones que efectivamente desempeñe dentro de la organización.

3. Alta o Modificación de Usuarios

En caso de que se desee realizar un alta o una modificación de un usuario, la Dirección Adjunta de Recursos Humanos procede a notificar a la Dirección de Tecnologías de la Información a través de un correo electrónico donde se informa de los atributos necesarios para el nuevo usuario (aplicación o aplicaciones a las que necesita acceso, perfil requerido, etc.). Dichos atributos, normalmente, vendrán determinados por el cargo que vaya a ocupar el nuevo usuario dentro del departamento.

La creación y modificación de los usuarios en los sistemas y aplicaciones se realiza siguiendo las normas y procedimientos establecidos para los procesos de identificación, autenticación, nomenclatura, confidencialidad y distribución de las contraseñas, expuestos en el apartado relativo a la Identificación y Autenticación de los usuarios.

El mismo procedimiento se seguirá en el caso de que exista la necesidad por motivos justificados de trabajo, de dar de alta en los sistemas y aplicaciones de ICEX a colaboradores externos.

Los accesos otorgados a los usuarios nuevos o modificados serán, únicamente, los necesarios para el desarrollo de sus funciones. El establecimiento de los permisos de acceso sobre los recursos se realizará según las especificaciones del Responsable del Fichero de manera que:

- Queden claramente establecidos los recursos a los que el usuario podrá acceder, incluyéndolo en el grupo(s) que le corresponda en función del departamento al que pertenezca.
- En el caso de que un usuario necesite acceder a un recurso no permitido para él, se seguirá el procedimiento de seguridad establecido en la Entidad para el mantenimiento de usuarios, siendo necesaria una autorización del Responsable del Fichero o encargado del tratamiento.
- Si se produce el cambio de una persona de un departamento a otro, se debe crear un nuevo usuario para el nuevo departamento y eliminar el del antiguo.
- El Responsable de Seguridad recibirá notificación sobre la aparición de nuevos recursos a proteger, a fin de que se controlen los accesos correspondientes.

- Todo recurso para el que su responsable no haya establecido un nivel de criticidad, deberá estar restringido a todos los usuarios.

Finalizado el proceso, los técnicos de la Dirección de Tecnologías de la Información se lo comunicarán al Responsable de Seguridad.

La Dirección de Tecnologías de la Información se pondrá en contacto con el nuevo usuario para notificarle su identificador y contraseña, garantizando en todo momento la confidencialidad. También comunicará al responsable del departamento que la petición ha sido realizada.

Además, se aprovechará para informar al usuario acerca de su compromiso ante el mantenimiento de la integridad y confidencialidad de su clave, así como, la responsabilidad de toda acción efectuada dentro del sistema bajo el nombre de usuario que le es asignado. Complementariamente se le hará entrega de un impreso informativo, conteniendo sus responsabilidades respecto a su clave y usuario.

Si se trata de una solicitud de modificación, el procedimiento a seguir es el mismo que para la realización de un alta, salvo el tema de concienciación del usuario.

4. Bajas de Usuarios

Las bajas de usuarios seguirán el mismo procedimiento de comunicación que las altas (correo electrónico procedente de la Dirección Adjunta de Recursos Humanos).

4.4.2. Control de Acceso Físico.

1. Introducción

Los centros y locales de ICEX tienen una gran trascendencia en orden a asegurar la confidencialidad, integridad y disponibilidad de la información del fichero, puesto que en estas dependencias se encuentran los ordenadores que albergan los ficheros con datos de carácter personal objeto de tratamiento. Para ejercer este control de acceso físico, el Responsable de Seguridad elaborará y mantendrá actualizado un registro de accesos para el personal interno y externo, velando especialmente por la permanencia en las dependencias de la compañía fuera del horario establecido, así como, para toda persona ajena al ámbito laboral de la Entidad.

Los centros y locales deben ser objeto de protección y estar provistos de los medios necesarios, para evitar los riesgos de falta de disponibilidad de los ficheros como consecuencia de una incidencia.

El acceso físico a los locales de ICEX donde se encuentran los ficheros estará restringido a:

- Las personas reflejadas como autorizadas en el presente Documento de Seguridad, o terceras personas acompañadas y supervisadas por las primeras, siempre que en ambos casos cuenten con una autorización del Responsable de Seguridad, justificada, específica, individualizada e intransferible.

- Los administradores del sistema autorizados por el Responsable de Seguridad, exclusivamente para realizar labores de mantenimiento.

El Responsable de Seguridad verificará que todos los sistemas y medios de seguridad funcionan correctamente, resolviendo las posibles deficiencias que pudieran detectarse.
Para ICEX, el control de acceso físico a locales donde se encuentren ubicados datos de carácter personal es un punto esencial a tener en cuenta para evitar el acceso de personal no autorizado a dichos datos o a los sistemas que los gestionan.

En este sentido, se dispone de unas políticas, normas y procedimientos que evitan:

- Acceso no autorizado a los locales donde se encuentren situados los sistemas de información con datos de carácter personal clasificados como de nivel medio y alto (extendiéndose la protección a los de nivel básico).

- Acceso no autorizado al lugar o lugares donde son almacenados datos de carácter personal.

2. Restricciones de acceso a las salas de ordenadores

El acceso a la sala de ordenadores está permitido exclusivamente al personal de la Dirección de Tecnologías de la Información y a los encargados del mantenimiento de los equipos informáticos.

La lista de personas con permiso para acceder a la sala de ordenadores, es confeccionada por el Departamento de Informática, en función de las necesidades derivadas de la actividad que desarrolle cada persona autorizada.

El control de los CPDs de ICEX es responsabilidad de la Dirección de Tecnologías de la Información. El acceso a esta sala está restringido por una puerta que se mantiene cerrada de forma permanente.

Únicamente, se permite el acceso a las personas que disponen de los permisos correspondientes. De esta forma también Las copias de seguridad se encuentran en un despacho junto a la sala técnica.

La gestión y asignación de permisos es tarea de la Dirección de Tecnologías de la Información, mediante autorizaciones expresas de la Dirección Adjunta de Recursos Humanos.

3. Control de acceso de visitas a la sala de ordenadores

El acceso de cualquier otra persona a las salas de ordenadores debe tener carácter excepcional y ser autorizado por el Responsable de Seguridad. Durante la visita la persona deberá estar permanentemente acompañada por una de las personas autorizadas anteriormente reseñadas.

Cada uno de los accesos a las salas de ordenadores queda registrado a través de un control de acceso a la entrada en la sala que corresponde.

En ambos controles de accesos se registra la siguiente información:

- Fecha del acceso.

- Nombre y apellidos de la persona que accede.

- Motivo del acceso.

- Empresa a la que pertenece.

- Persona que autoriza el acceso o persona autorizada que acompaña al visitante.

- Hora de entrada.

- Hora de salida.

- Observaciones.

Asimismo, las personas que hayan superado dichos controles de acceso solamente podrán acceder a la sala de ordenadores acompañados por un miembro de la Dirección de Tecnologías de la Información que cuente con las autorizaciones necesarias para dicho acceso, así como, con la tarjeta o dispositivo equivalente dispuesto al efecto. Durante el acceso a dicha sala el visitante se encuentra continuamente acompañado, quedando registrado la persona que acompaña al visitante mediante el log generado como consecuencia del acceso efectuado. El control de dichos accesos es responsabilidad de la Dirección de Tecnologías de la Información.

Por cada uno de estos accesos deberá rellenarse el Registro de Accesos.

4. Control de Acceso Físico a Ficheros Automatizados

El control de acceso a las ubicaciones donde se encuentran los sistemas de información con datos de carácter personal incluye mecanismos que obstaculicen el acceso de personas no autorizadas, permitiéndose exclusivamente a determinadas personas de ICEX.

Los accesos extraordinarios (terceras personas o personal no autorizado de ICEX) son documentados por el Responsable de Seguridad en el correspondiente registro. En este formato se recoge la siguiente información:

- Fecha
- Nombre y apellidos de la persona que accede.
- Motivo del acceso.
- Empresa a la que pertenece.
- Persona que autoriza el acceso o persona autorizada que acompaña al visitante.
- Hora de entrada.
- Hora de salida.
- Observaciones.

En caso de almacenamiento de datos de nivel alto, las ubicaciones deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistema de apertura mediante llave u otro dispositivo equivalente.

5. Control de Acceso Físico a Archivos de Documentos

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal disponen de mecanismos que obstaculizan su apertura.

En caso de almacenamiento de datos de nivel alto, los armarios, archivadores u otros elementos en los que se almacenen los datos se encuentran en áreas en las que el acceso está protegido con puertas de acceso dotadas de sistema de apertura mediante llave u otro dispositivo equivalente.

El Responsable de Seguridad define que personas están autorizadas para acceder a estos archivos de documentos.

6. Normas para la protección de soportes

Considerando los soportes (cintas para copias de seguridad) como ubicaciones susceptibles de albergar información de carácter personal, ICEX especifica que éstos son debidamente protegidos, manteniéndose almacenados bajo llave cuando no estén siendo utilizados. El almacenamiento de los soportes se realiza en dependencias específicas que cumplen rigurosas medidas de control de acceso y acondicionamiento. En concreto, todo el software se encuentra en un armario ignífugo que está en la sala de sistemas de Castellana 278.

Las normas específicas para la protección de soportes se recogen en el Apartado 4.6 relativo a Gestión de Soportes.

4.5. Registro de Accesos.

Las aplicaciones informáticas destinadas al tratamiento de datos de carácter personal a los que se debe de aplicar el nivel de seguridad alto, deben disponer de un registro de acceso en los términos establecidos en el RLOPD. El registro de acceso ha de permanecer siempre activo.

Debe registrarse cada intento de acceso, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se guardará la información que permita identificar el registro accedido.

Los mecanismo que permiten el registro de accesos, estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación ni la manipulación de los mismos.

El periodo mínimo de conservación de los datos del registro de accesos será de dos (2) años.

El Responsable de Seguridad revisará al menos una (1) vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Este registro de accesos no será necesario cuando concurran las siguientes circunstancias:

- El responsable del fichero o tratamiento sea una persona física
- El responsable del fichero o tratamiento garantice que sólo él tiene acceso y trata los datos personales.

La concurrencia de estas dos circunstancias debe de hacerse constar expresamente en éste documento de seguridad, en éste mismo apartado.

4.5.1. Acceso a la Documentación

El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el Anexo VIII: Relación del personal autorizado.

Para los documentos que puedan ser utilizados por múltiples usuarios, se establecerán mecanismos que permitan identificar los accesos realizados.

4.6. Gestión de Soportes y Documentación

4.6.1. Salidas/entradas y gestión de soportes y documentación

El objetivo de ésta política es regular las condiciones generales para el control y distribución de cualquier tipo de soporte manejado por el personal de ICEX, y que contenga datos personales de su responsabilidad.

4.6.1.1. Identificación, inventario y almacenamiento

Los soportes informáticos son todos aquellos medios físicos susceptibles de ser tratados en sistemas de información, y sobre los que se pueden grabar o recuperar datos. Con documentos nos referimos a todos aquellos soportes que no sean automatizados (archivos documentales), como el fichero papel, que puede ser fácilmente accedido y destruido por personas no autorizadas. El control de estos medios, tanto automatizados como no, tiene una importancia fundamental en la seguridad de los datos contenidos en los ficheros dada la facilidad para su transporte y reproducción. Los soportes que se utilicen deberán estar expresamente aprobados, identificados y asignados por el Responsable de Seguridad de ICEX.

Los soportes que contengan datos de carácter personal por el motivo que sea, deberán estar claramente inventariados e identificados con una etiqueta externa que indique de qué fichero se trata, qué tipo de datos contiene, el proceso que los ha originado, la fecha de creación, así como un número identificativo del mismo. En caso de tratarse de ficheros en formato papel, se guardarán en carpetas en cuyo exterior se puedan adherir etiquetas similares a las de los ficheros automatizados.

El inventariado seguirá el modelo recogido en los anexos indicados a continuación:

- ANEXO II: Inventario de Equipos.
- ANEXO III: Inventario de Software.
- ANEXO IV: Inventario de Soportes.

La salida del ámbito físico de ICEX de cualquier soporte que contenga datos de carácter personal, deberá ser expresamente autorizada y ratificada por el Responsable de Seguridad y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Los soportes informáticos portátiles solamente son tratados por el personal de la Dirección de Tecnologías de la Información a excepción de los usuarios que soliciten las correspondientes autorizaciones según el procedimiento establecido.

De igual manera, los documentos son tratados únicamente por el personal autorizado a tal efecto de forma expresa, con la salvedad de todos aquellos autorizados de forma temporal a manipular los documentos referenciados.

Cuando por las características físicas del negocio, se detecte la necesidad de emplear equipos fijos o portátiles u otros dispositivos móviles que vayan a tratar información, el responsable del departamento interesado deberá solicitar dicho dispositivo a la Dirección de Tecnologías de la Información. En la solicitud se deberá indicar:

- Motivo de la solicitud.
- Usuario que utilizará el equipo.
- La información a la que tendrá acceso (aplicaciones, software, recursos, etc.).

La Dirección de Tecnologías de la Información establecerá las siguientes medidas de seguridad, en caso de ser factibles:

- Control de acceso previo al arranque del sistema operativo.

- Cifrado de unidades lógicas para almacenamiento de información.
- Aplicación de políticas de seguridad del dominio.
- Instalación y configuración del agente del software corporativo para antivirus.

Cuando el equipo esté preparado, y se haya verificado la aplicación de todas las medidas de seguridad, será entregado al usuario, informando al responsable del departamento correspondiente.

4.6.2. Identificación e Inventario:

Cada uno de los soportes automatizados o no, con datos de carácter personal se identifica de forma que permita identificar claramente los siguientes datos:

- Información que contiene.
- Fecha de alta y Fecha de baja
- Identificación del soporte
- Número de soportes que componen la información

4.6.3. Almacenamiento:

El almacenamiento de soportes es realizado en dependencias específicas (caja de seguridad, salas de ordenadores, lugares protegidos, armarios con llave, etc.) que cumplen con los requerimientos en el ámbito de seguridad física en cuanto a medidas de protección de acceso y acondicionamiento. Además, en todos los casos hay una persona del

La Dirección de Tecnologías de la Información es la encargada del cambio de cintas, y es la única que tiene acceso al lugar de almacenaje.

Asimismo, respecto de las copias de seguridad, aunque se indicará en su procedimiento concreto, se indica que existe un intercambio de cintas entre el CPD de Castellana 278 y la sala técnica de ICEX-CECO (Dirección Ejecutiva de Formación de ICEX) que se hace de forma semanal a través de la gestión autorizada en un formulario donde se registran las entradas y salidas de los soportes.

Los soportes papel se almacenan en archivadores, cajones y armarios, disponiendo todos ellos de cerradura para asegurar que nadie acceda a los datos de forma no consentida. Cuando la documentación se encuentra fuera de los lugares de almacenamiento previstos, se encuentra bajo la supervisión de la persona que está accediendo a la información contenida en el papel, de tal forma que siempre estén a buen recaudo.

No está permitida la existencia de cintas, cartuchos, disquetes o documentos fuera de las dependencias previstas para su custodia cuando no estén siendo utilizados.

Únicamente ICEX podrá autorizar la salida de soportes tanto informáticos como físicos que contengan datos personales, fuera de los locales en los que esté ubicado el Fichero.

4.6.4. Eliminación de información almacenada en soportes:

La información correspondiente a ficheros almacenada en equipos, soportes magnéticos y otro tipo de soporte, debe someterse a la siguiente normativa y medidas de seguridad encaminadas a la protección de la misma:

- Los soportes magnéticos que vayan a ser reciclados o reutilizados, deben ser sometidos a procesos de borrado o formatos completos que garanticen la imposibilidad de recuperación posterior, incluso parcialmente, de la información que contienen

- Serán sometidos a las mismas consideraciones especificadas en el punto anterior, aquellos equipos informáticos con capacidad de almacenamiento (discos duros internos) que vayan a ser retirados o reutilizados por usuarios diferentes a los usuales.

- En el caso de rotura de equipos con capacidad de almacenamiento que deban ser reparados fuera de las dependencias de la Entidad, deben tomarse medidas que impidan la posibilidad de extraer la información y –en caso de resultar viable-, el dispositivo de almacenamiento debe ser retirado.

- En caso de retiro o eliminación de soportes por resultar caducos o defectuosos, deberá procederse a su destrucción física, de modo tal que se garantice la imposibilidad de recuperar cualquier dato que pudiera haber contenido.

- Todos aquellos soportes no automatizados serán completamente destruidos una vez se decida que han devenido inútiles, garantizando con su destrucción la imposibilidad de recuperar ningún dato que contuvieran.

4.6.5. Alta e inventario de soportes físicos:

Los soportes y documentos que contengan información relevante para ICEX, independientemente de la clasificación asignada, estarán claramente identificados salvo que las características físicas del propio soporte o documento lo impidan.

Cuando las características físicas del soporte imposibiliten su etiquetado, inventariado o accesibilidad limitada al personal autorizado, se dejará constancia en el inventario de soportes, de acuerdo con el Anexo VII: Centros de tratamiento y locales.

La identificación de los soportes para información especialmente sensible (confidencial y/o secreta) podrá establecerse mediante una codificación que dificulte la identificación para personas que no deban tener acceso a la misma.

Los soportes físicos deberán estar inventariados, incluyendo el tipo de información que contiene, la fecha de creación o adquisición, fecha de baja, motivo de la baja, etc.

Cuando por las necesidades del negocio, se detecte la necesidad de emplear soportes físicos para almacenar y/o tratar datos de carácter personal, el Responsable de Seguridad por Departamento interesado solicitará a la Dirección de Tecnologías de la Información dicha necesidad. Deberá indicar:

- Motivo de la solicitud.

- Usuario(s) autorizado(s) a enviar o recibir información en el soporte.

- La información que contendrá.

- En su caso, entidad o entidades a las que se enviará el soporte.

La Dirección de Tecnologías de la Información registrará la petición en el inventario de equipos y soportes disponible a tal fin, así como el resto de información proporcionada.

Las Dirección de Tecnologías de la Información entregará al usuario las normas que afectan a la seguridad de los soportes.

4.6.5.1. Mantenimiento de equipos

La Dirección de Tecnologías de la Información realizará directamente el mantenimiento y/o reparación de los equipos en aquellos casos en que sea posible, y contactará con los fabricantes de los mismos en caso de no poder llevar a cabo las tareas de mantenimiento requeridas.

La Dirección de Tecnologías de la Información gestionará a partir de ese momento las reparaciones de equipos verificándose la garantía de dichos equipos por albarán y número de serie.

4.6.5.2. Gestión de Intercambio de Información

Los documentos que contengan datos personales, independientemente del soporte en el que se encuentren (incluido los documentos anejos a un correo electrónico) y el nivel de seguridad aplicable, deben estar claramente identificados (salvo que las características físicas del propio soporte o documento lo impidan).

Los datos personales que necesiten ser intercambiados con otras organizaciones o entidades deberán ser registrados e inventariados para su control y gestión. El inventario recogerá la información referida, los soportes involucrados (físicos o lógicos), así como el personal responsable del intercambio (envío y/o recepción).

Cuando por las necesidades del negocio, se detecte la necesidad de intercambiar datos personales con terceras partes, el responsable del departamento interesado deberá autorizar el envío de información. El solicitante deberá indicar:

- Motivo del intercambio.
- Usuario(s) autorizado(s) a recibir información en el soporte físico o lógico.
- Los datos personales que contendrá.
- Entidades a las que se enviarán los datos personales.
- Modo y soporte para el envío de los datos personales.

El responsable del departamento interesado registrará la petición en el inventario de equipos y soportes disponible a tal fin.

En el caso de documentos el Responsable de Seguridad por Departamento se asegurará de la implantación de mecanismos que obstaculicen la apertura de los dispositivos de almacenamiento de documentos. Si las características del dispositivo no permiten tales mecanismos, deberán adoptarse medidas que impidan el acceso de personas no autorizadas.

El Responsable de Seguridad por Departamento entregará al usuario las normas que afectan a la seguridad de los soportes.

4.6.5.3. Salidas y entradas de soportes

4.6.5.3.1. Salida de soportes informáticos y documentación.

La salida de soportes informáticos y documentación en papel de las dependencias físicas donde se ubican, no está permitida, salvo en las siguientes situaciones:

- Soportes planificados y controlados.
- Soportes correspondientes a productos de software de aplicación:

  Aplicaciones, actualizaciones de software, etc.
- Salida de documentación a gestorías, despachos de abogados, instituciones de la Administración, etc.

Cualquier otro uso o cesión de soportes magnéticos que no se ajuste a las situaciones anteriores deberá ser solicitado por escrito y autorizado por el Responsable de Seguridad para cada uno de los casos. En el caso de soportes que contengan datos de carácter personal, únicamente podrá ser autorizada la salida por el Responsable del Fichero. La solicitud y autorización de salida de soportes se anota en el registro de Entradas y Salidas del Anexo IV.

El traslado de soportes automatizados y no automatizados fuera de las ubicaciones físicas de ICEX, se produce bajo estrecha supervisión del personal encargado de su transporte. Cuando se trate de datos de Nivel Alto de Seguridad, se procederá al cifrado de la información que viaja en el soporte. Así mismo, cualquier información enviada por cualquier medio (email, etc.) con datos de nivel alto, deberá ser cifrada antes de su comunicación. Cualquier documento que contenga dichos datos saldrá en un sobre cerrado y con el sello de ICEX en el cierre del mismo, avisando además de la confidencialidad del contenido del sobre.

4.6.5.3.2. Entrada de Soportes y documentos.

ICEX cuenta con un sistema de registro de entrada y salida de soportes y documentos que contengan datos de carácter personal.

A fin de preservar la integridad de los datos contenidos en el sistema de información de ICEX, se ha instalado en el sistema informático el antivirus contratado por ICEX que está configurado de manera que se efectúen búsquedas automáticas en cada fichero abierto desde cualquiera de los soportes introducidos en el sistema.

La solicitud y autorización de entrada de soportes se anota en el correspondiente registro.

4.6.5.4. Gestión de Soportes aplicable a Nivel Medio de Seguridad

4.6.5.4.1. Objetivo

El objetivo de esta política es regular las condiciones generales para el control y gestión de cualquier tipo de soporte manejado por el personal de ICEX, y que contenga datos personales de su responsabilidad a los que les sea aplicable el Nivel Medio de seguridad.

4.6.5.4.2. Contenido

Además de las obligaciones establecidas en el Nivel Básico, con respecto a la Gestión de Soportes y Documentos, debe registrarse la entrada y salida de soportes, de forma que directa o indirectamente, se conozca el tipo de documento o soporte, la fecha y hora de la entrada o salida, el emisor o receptor, el número de documentos o soportes incluidos en el envío y la persona responsable de la recepción o entrega, que debe estar debidamente autorizada.

Estas obligaciones deben alcanzar a todo soporte físico y lógico, así como cualquier documento, incluidos los comprendidos y/o anejos a un correo electrónico, independientemente del soporte en el que se encuentre, que contenga datos de carácter personal.

Debido a la gran dificultad de establecer este control en ICEX de forma universal, el Responsable de Seguridad de cada Departamento debe responsabilizarse de cumplir con estas obligaciones.

4.6.5.4.3. Procedimiento

1. *Autorización de entrada y salida de soportes y documentos*

Cuando por motivos excepcionales, sea necesario el envío de documentos y/o soportes con información confidencial o de carácter personal, se solicitará autorización al Responsable de Seguridad del departamento interesado.

Los documentos y/o soportes que previamente hayan sido inventariados y autorizados por el Responsable de Seguridad por Departamento interesado, podrán ser empleados en operaciones de entrada y salida de ICEX.

Registro de entrada y salida de soportes y documentos

La entrada o salida de soportes será controlada directamente por el Responsable de Seguridad por Departamento, quien registrará dicho evento en el Registro de Entrada y Salida, conforme al modelo del ANEXO IV: Inventario de Soportes.

La entrada o salida de archivos anexos a correos electrónicos será registrada en la bandeja de entrada o de salida de gestor de correo electrónico.

En cualquier caso, el Responsable de Seguridad por Departamento interesado, registrará la solicitud, así como si fue autorizada o no. Dicho registro contendrá al menos la siguiente información:

- Tipo de documento o soporte.
- Fecha y hora de la entrada/salida.
- Destinatario/Remitente.
- Número de documentos o soportes incluidos en el envío.
- Tipo de información que contiene.
- Forma de envío.

4.6.5.5. Gestión de Soportes aplicable a Nivel Alto de Seguridad

4.6.5.5.1. Objetivo

El objetivo de esta política es regular las condiciones generales para el control y distribución de cualquier tipo de soporte manejado por el personal de ICEX, y que contenga datos personales de su responsabilidad a los que les sea aplicable el Nivel Alto de seguridad.

4.6.5.5.2. Contenido

La identificación de los soportes que contengan datos de carácter personal responsabilidad de ICEX a los que les sea aplicable el Nivel Alto de seguridad, debe realizarse utilizando sistemas de etiquetado comprensibles únicamente por los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

La distribución de los soportes que contengan datos de carácter personal debe realizarse cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, deben cifrarse los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control de ICEX.

Debe evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el presente Documento de Seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

4.6.5.5.3. Procedimiento

1. *Etiquetado e inventariado de los soportes*

El etiquetado de los soportes establecido en el Nivel Alto de Seguridad del presente Documento de Seguridad se hará de forma codificada, de forma que sólo los usuarios autorizados puedan conocer la información que contienen.

El Responsable de Seguridad por Departamento coordinará las acciones necesarias para que todo soporte sea etiquetado e inventariado en siguiendo el modelo del Anexo IV: Inventario de Soportes.

2. *Mecanismos de cifrado de soportes y dispositivos portátiles*

El Responsable de Seguridad del Departamento informará al personal a su cargo de la obligatoriedad de utilizar mecanismos de cifrado cuando la información salga fuera de los locales bajo el control de ICEX.

En caso de que sea necesario distribuir, extraer, enviar o sacar soportes o dispositivos portátiles que contengan datos personales responsabilidad de ICEX fuera de los locales bajo su control, el usuario que haya detectado tal necesidad, la trasladará al Responsable de Seguridad Departamento.

El Responsable de Seguridad del Departamento solicitará al Responsable de la Dirección de Tecnologías de la Información la instalación, configuración y formación para los empleados afectados sobre los mecanismos de cifrado para soportes, dispositivos portátiles y documentos adjuntos a correos electrónicos.

4.7. Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponde con arreglo a lo dispuesto en el RLOPD y lo expresado en éste documento.

Los ficheros temporales o copias de documentos así creados serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.
Lo anterior incluye los ficheros temporales que utilicen y generen las aplicaciones de acceso al Fichero,

Las copias de trabajo de documentos en formato papel, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de fomentos o copias de trabajo en formato papel.

El Responsable del Fichero o, en su caso, el Responsable de Seguridad, deberá asegurarse de que los ficheros temporales o copias de trabajo de los documentos no son accesibles para personal no autorizado.

4.8. Responsable de Seguridad

El Responsable del Fichero designará uno o varios Responsables de Seguridad encargados de coordinar y controlar las medidas definidas en este Documento de Seguridad.

Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados.
En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al Responsable del Fichero de acuerdo con el RLOPD.

El Responsable/es de Seguridad desempeñará las funciones encomendadas durante el periodo de vigencia que se haya asignado para el cargo. Transcurrido el plazo, el Responsable del Fichero nombrará un nuevo Responsable de Seguridad o lo renovará por un período de tiempo igual al que ha desempeñado hasta ahora.

Es fundamental, en la política de protección de datos de carácter personal, que exista una efectiva correlación entre las funciones y obligaciones que desarrolla cada usuario del sistema y la realidad, así como el conocimiento por parte del personal de ICEX de la normativa de seguridad que afecta al desarrollo de sus funciones, garantizándose el cumplimiento de lo dispuesto en el artículo 89 RLOPD. Es tarea del Responsable de Seguridad concienciar al personal acerca de la importancia de la protección de los datos contenidos en el sistema informático de ICEX.

A efectos del presente documento de seguridad se distinguen las siguientes categorías:

CATEGORÍA	RESPONSABLES
Responsable del Fichero	ICEX España Exportación e Inversiones
Responsable de Seguridad	Se nombrará a un Responsable de Seguridad por cada Departamento. ANEXO IX: Identificación de Res-
Administrador de Sistemas	Que nombrara la Direccion de Tecnologías de la Información

4.8.1. Obligaciones específicas del Responsable de Seguridad

Persona o Personas Físicas, designadas por el Responsable del Fichero, con la misión de coordinar y controlar las medidas de seguridad aplicables. Sus funciones son:

- Informar periódicamente al Responsable del Fichero de todas las actuaciones y anomalías e incidencias acaecidas en los sistemas de información de ICEX en materia de protección de datos.
- Cooperar con el Responsable del Fichero controlando el cumplimiento de las normas.
- Habilitar y gestionar un registro central de incidencias dependiente del servicio de atención al usuario. Adoptar las medidas precisas para hacer frente a cualquier incidencia que pudiera sobrevenir.

- Mantener actualizado el Documento de Seguridad, realizando las modificaciones oportunas siempre que se produzcan cambios relevantes en el mismo, así como para adaptarlo a la normativa vigente de cada momento. Para ello deberá evaluar las modificaciones propuestas por los responsables jurídicos y de seguridad, así como de los usuarios del sistema. Supervisar la puesta en marcha de las medidas de seguridad en el área que le fuera asignada.

- Realizar controles periódicos de verificación del cumplimiento de las medidas de seguridad.

- Controlar la existencia y el cumplimiento por parte del personal, de los procedimientos de acceso establecidos.

- Habilitar y gestionar un inventario de soportes y un libro-registro de entradas y salidas de soportes informáticos, que contengan datos de carácter personal fuera del ámbito físico de ICEX que se efectúen desde sus respectivos departamentos.

En ICEX se constituye a un Responsable de Seguridad por cada departamento, el cual tendrá las siguientes funciones:

- En el caso del Responsable de Seguridad por Departamento de Recursos Humanos, se adoptarán las medidas necesarias para que el personal interno y externo conozca sus funciones y obligaciones en materia de protección de datos, ya sea a través de la firma del contrato laboral, o a través de la firma de un documento que recoja las Funciones y Obligaciones Generales recogidas en el presente Documento de Seguridad. En cualquier caso, se conservará acreditación del cumplimiento de esta función.

- Decidir sobre la finalidad, contenido y uso de un fichero cuando algún empleado a su cargo le haya expresado la necesidad de crearlo, y seguir el procedimiento descrito en el presente Documento de Seguridad para la notificación de ficheros.

- Decidir sobre la modificación o eliminación de ficheros de su departamento, y seguir el procedimiento descrito en el presente Documento de Seguridad para la notificación de ficheros.

- Autorizar la creación de nuevos formularios de recogida de datos dentro de su departamento de forma que lleven incorporada las cláusulas informativas pertinentes.

- Autorizar la concesión, modificación y supresión de permisos de acceso a ficheros y recursos de la Entidad para los empleados a su cargo.

- Autorizar la salida de equipos portátiles y soportes fuera de los locales de ICEX.

- Autorizar la salida de ficheros fuera de los locales de ICEX, incluidos los adjuntos a un correo electrónico.

- Solicitar el alta, baja o modificación de usuarios y contraseñas para los empleados a su cargo.

- Autorizar los procedimientos de restauración de los ficheros de Nivel Medio y Alto de su departamento.

- Autorizar la copia o reproducción de documentos que contengan información clasificada de nivel Alto.

- Autorizar el acceso a la documentación de su departamento clasificada de Nivel Alto.

- Controlar directamente los mecanismos que registren el acceso a los ficheros de Nivel Alto que sean responsabilidad de su departamento.

De otra parte, las obligaciones del Responsable de Seguridad de cada Departamento serán:

- Colaborar con el Responsable ARCO cuando se reciba una solicitud de ejercicio de Derechos ARCO.
- Definir los criterios de archivo de la documentación dentro de su departamento.
- Controlar el buen uso de los dispositivos de almacenamiento de la documentación dentro de su departamento.
- Controlar que el personal a su cargo custodia debidamente la documentación del departamento.
- Controlar el acceso a las áreas donde se encuentren los dispositivos de almacenamiento de ficheros de Nivel Alto de su departamento.
- Colaborar en el mantenimiento de los anexos del presente Documento de Seguridad.
- Conocer y aplicar los procedimientos establecidos en el presente Documento de Seguridad para su difusión entre el personal a su cargo.
- Controlar directamente los mecanismos que registren el acceso a los ficheros de Nivel Alto que sean responsabilidad de su departamento.
- Revisar mensualmente el registro de accesos a los ficheros de nivel alto que sean responsabilidad de su departamento.
- Elaborar mensualmente un informe del registro de accesos de los ficheros de Nivel Alto que sean responsabilidad de su departamento.

Adicionalmente a las funciones desempeñadas por el Responsable de Seguridad, en ICEX se podrá constituir un Comité de Seguridad con las funciones y obligaciones descritas en el apartado 3.3.3.

El Comité de Seguridad se reunirá y pondrá de manifiesto la evolución y obligaciones en materia de seguimiento y mantenimiento de las medidas de seguridad.

4.8.2. Nombramiento del Responsable de Seguridad.

El nombramiento oficial del Responsable de Seguridad de cada departamento se recoge en el Anexo X: Nombramiento Responsable de Seguridad.

4.9. Copias de Seguridad

Se realizará como mínimo una copia de seguridad semanal. El procedimiento para la recuperación de los datos debe garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Por ello, estas cláusulas tienen como objeto regular las condiciones generales para la generación y restauración de copias de seguridad de los datos personales responsabilidad de ICEX.

Para garantizar la seguridad de los datos, además de procurar la confidencialidad de los mismos es preciso certificar su integridad y disponibilidad.

Para asegurar la existencia de estas dos características fundamentales de la protección de datos, es preciso establecer procedimientos de respaldo y recuperación de los mismos, que en el supuesto de fallo del sistema permitan recuperar y en su caso reconstruir dicha información.

Se designará a una o varias personas de la Dirección de Tecnologías de la Información que deberán obtener periódicamente backups de los sistemas de información de ICEX, a efectos de crear un respaldo a fin de efectuar las tareas de recuperación de datos en caso de que se suscitara una pérdida de los mismos. Cuando se utilicen procesos automatizados basados en robots o similares, el sistema deberá controlar el correcto funcionamiento del dispositivo. Esta es la tarea de los operadores ya que dichos procesos son automáticos y el operador lo que controla que la tarea del día se haya efectuado correctamente, y que la del día siguiente se encuentre correctamente preparado en su lanzamiento.

4.9.1. Procedimiento de realización de copias de respaldo

Las copias de seguridad deben de realizarse como mínimo con una periodicidad semanal, salvo en el supuesto de que no se hubiera producido ninguna actualización de datos, dejando constancia en su caso, de la aplicación través de la cual se automatiza el proceso de generación de copias de seguridad. En tal caso deberá conservarse el LOG generado por la aplicación que confirme la correcta generación de la copia de seguridad. El soporte magnético que las almacena dispondrá de toda la información del sistema.

Se designará a una o varias personas del Departamento de Informática que deberán obtener periódicamente backups de los sistemas de información de ICEX, a efectos de crear un respaldo a fin de efectuar las tareas de recuperación de datos en caso de que se suscitara una pérdida de los mismos. Cuando se utilicen procesos automatizados basados en robots o similares, el sistema deberá controlar el correcto funcionamiento del dispositivo. Esta es la tarea de los operadores ya que dichos procesos son automáticos y el operador lo que controla que la tarea del día se haya efectuado correctamente, y que la del día siguiente se encuentre correctamente preparado en su lanzamiento.

Para garantizar en todo momento la integridad de la información de la ICEX dispone de un procedimiento de copias de seguridad basado en un sistema de copiado de datos en cintas denominado Data Protector.

En el caso de que se produzca un fallo en el sistema con pérdida total o parcial de los datos del fichero, existirá un procedimiento informático o manual que permita reconstruir la información al estado en que se encontraban en el momento en que se produjo la incidencia. Esta operación deberá realizarse partiendo de la última copia de respaldo obtenida.

4.9.1.1. Procedimientos de Backup

La creación o modificación, de forma puntual o definitiva del tratamiento de los procedimientos de backup para un fichero con datos de carácter personal, deberá ser autorizada por el Responsable de Seguridad y posteriormente enviada al responsable técnico correspondiente de la Dirección de Tecnologías de la Información.

El mantenimiento y seguimiento de las políticas de seguridad descritas a continuación será responsabilidad de la Dirección de Tecnologías de la Información. No obstante el incumplimiento de las mismas podría considerarse como una incidencia de seguridad y el Responsable de Seguridad de la Entidad podría tomar las medidas oportunas.

El Responsable de Seguridad, o cualquier otra persona en su nombre, tiene la potestad de realizar revisiones periódicas con el objetivo de controlar el seguimiento de las políticas establecidas en materia de seguridad.

Las características básicas de los procedimientos de backup llevados a cabo en cada sistema son las siguientes:

- La copia incluye los datos sensibles de la instalación.
- El proceso se lanza automáticamente todos los días, una vez finalizados los procesos diarios.
- La copia diaria de los datos es incremental.
- Se registra en un LOG el resultado del proceso, siendo consultado posteriormente por el administrador del sistema.

Asimismo, respecto de las copias de seguridad, aunque se indicará en su procedimiento concreto, se indica que existe un intercambio de cintas entre la Sala técnica de C278 y la de ICEX-CECO (c/ Herrera Oria) que se hace de forma semanal a través de la gestión autorizada en un formulario donde se registran las entradas y salidas de los soportes.

4.9.1.2. Procedimientos de Recuperación

Los procedimientos existentes para la realización de copias de respaldo y para la recuperación de los datos garantizan su reconstrucción en el estado en que estaban a tiempo de producirse la incidencia, pérdida o destrucción de la información.

La creación o modificación, de forma puntual o definitiva del tratamiento de los procedimientos de recuperación para un fichero con datos de carácter personal, deberá ser autorizada por el Responsable de Seguridad y ejecutado por la Dirección de Tecnologías de la Información.

El Responsable de Seguridad, o cualquier otra persona designada de la Dirección de Tecnologías de la Información de ICEX, tiene la potestad de realizar revisiones periódicas con el objetivo de controlar el seguimiento de las políticas establecidas en materia de seguridad.

4.9.1.3. Recuperación de datos

El procedimiento para la recuperación de datos debe garantizar en todo momento su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción.

En caso de fallo del sistema con pérdida total o parcial de los datos del Fichero existiría un procedimiento, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente respecto de los ficheros parcialmente automatizados (mixtos) y siempre que exista documentación que permita alcanzar la recuperación de los datos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción, se procederá a grabar manualmente los datos quedando constancia motivada de este hecho en el registro de incidencias.

La recuperación de datos se realizará con el visto bueno del Responsable de Seguridad, y previa autorización escrita del Responsable del fichero. La creación o modificación, de forma puntual o definitiva del tratamiento de los procedimientos de recuperación para un fichero con datos de carácter personal, deberá ser autorizada por el Responsable de Seguridad y ejecutado por la Dirección de Tecnologías de la Información.

El Responsable de Seguridad, o cualquier otra persona designada por la Dirección de Tecnologías de la Información de ICEX, tiene la potestad de realizar revisiones periódicas con el objetivo de controlar el seguimiento de las políticas establecidas en materia de seguridad.

Las recuperaciones figurarán en el Registro de Incidencias, indicando los procedimientos realizados de recuperación de datos, la persona que ejecutó el proceso, los datos restaurados y, en su caso, los datos que ha sido necesario grabar manualmente en el proceso de recuperación.

Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

4.9.1.4. Verificación de los procedimientos de copia y recuperación de datos

El Responsable del Fichero o la persona con autorización delegada del responsable del fichero o tratamiento verificará, cada seis (6) meses, la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.

4.9.1.5. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que previamente se hayan realizado una copia de seguridad y se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

De las pruebas realizadas conforme al párrafo anterior deberá quedar constancia en el registro de incidencias.

4.9.1.6. Almacenamiento de las copias de seguridad

Las copias de respaldo y recuperación se encuentran almacenadas según lo establecido en el Anexo XI: Copias de seguridad.

4.9.2. Copias de respaldo de Nivel Alto de Seguridad

4.9.2.1. Objetivo y Contenido

El objetivo de esta política es regular las condiciones generales para la conservación de copias de seguridad de los datos personales responsabilidad de ICEX a los que les sean aplicables las medidas de seguridad de Nivel Alto.

Debe conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan. Este lugar también debe estar sometido a las medidas de seguridad establecidas en el presente Documento de Seguridad.

4.9.2.2. Procedimiento

4.9.2.2.1. Conservación en lugar diferente

El Responsable de la Dirección de Tecnologías de la Información dejará constancia del lugar físico separado en el que se conservan las copias de respaldo.

4.9.2.2.2. Procedimiento de traslado

El procedimiento de traslado de las copias de seguridad, deberá cumplir íntegramente con lo establecido en el presente Documento de Seguridad para la Gestión de Soportes, indicado anteriormente en el apartado 4.6.

4.10. Procedimiento de Notificación, Registro, Gestión y Respuesta ante las incidencias

4.10.1. Definición

Una incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, es decir, a la confidencialidad, integridad y disponibilidad de los datos del fichero. Cualquier incumplimiento de la normativa del presente Documento de Seguridad se considera una incidencia. El objetivo de éstas cláusulas es regular las condiciones generales para la gestión y el control de todas las incidencias que pudiesen afectar a la seguridad de los datos personales de los que ICEX es responsable

Con el fin de optimizar la gestión de las incidencias que puedan producirse el Responsable de Seguridad se responsabiliza de que todo el personal tenga conocimiento de:

- A quién debe recurrir cuando sea detectada una incidencia.
- La existencia de un catálogo de incidencias al que debe dar notificación.
- El procedimiento a seguir.
- La documentación que se precise a la hora de proceder a notificar una incidencia.

4.10.2. Procedimiento

Todo usuario que tenga conocimiento de una incidencia será responsable del registro de la misma y de su comunicación por escrito al Responsable del Fichero o la persona con autorización delegada.

El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del fichero o tratamiento por parte de ese usuario.

Todo usuario que detecte una incidencia que pueda afectar a la seguridad de los datos de carácter personal, deberá comunicárselo al Responsable de la Dirección de Tecnologías de la Información con indicación de:

- Fecha y hora en que se produjo o se ha detectado
- Identidad del usuario que hubiese detectado la incidencia y que por tanto realiza la notificación
- Descripción de la incidencia, es decir el tipo de incidencias
- Persona a quién se le comunica
- Efectos que se hubieran derivado de las mismas y medidas correctoras aplicadas

Éste debe gestionar, solucionar y registrar todas las incidencias que le hayan sido notificadas, de forma que se puedan evaluar periódicamente los aspectos más débiles de la seguridad de ICEX y adoptar las medidas oportunas para reforzar dichos aspectos.

El procedimiento de incidencias se divide en dos soportes de comunicación:

1. a través del CSU - consultas internas mediante correo electrónico.

2. y a través del Contact Center - consultas e incidencias externas.

El proceso de resolución de la incidencia deberá seguir las siguientes fases:

Detección de la incidencia. El usuario descubre alguna anomalía con relación a la seguridad de datos de carácter personal.

Comunicación de la incidencia a través del sistema correspondiente en función de su tipología (CSU o contact center).

Registro de la incidencia. El Comité de Seguridad recibe los datos descriptivos de la anomalía, dichos datos se incluyen en la base de datos de la propia aplicación, según la que corresponda. En función del tipo de incidencia, y en virtud de los tres perfiles existentes en el seno del Comité de Seguridad, será asignada la incidencia a uno u otro componente.

Análisis y Diagnóstico. Definición y ejecución de la acción correctora / preventiva. El Comité de Seguridad (o la persona o personas encargadas de la incidencia en virtud de su tipología) analiza la incidencia reportada. Se buscará una relación entre el efecto y todas las posibles causas. Para la resolución de la incidencia, el Comité de Seguridad contará además de con su propia práctica, con la experiencia ya registrada sobre otras incidencias que pudieran estar relacionadas o responder a la misma causa, así como, con la colaboración de todas aquellas personas que pudieran estar involucradas en la incidencia registrada. Se tendrá que determinar, entre todas las causas posibles, la más probable como origen del problema. En caso de no ser posible establecer la resolución de la incidencia se reportará esta situación al responsable afectado.

Resolución de la incidencia. El Comité de Seguridad (o la persona o personas encargadas de la incidencia en virtud de su tipología) una vez resuelta la incidencia registrará la información de las acciones tomadas para la resolución de la misma, de manera que la persona que detectó la incidencia así como aquellas personas que hayan estado involucradas puedan conocer tales acciones correctoras.

Documentación y cierre de la acción correctora / preventiva. Una vez solucionada la anomalía, el Comité de Seguridad comprobará que la incidencia queda guardada en el registro de incidencias (cualquiera que fuera el origen, y por tanto la aplicación de gestión), con constancia del problema y de las acciones llevadas a cabo para su resolución. No obstante, la incidencia no quedará totalmente cerrada hasta que el usuario acepte la resolución de la misma o lleve a cabo las acciones tendentes para resolver la anomalía, si es necesario.

Clasificación de la incidencia. Todas las incidencias registradas serán clasificadas de forma que dicha clasificación ayude al diagnóstico y resolución de futuras incidencias, así como al establecimiento de prioridades en la resolución de las mismas.

Elaboración de Informes de seguimiento y control de las incidencias. El Comité de Seguridad podrá facilitar listados de las incidencias pendientes, así como cualquier otro informe o listado que puntualmente le sea solicitado y que pueda obtenerse a través de la información disponible. Concretamente, se elaboran informes de seguimiento de las incidencias tomando como referencia las categorías existentes en el registro de incidencias. Con dichos informes se analizan los motivos que las están ocasionando y se adoptan medidas preventivas en función de las incidencias con el fin de evitar que vuelvan a producirse (como por ejemplo la formación de usuarios y técnicos...etc.).
Gestión de incidencias: El registro de la gestión de incidencias se llevará a través de las dos aplicaciones de control.

Catálogo de incidencias: tabla.

Registro y resolución de incidencias: Con el fin de optimizar la gestión de las incidencias que puedan producirse el Comité de Seguridad de ICEX se responsabiliza de que todo el personal tenga conocimiento de:

- A quién debe recurrir cuando sea detectada una incidencia.
- La existencia de un catálogo de incidencias al que debe dar notificación.
- El procedimiento a seguir.
- La documentación que se precise a la hora de proceder a notificar una incidencia

El Registro de Incidencias debe ser conservado por la Dirección de Tecnologías de la Información durante un plazo mínimo de dos (2) años, para la atención de las posibles responsabilidades ante la AEPD.

Se consideran incidencias que pueden afectar a la seguridad de los datos de carácter personal, entre otras, las siguientes:

- La creación de bases de datos de carácter personal sin haber cursado solicitud de registro en la AEPD.
- El recabo de datos de carácter personal sin la autorización del afectado y sin informarle de sus derechos.
- El uso de los datos de carácter personal para otra finalidad diferente a la registrada en la AEPD.
- La violación de los sistemas de control de acceso.
- La pérdida o revelación accidental de contraseñas de acceso.
- El borrado fortuito de datos de carácter personal.
- La salida de datos en soportes informáticos sin la autorización pertinente.
- La salida de datos en soportes diferentes a los autorizados en el registro de la base de datos.
- El uso ilícito de datos de carácter personal.
- La ejecución del proceso de recuperación de datos.
- La incidencia en la gestión de los backups.
- La pérdida, hurto o robo de tarjetas, llaves u otros mecanismos de acceso físico.
- La pérdida, hurto o robo de recursos protegidos de la Entidad, ya sean soportes, documentos, o equipos informáticos.
- El mal funcionamiento de equipos o aplicaciones informáticas destinadas al tratamiento de datos personales.

Gestión de incidencias: análisis, diagnóstico y resolución de incidencias

En persona, o bien a través de algún técnico del departamento, el Responsable de la Dirección de Tecnologías de la Información deberá ponerse en contacto con el usuario que notificó la incidencia, realizar las averiguaciones pertinentes a fin de poder analizar la incidencia y determinar la mejor solución a la misma.

Una vez resuelta la incidencia, el Responsable de la Dirección de Tecnologías de la Información o el técnico en que hubiese delegado, informará convenientemente de las acciones tomadas para la resolución de la misma a la persona que detectó la incidencia así como a aquellas personas que hayan estado involucradas.

En caso de ser necesario, se harán recomendaciones al usuario o se le impartirá la formación necesaria para evitar que en un futuro vuelva a repetirse la misma incidencia.

4.10.3. Registro de Incidencias

4.10.3.1. Procedimiento

Una vez solucionada la incidencia, el Responsable de la Dirección de Tecnologías de la Información deberá registrarla en el Anexo XII: Gestión de incidencias.

- Fecha y hora de la incidencia.
- Identidad del usuario que hubiese detectado la incidencia.
- Descripción de la incidencia.
- Identidad de la persona que gestionó la incidencia.
- Efectos derivados de la incidencia
- Medidas correctoras aplicadas

Los registros correspondientes a la gestión de incidencias se podrán analizar desde las dos aplicaciones de notificación y gestión.

4.10.3.2. Procedimiento para datos de Nivel de Seguridad Medio

Para la gestión de las incidencias que puedan afectar a la seguridad de los datos personales responsabilidad de ICEX a los que sea aplicable el Nivel Medio de Seguridad, en el registro de incidencias establecido para el Nivel Básico, deben consignarse, además, los procedimientos realizados de recuperación de datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

El Responsable de Seguridad por Departamento debe autorizar previamente la ejecución de los procedimientos de recuperación de datos.

El procedimiento será el siguiente: Cuando la incidencia requiera la recuperación de datos personales a los que les sea aplicable el Nivel Medio de seguridad, además de seguir el procedimiento establecido para el Nivel Básico, el Responsable de la Dirección de Tecnologías de la Información solicitará la autorización del Responsable de Seguridad por Departamento afectado y dejará constancia del hecho en el Registro de Incidencias, conforme al Anexo XII: Gestión de incidencias.

4.10.4. Elaboración de Informes

El Responsable de la Dirección de Tecnologías de la Información podrá facilitar listados de las incidencias pendientes, así como cualquier otro informe o listado que puntualmente le sea solicitado y que pueda obtenerse a través de la información disponible.

Concretamente, se elaborarán informes de seguimiento de las incidencias tomando como referencia las categorías existentes en el registro de incidencias.

Dichos informes se analizarán conjuntamente con el Comité de Seguridad examinando los motivos que ocasionaron las incidencias con el fin de adoptar las medidas preventivas para evitar que vuelvan a producirse (como por ejemplo la formación de usuarios y técnicos, etc.).

5. Niveles de Seguridad

5.1. Aplicación de los niveles de seguridad

Se deben adoptar las medidas de índole técnica que garanticen la seguridad de los datos de carácter personal y eviten su alteración, perdida, tratamiento o acceso no autorizado.
El RLOPD clasifica en su artículo 80, las medidas de seguridad exigibles a los ficheros y tratamiento en tres niveles: básico, medio y alto, atendiendo a la naturaleza de la información.

Los niveles de seguridad son acumulativos, de modo que un fichero de nivel alto deberá aplicar también las medidas previstas en los niveles básico y medio. Las medidas de seguridad se aplican tanto a los ficheros como a los tratamientos, en soportes automatizados y no automatizados, así como deben aplicarse tanto por el Responsable del Fichero como por el Encargado del Tratamiento. Las medidas incluidas en cada una de los niveles de seguridad tienen la condición de mínimo exigibles, sin perjuicio de las disposiciones legales o reglamentariamente especificas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adopte el responsable del fichero.

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de Nivel Básico.

En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de **Nivel Básico** cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
- Los ficheros o tratamientos contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Deberán implantarse, además de las medidas de seguridad de Nivel Básico, las medidas de **Nivel Medio**, en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Aquellos relativos a la prestación de servicios de solvencia patrimonial y crédito.
- Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

- Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Además de las medidas de Nivel Básico y Medio, las medidas de **Nivel Alto** se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal especialmente:

- Los que se refieran a datos especialmente protegidos, relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

- Aquellos que contengan datos derivados de actos de violencia de género.

Cuando en el sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza d ellos datos que contenga, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos y que esto se haga constar en el documento de seguridad.

5.2. Cuadro resumen de la tipología de datos por niveles de seguridad

<table>
<tr><td>NIVEL BÁSICO</td><td colspan="2"></td></tr>
<tr><td colspan="3">NIVEL MEDIO</td></tr>
<tr><td colspan="3">NIVEL ALTO</td></tr>
<tr><td>Nombre y apellidos</td><td>Multas, infracciones administrativas o penales</td><td>Ideología</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>DNI</td><td></td><td>Afiliación sindical</td></tr>
<tr><td></td><td rowspan="2">Conjuntos de datos que permitan definir la personalidad del individuo</td><td></td></tr>
<tr><td>Firma</td><td>Religión</td></tr>
<tr><td>Dirección</td><td rowspan="4">Datos sobre impagos responsabilidad de empresas que prestan servicios de información sobre solvencia patrimonial y crédito</td><td></td></tr>
<tr><td></td><td>Creencias</td></tr>
<tr><td>Teléfono</td><td></td></tr>
<tr><td></td><td>Origen racial</td></tr>
</table>

E-mail	Datos fiscales responsabilidad de las administraciones tributarias	
		Salud
Foto		
Cuenta bancaria	Datos económicos responsabilidad de las entidades financieras	Vida sexual
Número de tarjeta de crédito	Datos responsabilidad de la Seguridad Social	
Estado civil		Violencia de género
Fecha de nacimiento		
Lugar de nacimiento		
Sexo		
Nacionalidad		
Lengua materna		
Licencias, permisos, autorizaciones		
CV, formación, titulaciones, expediente		
Profesión, ocupación, experiencia.		
Resto de datos personales a los que no les aplique el Nivel Medio ni el Nivel Alto.		

5.3. Cuadro resumen de las medidas del RLOPD por niveles de seguridad y tipos de tratamiento.

MEDIDAS DE SEGURIDAD	NIVEL BÁSICO	
	NIVEL MEDIO	
	NIVEL ALTO	

RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento. Se designará un responsable de seguridad por departamento.	
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
REGISTRO DE INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	**SOLO FICHEROS AUTOMATIZADOS** Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado.	**SOLO FICHEROS AUTOMATIZADOS** Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	**SOLO FICHEROS AUTOMATIZADOS** Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación dos (2) años.

CONTROL DE ACCESOS	Mismas condiciones para personal ajeno con acceso a los recursos de datos.		**SOLO FICHEROS NO AUTOMATIZADOS** Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

MEDIDAS DE SEGURIDAD	**NIVEL BÁSICO**		
	NIVEL MEDIO		
	NIVEL ALTO		
CRITERIOS DE ARCHIVO	**SOLO FICHEROS NO AUTOMATIZADOS** El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)		
ALMACENAMIENTO	**SOLO FICHEROS NO AUTOMATIZADOS** Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura		**SOLO FICHEROS NO AUTOMATIZADOS** Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	**SOLO FICHEROS NO AUTOMATIZADOS** Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		

COPIA O REPRODUCCIÓN			**SOLO FICHEROS NO AUTOMATIZADOS** Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
AUDITORIA		Al menos cada dos (2) años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis y conclusiones determinadas por el Comité de Seguridad.	

MEDIDAS DE SEGURIDAD	**NIVEL BÁSICO**		
	NIVEL MEDIO		
	NIVEL ALTO		
TELECOMUNICACIONES			**SOLO FICHEROS AUTOMATIZADOS** Transmisión de datos a través de redes electrónicas cifradas.
TRASLADO DOCUMENTACIÓN			**SOLO FICHEROS NO AUTOMATIZADOS** Medidas que impidan el acceso o manipulación en su traslado o transporte.

- Los niveles son acumulativos y tienen la condición de mínimos exigibles.

- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.

- Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del fichero o tratamiento, o encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, que tendrá que costar en el documento de seguridad, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- Los ficheros temporales o copias de documentos creados para la realización de trabajos temporales, deberán cumplir el nivel de seguridad correspondiente y serán borrados o destruidos una vez que hayan dejado de ser necesarios.

6. Medidas Aplicables a terceros con acceso a datos personales

6.1. Prestaciones de Servicios con acceso a datos personales

6.1.1. Contenido

La figura del acceso a los datos por cuenta de terceros es una excepción a la exigencia de consentimiento para poder realizar una cesión de datos. De esta manera, no se considerará cesión de datos el acceso de un tercero, a los datos de carácter personal, cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. En concreto, el Responsable del Tratamiento es la persona o entidad, autoridad pública, servicio o cualquier otro organismo que, sólo o con otros, trate datos por cuenta del responsable del fichero. En estos casos, el encargado del tratamiento también responde si incumple la normativa de protección de datos.

La realización de un tratamiento por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. No se considera encargado del tratamiento a la persona física que tenga acceso a los datos personales en su condición de empleado dentro de la relación laboral que mantiene con el responsable del fichero.

6.1.2. Encargado de tratamiento

La LOPD exige que el tratamiento por cuenta de terceros esté regulado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, donde han de cumplirse los siguientes requisitos:

- Debe establecerse expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.

- El encargado del tratamiento no aplicará o utilizará los datos con un fin distinto al que figure en el citado contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

- En el contrato habrán de estipularse las medidas de seguridad que el encargado del tratamiento estará obligado a implementar.

- Debe de incluirse en el contrato el compromiso de que, una vez cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No obstante, el encargado de tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

Además, el responsable deberá velar por que el encargado reúna las garantías necesarias para el cumplimiento del servicio encomendado.

ICEX establece, dentro de su política de seguridad, la prohibición expresa de iniciar relación alguna con terceros para el tratamiento de datos de carácter personal, si no existe la firma de un contrato revisado por la Dirección Adjunta de Asesoría Jurídica y Ayudas o del Departamento de Contratación, que garantice el nivel de seguridad requerido por ley para dicho tratamiento. Consecuentemente, todo Departamento tiene prohibido comunicar los datos de carácter personal al tercero mientras no esté firmado dicho contrato.

6.1.3. Procedimiento

Cuando se detecta una necesidad de contratación de un servicio para realizar el cual es necesario el acceso a los datos personales por parte de la parte contratada, la persona del Departamento que va a contratar los servicios del tercero, comunica a su Responsable el alcance y finalidad del servicio de tratamiento a contratar.

Obtenido el visto bueno del Responsable, la Dirección o el Departamento contratante comunica las condiciones de la operación a la Dirección Adjunta de Asesoría Jurídica y Ayudas o al Departamento de Contratación, que elabora el contrato pertinente, encargándose de regular los términos del contrato de acuerdo con lo dispuesto en el artículo 12 de la LOPD y en los artículos 20, 21, 22 y 26 del RLOPD. En concreto, éste contrato contemplará, entre otros, los siguientes aspectos:

- Obligación del tercero a tratar los datos conforme a las instrucciones de ICEX.
- Obligación del tercero a no aplicar ni utilizar los datos con un fin distinto al que figura en el contrato, ni a su comunicación a otras personas, ni siquiera para su conservación.
- Obligaciones de índole técnica y organizativas que el tercero esté obligado a implementar.
- Obligación de asunción de las medidas de seguridad en función del lugar donde se realice la prestación.
- Obligación del tercero a guardar el debido secreto profesional.
- Obligación de destruir o devolver a ICEX los datos tratados una vez ha finalizado la relación contractual.

Una vez elaborado el contrato, se ha de firmar por las partes autorizadas, quedando el original del contrato en la Dirección Adjunta de Asesoría Jurídica y Ayudas o en el Departamento de Contratación (según cuál de éstos haya gestionado el expediente de contratación) y copia del mismo en el Departamento solicitante.

En cumplimiento del artículo 82 RLOPD, la Dirección Adjunta de Asesoría Jurídica y Ayudas y el Departamento de Contratación mantienen en su habitual registro de contratos, un registro de aquellos que suponen acceso a datos por cuenta de terceros, de forma que ha creado una columna más en dicho registro donde deja marcado los contratos que tienen que ver con tratamiento de datos personales artículo 12 LOPD.

6.1.3.1. Prestación de Servicios en locales de ICEX

El Responsable de Seguridad por Departamento bajo cuya responsabilidad actúen los empleados externos, informará a dichas personas de sus Funciones y Obligaciones Generales en materia de protección de datos como usuarios del sistema de información, dejando constancia de ello a través del Anexo XIII: Ficheros con acceso de terceros.

6.1.3.2. Acceso remoto a los datos

El Responsable de Seguridad por Departamento que recibe el servicio contratado o, en caso de conflicto de responsables, el Responsable de Seguridad por Departamento que tenga mayor control sobre el fichero accedido, dejará constancia del acceso remoto por parte de un prestador de servicios en el Anexo XIII: Ficheros con acceso de terceros.

6.1.3.3. Prestaciones de Servicios en locales del prestador

El responsable de gestionar la contratación del servicio, regulará los términos del contrato de forma que se responsabilice al prestador de la inclusión del fichero o ficheros accedidos en su propio Documento de Seguridad.

Por su parte, el Responsable de Seguridad por Departamento que recibe el servicio contratado o, en caso de conflicto de responsables, el Responsable de Seguridad por Departamento que tenga mayor control sobre el fichero accedido, dejará constancia de la prestación de servicios a través del Anexo XIII: Ficheros con acceso de terceros.

6.2. Prestaciones de Servicios sin acceso a datos personales

En los supuestos en los que la contratación de un tercero o empresa para la prestación de un servicio no lleve aparejado el tratamiento de datos personales, ICEX adoptará las medidas adecuadas para limitar el acceso a los soportes que los contengan o a los recursos del sistema de información y establecerá expresamente en el contrato de prestación de servicios la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

En cumplimiento del artículo 83 RLOPD, se mantiene un registro de las empresas que prestan servicios sin acceso a datos de carácter personal en su habitual registro de contratos.

7. Medidas de Seguridad Aplicables a Ficheros no Automatizados

El RLOPD establece en sus artículos 105 a 114, las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados. El resto de medidas que han sido expuestas a lo largo del presente Documento de Seguridad son aquellas que son comunes para ficheros y tratamientos automatizados y no automatizados.

Por tanto, dado que ICEX dispone de ficheros y tratamientos no automatizados, será necesario implantar, además de las medidas comunes ya expuestas, las detalladas en el epígrafe siguiente.

7.1. Medidas de Nivel Básico

7.1.1. Criterios de Archivo

- **Concepto**

El archivo de los soportes o documentos debe realizarse de acuerdo con los criterios previstos en su respectiva legislación.

Estos criterios deben garantizar la correcta conservación, localización y consulta de la información contenida en los documentos, así como posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación (Derechos ARCO).

En el caso de que no exista norma aplicable, el Responsable del Fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

La documentación con datos de carácter personal propiedad de ICEX se encuentra almacenada en archivos metálicos, ordenada alfabéticamente, lo cual facilita la búsqueda y el manejo de la referida documentación.

- **Procedimiento**

El Responsable de Seguridad del Departamento se asegurará de aplicar los criterios de archivo exigidos por la legislación o conforme a su propio criterio.
El Responsable de Seguridad por Departamento informará al personal a su cargo de los criterios de archivo aplicables en su departamento y de la obligatoriedad de utilizarlos.

7.1.2. Dispositivos de almacenamiento

- **Concepto**

El RLOPD establece que los dispositivos de almacenamiento de la documentación que contenga datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características físicas de esos dispositivos no permitan adoptar esta medida, el Responsable del Fichero o tratamiento deberá adoptar las medidas que impidan el acceso de personas no autorizadas.
ICEX almacena la documentación con datos personales en archivos metálicos que disponen de llave para su apertura, y en cajones dotados también de apertura mediante llave. Los despachos donde se encuentra almacenada la información también disponen de puerta con llave, obstaculizando así la entrada a aquellas personas no autorizadas.

- **Procedimiento**

Los armarios y dispositivos de almacenamiento que dispongan de mecanismos de cierre, permanecerán cerrados cuando no estén siendo utilizados por el personal autorizado. En caso de disponer de cierre bajo llave, la llave estará en poder del Responsable de Seguridad por Departamento o del personal autorizado.

El acceso a los armarios y dispositivos de almacenamiento que no dispongan de mecanismos de cierre será controlado por el personal del departamento responsable de la custodia de los ficheros almacenados en el armario.

En todo caso, el Responsable de Seguridad por Departamento hará constar en el Anexo IV: Inventario de Soportes el control de seguridad ejercido sobre los armarios o dispositivos de almacenamiento.

7.1.3. Custodia de Soportes

7.1.3.1. Concepto

Mientras la documentación con datos de carácter personal no se encuentre archivada, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma debe custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

7.1.3.2. Procedimiento

Todo documento será archivado debidamente siguiendo el criterio legal o interno establecido por el Responsable de Seguridad por Departamento, según lo dispuesto en el Anexo IV: Inventario de Soportes.

Todo documento que se encuentre fuera del archivo será custodiado permanentemente por la persona que se encuentre al cargo de la misma, quien deberá proceder a su archivo en cuanto termine la tarea que motivó su extracción del archivo.

7.2. Medidas de Nivel Medio

7.2.1. Criterios de Archivo

El archivo de los soportes o documentos debe realizarse de acuerdo con los criterios previstos en su respectiva legislación.

Estos criterios deben garantizar la correcta conservación, localización y consulta de la información contenida en los documentos, así como posibilitar el ejercicio de los Derechos ARCO.

En el caso de que no exista norma aplicable, el Responsable del Fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

La documentación con datos de carácter personal propiedad de ICEX se encuentra almacenada en archivos metálicos, ordenada alfabéticamente, lo cual facilita la búsqueda y el manejo de la referida documentación.

7.2.2. Dispositivos de Almacenamiento

El RLOPD establece que los dispositivos de almacenamiento de la documentación que contenga datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.

Cuando las características físicas de esos dispositivos no permitan adoptar esta medida, el Responsable del Fichero o tratamiento deberá adoptar las medidas que impidan el acceso de personas no autorizadas.

ICEX almacena la documentación con datos personales en archivos metálicos que disponen de llave para su apertura, y en cajones dotados también de apertura mediante llave. Los despachos donde se encuentra almacenada la información también disponen de puerta con llave, obstaculizando así la entrada a aquellas personas no autorizadas.

7.2.3. Custodia de Soportes

El RLOPD establece que mientras la documentación que contenga datos de carácter personal se encuentra archivada en los dispositivos de almacenamiento destinados a tal efecto, la persona que se encuentre a cargo de la misma, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

7.3. Medidas de Nivel Alto

7.3.1. Dispositivos de almacenamiento

7.3.1.1. Concepto

Los armarios, archivadores u otros dispositivos de almacenamiento de ficheros no automatizados deben encontrarse dentro de zonas restringidas con puertas de acceso dotadas de llave o dispositivo equivalente.

Estas áreas deben permanecer cerradas cuando no sea preciso el acceso a los documentos.

Si no fuera posible ubicar estos dispositivos en áreas restringidas, deben tomarse medidas alternativas, dejando constancia motivada en el presente Documento de Seguridad.

7.3.1.2. Procedimiento

El Responsable de Seguridad por Departamento procurará que todos los armarios, archivadores y dispositivos de almacenamiento estén ubicados en salas o despachos bajo llave, que estará bajo su control.

El Responsable de Seguridad por Departamento se encargará de que dichas salas o despachos estén cerrados cuando no sea preciso el acceso a estas áreas.

Si no fuera posible ubicar estos dispositivos en áreas restringidas, deben tomarse medidas alternativas, de las que el Responsable de Seguridad por Departamento dejará constancia motivada en el Anexo IV: Inventario de Soportes.

7.3.2. Copias de Ficheros no Automatizados

7.3.2.1. Concepto

Las cláusulas aquí recogidas tienen como fin regular las condiciones generales para la copia o reproducción de ficheros que contengan datos personales responsabilidad de ICEX a los que les sean aplicables las medidas de seguridad de Nivel Alto.

La generación de copias o la reproducción de los documentos debe ser realizada bajo el control del personal autorizado en el documento de seguridad.

El desecho de las copias debe impedir el acceso posterior a la información.

7.3.2.2. Procedimiento

El Responsable de Seguridad por Departamento autorizará al personal a su cargo la copia de documentos a los que les sean aplicables las medidas de seguridad de Nivel Alto.
El Responsable de Seguridad por Departamento concienciará al personal a su cargo de la necesidad de desechar los documentos por medios que impidan su acceso posterior.
El Responsable de Seguridad por Departamento consignará en el Anexo IV: Inventario de Soportes el medio por el que se llevará a cabo la destrucción de los documentos y soportes desechados.

7.3.3. Acceso a Ficheros no Automatizados

7.3.3.1. Contenido

Cuando un fichero que contenga datos personales responsabilidad de ICEX a los que les sean aplicables las medidas de seguridad de Nivel Alto y pueda ser utilizado o consultado por múltiples usuarios, debe establecerse un mecanismo que permita identificar los accesos realizados a dicho fichero.

7.3.3.2. Procedimiento

El Responsable de Seguridad por Departamento coordinará las medidas necesarias para que todas las carpetas y archivadores que contengan datos a los que les sean aplicables las medidas de seguridad de Nivel Alto, dispongan de la hoja de registro de acceso a la documentación del (Anexo IV: Inventario de Soportes).

7.3.4. Traslado de Ficheros no Automatizados

7.3.4.1. Concepto

El objetivo de esta política es regular las condiciones generales para regular y controlar el traslado de ficheros que contengan datos personales responsabilidad de ICEX a los que les sean aplicables las medidas de seguridad de Nivel Alto.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero que contenga datos personales responsabilidad de ICEX a los que les sean aplicables las medidas de seguridad de Nivel Alto, deben adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

7.3.4.2. Procedimiento

El Responsable de Seguridad por Departamento consignará en el Anexo IV: Inventario de Soportes las medidas a adoptar en el traslado de los ficheros no automatizados.

El Responsable de Seguridad por Departamento proveerá los dispositivos necesarios para el traslado de la documentación e informará al personal a su cargo de la obligatoriedad de utilizarlos.

8. Derechos de los Afectados

8.1. Concepto

La LOPD recoge una serie de derechos fundamentales de los ciudadanos. En este apartado del Documento de Seguridad se ofrece información detallada sobre los mismos y sobre cómo se ejercen los Derechos ARCO.

La LOPD y el RLOPD establecen el derecho de las personas físicas afectadas a que se les facilite de forma gratuita el acceso, rectificación, cancelación y oposición de los datos personales que estén en nuestros ficheros.

Los afectados tendrán derecho a solicitar y obtener de forma sencilla y gratuita información de sus datos de carácter personal, una (1) vez al año, o cuantas veces estime necesarias en caso de acreditar un interés legítimo. Para ello deberán identificarse (nombre, apellidos, fotocopia de documento que acredite su identidad; la utilización de la firma electrónica identificativa del interesado eximirá la presentación del documento acreditativo de identidad) e indicar los datos necesarios para poder identificar el fichero que corresponda, en general a través del documento donde se recogieron sus datos.

Estos derechos son personalísimos, y sólo pueden ser ejercidos por sus legítimos titulares o sus representantes legales o voluntarios, aportando siempre documentación acreditativa de su condición. Por lo tanto, deberán ser denegados si no se aportase tal documentación.

Los derechos son independientes, de forma que ninguno de ellos será requisito previo para el ejercicio de otro.

ICEX dispondrá de un procedimiento sencillo y gratuito para el ejercicio de los derechos, no siendo viable la imposición del envío de cartas certificadas o llamadas a números de tarificación adicional, recogido en el Apartado Derechos de los Afectados.

ICEX atenderá las solicitudes aun cuando no se hubiese utilizado el procedimiento establecido, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud.

ICEX solicitará subsanación de la solicitud en caso de faltar alguno de los siguientes contenidos:

- Nombre y apellidos del interesado.
- Fotocopia del DNI o equivalente y, en su caso, documento acreditativo de la representación legal o voluntaria. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de otro documento identificativo.
- Petición en la que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante. En caso de faltar esta información, se archivará la solicitud de acuerdo con el procedimiento establecido al efecto.
- En su caso, documentos acreditativos de la petición que se formula.

ICEX informará a todos sus empleados del procedimiento establecido para el ejercicio de derechos, de forma que puedan informar a los interesados del procedimiento a seguir.

Los Derechos ARCO cuentan con un plazo determinado por la normativa para que el Responsable del Fichero los haga efectivos. Dichos plazos empiezan a contar a partir del día en que se recibe la solicitud dentro de la Entidad. Siempre que se hable de días, se entenderán días hábiles; y cuando se hable de meses, se contarán de fecha a fecha.

8.1.1. Derecho de Acceso

El derecho de acceso es uno de los derechos que la LOPD reconoce a los ciudadanos para que el ciudadano pueda controlar por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a obtener información sobre si éstos están siendo objeto de tratamiento y, en su caso, la finalidad del mismo, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. Por tanto, es el derecho que permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento. De manera que el afectado (cliente, proveedor o empleado) tiene el derecho a solicitar información sobre sus datos personales que estén en los Ficheros titularidad de ICEX, el

origen de los mismos (cómo fueron recabados y por quién), identificación de su consentimiento tácito o expreso, una estimación de las comunicaciones que le hayan sido realizadas, a través de ese fichero, o que se prevea realizar en un futuro, los cesionarios y la especificación de los usos concretos y finalidades para los que se recabaron y almacenaron dichos datos.

Su ejercicio es personalísimo, por lo que sólo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público del que sabe o presume que tiene sus datos, pudiendo optar por visualizarlos directamente en pantalla u obtenerlos por medio de escrito, copia, fotocopia o cualquier otro sistema adecuado al tipo de fichero de que se trate.

El responsable del fichero deberá resolver sobre lo solicitado en el plazo de un (1) mes desde la recepción de la solicitud. También deberá hacerlo aunque no disponga de datos del afectado. Si transcurrido dicho plazo, la solicitud no ha sido atendida adecuadamente, el interesado podrá dirigirse a la Agencia con copia de la solicitud cursada y de la contestación recibida (si existiera), para que ésta a su vez se dirija a la oficina designada con el objetivo de hacer efectivo el ejercicio de ese derecho.

La información que se proporcione al afectado deberá ser legible e inteligible.

El derecho de acceso no puede ser ejercitado en intervalos inferiores a doce (12) meses, salvo que se acredite un interés legítimo.

Únicamente se podrá acceder a la información pretendida si se trata de información sobre los datos que le son propios, pero no de información de terceros. De igual manera, únicamente podrá denegarse el acceso cuando la solicitud sea formulada por persona distinta del afectado, no se haya acreditado su posible representación, o bien cuando una Ley o una norma de rango comunitario así lo prevea.

8.1.2. Derecho de Rectificación

El derecho de rectificación es otro de los derechos que la LOPD reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que éstos se modifiquen cuando resulten inexactos o incompletos. Este derecho se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

Su ejercicio es personalísimo, por lo que sólo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere y la corrección que se solicita, y aportando al efecto la documentación que lo justifique.

ICEX deberá resolver sobre lo solicitado en el plazo máximo de diez (10) días a contar desde la recepción de la solicitud. También deberá hacerlo aunque no disponga de datos del afectado.

8.1.3. Derecho de Cancelación

El derecho de cancelación permite que se supriman los datos que resulten ser inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD.
Al igual que los anteriores es un derecho personalísimo, por lo que sólo podrá solicitarlo la persona interesada, quién deberá dirigirse a la empresa u organismo público que sabe o presume que tiene sus datos, indicando a qué datos se refiere, y aportando al efecto la documentación que lo justifique.

ICEX deberá resolver sobre la solicitud de cancelación en el plazo máximo de diez (10) días a contar desde la recepción de la solicitud. Deberá hacerlo aunque no disponga de datos del afectado.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas, transcurrido el cual deberá procederse a la cancelación.

No procederá la cancelación cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las relaciones contractuales entre la entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

8.1.4. Derecho de Oposición

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.

Su ejercicio es personalísimo, por lo que sólo podrá hacerlo la persona interesada mediante solicitud dirigida al responsable del tratamiento, en la que deberán hacerse constar los motivos fundados y legítimos que lo justifican.

ICEX, en el plazo máximo de diez (10) días desde la recepción de la solicitud, deberá resolver sobre la misma, excluyendo del tratamiento los datos relativos al afectado o denegando motivadamente la misma. Igualmente deberá hacerlo aunque no disponga de datos del afectado.

8.2. Protocolo Dº ARCO en ICEX y en las Oficinas Económicas y Comerciales de España en el extranjero (OFECOMES)

La LOPD reconoce a los afectados una serie de derechos mediante los cuales pueden hacer valer ante el responsable del fichero su condición de auténticos propietarios de la información sobre ellos recogida en los ficheros.

Estos derechos por parte del afectado frente al responsable del fichero son:

- Acceso a sus datos.
- Rectificación de sus datos.
- Cancelación de sus datos.
- Oposición al tratamiento de sus datos.

Todos estos derechos son personalísimos, por lo que su ejercicio se limita al afectado, acreditando su identidad, a su representante legal cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, o por representante voluntario, expresamente designado para el ejercicio del derecho. El responsable del fichero debe contestar cualquier solicitud de estos derechos que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros.

1. ICEX

ICEX cuenta con un procedimiento especial, establecido para gestionar las respuestas a las solicitudes del ejercicio a los Derechos ARCO por parte de los ciudadanos, el cual está establecido en el documento Producto: Gestiones LOPD, articulado conforme a lo establecido en la LOPD. Si bien es cierto, es importante tener en cuenta que la ley establece un plazo para atender la consulta de diez (10) días desde la recepción de la solicitud, para las solicitudes de Rectificación, Cancelación u Oposición, y un plazo de un (1) mes desde la recepción de la solicitud para las solicitudes de Acceso, así como que existe la obligación de contestar al solicitante aunque

no figuren datos suyos. También es requisito establecido en la misma que se debe hacer por medios que permitan acreditar el envío y la recepción de la notificación.

En la actualidad ICEX tiene implantado el siguiente procedimiento:

De acuerdo con lo establecido en la LOPD, así como en el RLOPD, los usuarios tienen reconocidos, y podrán ejercitar los Derechos ARCO al tratamiento, uso y cesión de sus datos, para lo cual deberán enviar una carta o correo electrónico a la siguiente dirección:

Paseo de la Castellana 278, 28046 Madrid.
Att. Dirección Adjunta de Asesoría Jurídica y Ayudas
Icex@icex.es
Una vez el interesado presenta la solicitud, esta sigue el siguiente flujo:

Nivel 1	- El equipo de Nivel1 remite escrito al interesado para que indique sus datos identificativos y acredite su legitimidad, en el supuesto que no los incorpore (utilizar plantilla creada al efecto). En caso de que el interesado que ejerza el derecho no acredite legitimidad, ICEX debería formular en un plazo de 5 días las observaciones que estime pertinentes para que la solicitud pueda ser salvada. -Cuando se recibe el escrito cumplimentado y copia del DNI se asigna la consulta a Nivel2.
Nivel 2	- Asigna la consulta al Departamento Correspondiente para que compruebe la existencia o no de datos de carácter personal (Derecho Acceso), los modifique (Derecho Rectificación) o los elimine en su caso (Derecho Cancelación u Oposición). Si fuera una solicitud referida a datos de OFECOMES, se asigna también a la OFECOMES correspondiente para que también esta actúe en consecuencia.
Nivel 3	- Asigna a la Dirección Adjunta de Asesoría Jurídica y Ayudas tras confirmarnos el Departamento correspondiente y también la OFECOMES en su caso, la existencia o no de datos, su eliminación o modificación, para que se informe al solicitante. - ICEX debe cumplir con los plazos establecidos en la LOPD: - Plazo para atender consultas de Derecho Acceso: Un (1) mes, desde la recepción de la solicitud. Es importante tener en cuenta, que el derecho de acceso no puede ser ejercitado en intervalos inferiores a doce (12) meses, salvo que se acredite un interés legítimo. - Plazo para atender consultas de Derecho de Rectificación, Cancelación u Oposición: diez (10) días desde la recepción de la solicitud.

2. OFECOMES

Si fuera una solicitud referida a datos de OFECOMES, la solicitud se asignará también a la OFECOMES correspondiente para que también esta actúe en consecuencia, eliminando, cancelando, bloqueando o modificando los datos personales relativos a la misma.

Formularios para el ejercicio de derechos

Los formularios indicados en los anexos que se indican a continuación deberán estar a disposición del público con el objeto de que este pueda ejercer sus derechos pertinentes.

- ANEXO XIV.: Modelo de solicitud del derecho de Acceso

- ANEXO XV.: Modelo de solicitud del derecho de Rectificación
- ANEXO XVI.: Modelo de solicitud del derecho de Cancelación
- ANEXO XVII.: Modelo de solicitud del derecho de Oposición

9. Revisión del Documento de Seguridad

El Documento de Seguridad ha de mantenerse actualizado en todo momento, y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos como consecuencia de los controles periódicos realizados, en su caso, o con los eventuales cambios en la normativa vigente en la materia de Protección de Datos de Carácter Personal. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del Documento de Seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

ICEX mantendrá una reunión ordinaria cada seis (6) meses y con carácter extraordinario cada vez que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos, con el objetivo de coordinar los cambios a introducir en el Documento de Seguridad.

9.1. Procedimiento de Control del Cumplimiento

Han de establecerse controles periódicos para verificar el cumplimiento de lo establecido en este Documento de Seguridad.

Se establecen controles semestrales. El semestre que coincida con la auditoría no se efectuará el control del cumplimiento. Se verificará lo siguiente:

- El inventario de Hardware y software
- Cumplimiento de la política general de seguridad
- Registro de Incidencias
- Variaciones en el Inventario de ficheros
- Cumplimiento de la Política de Protección de Datos
- Clasificación de los datos
- Configuración del Sistema
- Relación del personal y accesos autorizados
- Procedimiento de gestión de soportes
- Procedimiento de identificación y autenticación
- Si se cumple el proceso de copias de respaldo y recuperación

- Prestaciones de servicios con acceso y sin acceso a datos
- Contratos de Encargo de Tratamientos
- Contratos de confidencialidad; prestación de servicios sin acceso a los datos
- Variaciones de la legislación

9.2. Auditoría

9.2.1. Concepto

Los sistemas de información e instalaciones de tratamientos y almacenamientos de datos que contengan los datos calificados de Nivel Medio/Alto, deben someterse, al menos cada dos (2) años, a una auditoría interna o externa que verifique el cumplimiento de lo establecido en el Título VIII del RLOPD.

Si bien su realización es obligatoria para ficheros de nivel medio y alto cada dos (2) años, con carácter extraordinario, si se han realizado modificaciones sustanciales en el sistema de información, se realizará una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. Esta auditoría iniciará el cómputo de dos (2) años.

Dicha auditoría, que puede ser realizada de forma interna o externa, deberá finalizar en la emisión de un Informe, y deberá dictaminar la adecuación de las medidas y controles del documento de seguridad al nuevo RLOPD, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias, incluyendo los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de Auditoría serán analizados por el Responsable de Seguridad, que elevará las conclusiones al Responsable del Fichero para que adopte las medidas correctoras adecuadas y en todo caso, el informe quedará a disposición de la AEPD.

9.2.2. Plan de Auditorías

El Comité de Seguridad, elaborará un plan bienal de auditorías de todos los ficheros a los que les sean aplicables las medidas de seguridad de Nivel Medio o Alto, conforme a lo establecido en el presente Documento de Seguridad. Del mismo modo, podrá planificar alguna auditoría especial o extraordinaria en función de:

- Criticidad del fichero afectado.
- Resultado de auditorias anteriores.
- Innovaciones producidas en relación con el tratamiento de datos personales.

O cuando:

- Se produzcan cambios significativos en los sistemas de información.
- Se sospeche o se tenga la certeza de que el nivel de cumplimiento de los requisitos legales y normativos está comprometido.
- Se deba verificar la implantación de acciones correctivas.
- Se produzcan situaciones que así lo requieran, por ejemplo: incidentes graves de seguridad, eventos de entorno con posibles consecuencias graves, daños a la imagen, etc.

Este plan contemplará tanto el sistema documental como el cumplimiento de las medidas implantadas.

El plan establecerá:

- Los ficheros que deben ser auditados, indicando la fecha de dichas auditorías.

- Los auditores que intervienen (denominado equipo auditor). Estos deben ser personas cualificadas e independientes del área responsable del fichero a auditar. Pueden ser personal propio de ICEX o personal externo, siempre que acrediten la cualificación necesaria.
- Documentación de seguridad auditable.
-

Será función del Comité de Seguridad la custodia del plan de auditoría el cual se elabora sin formato definido. Como mínimo se realizará una auditoría bienal.

Es responsabilidad del Comité de Seguridad garantizar que se lleve a cabo el plan de auditorías.

9.2.3. Procedimiento

ICEX establece en éstas cláusulas una ruta a seguir para la realización de la auditoría, que el auditor deberá cumplir en lo posible.

El auditor, con la colaboración del Responsable de Seguridad, así como otros responsables involucrados en el proyecto, revisará la documentación necesaria para llevar a cabo la Auditoría. Dicha documentación deberá incluir la siguiente:

- LOPD.
- RLOPD.
- Documento de seguridad vigente.
- Histórico de notificaciones al RGPD, con las respectivas copias de las altas, modificaciones y cancelaciones de ficheros
- Mapa de sistemas de ICEX.
- Relación de aplicaciones utilizadas en el sistema informático de ICEX.
- Organigrama con indicación de los departamentos de ICEX y sus responsables.
- Auditorías anteriores.
- Informes de controles periódicos de verificación efectuados.

Tras la revisión de la documentación aplicable, los auditores prepararán, si así lo estimaran necesario, una lista de comprobación en la que relacionen los aspectos a verificar durante la Auditoría, de forma que preparen la auditoría a realizar.

Esta fase consiste principalmente en el estudio y análisis de la documentación que consideren oportuna y en la elaboración de los cuestionarios de auditorías o listas de comprobación relacionadas con dicha documentación.

Se considerarán los siguientes apartados:

- La estructura organizativa.
- Políticas que afecten a los ficheros a auditar.
- Los procedimientos administrativos y de actuación.
- Las áreas de trabajo, operaciones y procesos.
- El cumplimiento de la legislación vigente.
- La comprobación del cumplimiento de otros requisitos establecidos por la organización.
- Niveles de protección implantados, comprobando su conformidad con las especificaciones.

Seguidamente elaborarán un programa de auditoría concreto, incluyendo, por lo menos:

- Fecha de auditoría.
- Equipo auditor.
- Alcance de la auditoría.

- Procesos de negocio y/o actividad a auditar.
- Responsables involucrados.
- Normativa de referencia.
- Desglose detallado y cronológico de las actividades a realizar.

Este programa será enviado por parte del auditor antes de la fecha prevista de ejecución de la auditoría, al Comité de Seguridad, a fin de que informe del programa de auditoría a los involucrados, con el propósito de comprobar su disponibilidad y poder establecer el programa definitivo.

Una vez establecido el programa, el Comité de Seguridad lo notificará al personal involucrado de acuerdo al citado procedimiento.

9.2.4. Auditoría Documental

El equipo auditor revisará la documentación necesaria durante la auditoría que, como mínimo, deberá ser:

- Documento de seguridad.
- Inscripción de ficheros ante la AEPD.

9.2.5. Auditoría In Situ

Posteriormente, el auditor realizará una auditoría in situ de las medidas de seguridad para comprobar que las actividades se desarrollan según lo indicado en la documentación descrita en el presente procedimiento.

Durante el desarrollo de la auditoría los responsables de cada fichero deberán proporcionar a los auditores evidencias de las medidas de seguridad implantadas de acuerdo con el Título VIII del RLOPD.

Durante la auditoría se hará un seguimiento del estado de las no conformidades, la implantación y efectividad de acciones correctivas y acciones de mejora pendientes de anteriores auditorías, si las hubiera.

El equipo auditor procurará que las desviaciones detectadas estén documentadas de forma precisa y concisa, soportándose en datos objetivos y no en impresiones subjetivas del auditor.

Una vez finalizada la auditoría, se realizará una reunión final, en la que el equipo auditor expone las desviaciones encontradas a los responsables auditados, se comentan las causas y se plantean las posibles acciones correctivas. A esta reunión deberán asistir, además del Comité de Seguridad, los responsables afectados por la auditoría.

9.2.6. Realización de las Auditorías

La Auditoría se llevará a cabo durante las fechas previstas en el calendario de trabajo propuesta y las verificaciones a efectuar durante la misma, serán en general, de la siguiente naturaleza:

1. Revisión del Documento de Seguridad.

2. Examen de los registros y evidencias documentales generadas (auditorías, informes de controles periódicos de verificación, ficheros de logs).

3. Supervisión directa de operaciones de control de acceso, identificación, archivo, etc. Se comprueba que cada una de las actividades que se está desarrollando de la manera prescrita en el Documento de Seguridad.

4. Muestreo de ficheros incontrolados conteniendo bases de datos de carácter personal en los distintos terminales de los usuarios.

En el desarrollo de la Auditoría, el Auditor tendrá en cuenta que:

- Se evalúan solamente evidencias objetivas y contrastadas
- La verificación no tiene por qué limitarse a los aspectos recogidos, en su caso en la lista de comprobación.
- En el caso de detectar una posible desviación se investiga hasta confirmarla y, en caso afirmativo, averiguar si es sistemática o fortuita e identificar sus efectos y causas.
- Se debe hacer un seguimiento de las acciones correctoras definidas para solucionar las desviaciones en Auditorías anteriores.

Una vez finalizada la Auditoría, los auditores se reunirán con el/los responsables de la auditoría designados por el Comité de Seguridad proyecto al objeto de exponer las desviaciones detectadas y proponer las medidas correctoras para su resolución.

9.2.7. Informe de Auditoría

Una vez realizada la Auditoría, se emitirá un informe por parte del Auditor, el cual especificará los siguientes datos:

- Objeto y fecha de la Auditoría.
- Alcance.
- Auditores.
- Interlocutores de ICEX.
- Documentación de referencia.
- Deficiencias detectadas.
- Medidas correctoras propuestas.
- Los datos, hechos y observaciones en los que se basen los dictámenes alcanzados y recomendaciones adicionales.
- Firma del auditor.

El Auditor, firmará el informe emitido y lo remitirá a la Dirección de la Entidad, así como al Responsable de Seguridad de cada Departamento, el cual procederá a distribuirlo entre las áreas implicadas de la Entidad para su revisión y análisis, archivando el original del mismo para realizar el seguimiento de las incidencias derivadas. Los Responsables de Seguridad de cada Departamento comunicarán el resultado de la auditoría al personal a su cargo (si les aplica), con el objeto de identificar acciones correctivas para subsanar las desviaciones detectadas en el caso de que las mismas no se hayan establecido en la reunión final de la auditoría. Estas acciones

correctivas deberán presentarse al Comité de Seguridad para su validación. Una vez validadas se adjuntarán al informe de auditoría previa.

El Comité de Seguridad conservará debidamente localizado y controlado el informe de auditoría durante, al menos, tres (3) años.

A través del al presente Documento de Seguridad, se dejará constancia de las auditorías LOPD que se hayan realizado en el Anexo XVIII: Control de auditorías.

10. ANEXOS

ANEXO I: Inventario de Ficheros

ANEXO II: Inventario de Equipos.

ANEXO III: Inventario de Software.

ANEXO IV: Inventario de Soportes.

ANEXO V: Circular Personal LOPD.

ANEXO VI: Política de seguridad para usuarios.

ANEXO VII: Centros de tratamiento y locales.

ANEXO VIII: Relación del personal autorizado.

ANEXO IX: Identificación de Responsables.

ANEXO X: Nombramiento Responsable de Seguridad.

ANEXO XI: Copias de Seguridad.

ANEXO XII: Gestión de incidencias.

ANEXO XIII: Ficheros con acceso de terceros.

ANEXO XIV.: Modelo de solicitud del derecho de Acceso.

ANEXO XV.: Modelo de solicitud del derecho de Rectificación.

ANEXO XVI.: Modelo de solicitud del derecho de Cancelación.

ANEXO XVII.: Modelo de solicitud del derecho de Oposición.

ANEXO XVIII: Control de auditorías.

10.1. ANEXO I: Inventario de Ficheros

El contenido de los ficheros y la confirmación de su inscripción en el Registro General de Protección de Datos, se conservará indefinidamente en la Dirección Adjunta de Asesoría Jurídica y Ayudas.

FICHERO	CÓDIGO DE INSCRIPCIÓN	NIVEL DE SEGURIDAD	UBICACIÓN
APRENDIENDO A EXPORTAR	2063330104	BÁSICO	RGLP (AEPD)
ASESORIA JURÍDICA	2100481162	BÁSICO	RGLP (AEPD)
ASISTENTES A CONGRESOS Y FERIAS	2063320386	BÁSICO	RGLP (AEPD)
AUTORES	2100481259	MEDIO	RGLP (AEPD)
AYUDAS ICEX	2100481246	BÁSICO	RGLP (AEPD)
BASES DE DATOS CORPORATIVA	2063320383	BÁSICO	RGLP (AEPD)
BECARIOS ICEX	2050900475	MEDIO	RGLP (AEPD)
COMUNICACIÓN NOVEDADES EDITORIALES	1943292435	MEDIO	RGLP (AEPD)
CONFERENCIANTES AULA VIRTUAL ICEX	2050900437	BÁSICO	RGLP (AEPD)
CONSEJO DE ADMINISTRACIÓN ICEX	2063320387	BÁSICO	RGLP (AEPD)
CONTROL DE ACCESOS	2050900309	BÁSICO	RGLP (AEPD)
CONTROL DE PRESENCIA	2130450104	BÁSICO	RGLP (AEPD)
FERIAS	2063320385	BÁSICO	RGLP (AEPD)
GESTIÓN DE PERSONAL Y NÓMINAS	1943292421	ALTO	RGLP (AEPD)
GESTOR DE CONSULTAS	2063320384	BÁSICO	RGLP (AEPD)
OPORTUNIDADES DE NEGOCIO	1943292433	BÁSICO	RGLP (AEPD)
PIPE	2063330112	MEDIO	RGLP (AEPD)
SAP R/3 ACREEDORES	2063330066	BÁSICO	RGLP (AEPD)
SAP R/3 DEUDORES	2063320390	BÁSICO	RGLP (AEPD)

FICHERO	CÓDIGO DE INSCRIP-CIÓN	NIVEL DE SEGURIDAD	UBICACIÓN
SUSCRIPTORES DE REVISTAS DEL ICEX	1943292434	BÁSICO	RGLP (AEPD)
USUARIOS WEB	2100481176	BÁSICO	RGLP (AEPD)
VIDEOVIGILANCIA	2100481183	BÁSICO	RGLP (AEPD)
ICEX-CECO ANTIGUOS ALUMNOS	2043560033	BÁSICO	RGLP (AEPD)
CEX-CECO CURRICULAS	2043560031	BÁSICO	RGLP (AEPD)
ICEX-CECO HISTORICO CALIFICACIONES	2043560032	BÁSICO	RGLP (AEPD)
ICEX-CECO PROFESORES Y COLABORADORES	2043560029	BÁSICO	RGLP (AEPD)
ICEX-CECO PROVEEDORES	2043560034	BÁSICO	RGLP (AEPD)
ICEX-CECO SOLICITANTES DE INFORMACION	2043560036	BÁSICO	RGLP (AEPD)
ICEX CECO ALUMNOS	2043560030	MEDIO	RGLP (AEPD)
ICEX CECO BOLSA DE TRABAJO	2043560035	MEDIO	RGLP (AEPD)
EXPERTOS EXTERNOS (EEE)	2100050274	BÁSICO	RGLP (AEPD)
RELACIONES PÚBLICAS (EEE)	2100050276	BÁSICO	RGLP (AEPD)
CLIENTES Y PROVEEDORES MEDIO PROPIO (EEE)	2100050335	BÁSICO	RGLP (AEPD)
GESTIÓN RECURSOS HUMANOS (EEE)	2100050338	BÁSICO	RGLP (AEPD)
LICITADORES (EEE)	2111851290	BÁSICO	RGLP (AEPD)
CANDIDATOS (EEE)	2111661646	BÁSICO	RGLP (AEPD)
CLIENTES Y PROVEEDORES APOYO EMPRESA (EEE)	2131370283	BÁSICO	RGLP (AEPD)

10.2. ANEXO II: Inventario de Equipos

- **Servicios y Centros de Proceso de Datos**

El ANEXO III contiene la relación de dichos servidores y CPD's. Su actualización es responsabilidad del Departamento de Tecnologías de la Información.

Nº DE ORDEN	TIPO DE HARDWARE	FABRI-CANTE	MODELO	SISTEMA OPERATIVO	USO	FECHA
0001	Servidor					
0002	CPD	...	...	...	...	...
...	...					

- **Equipos Informáticos**

El ANEXO III contiene la relación de equipos informáticos u ordenadores personales destinados al tratamiento de datos personales. Su actualización es responsabilidad del Departamento de Informática.

Nº DE ORDEN	TIPO DE HARD-	FABRICANTE	MODELO	SISTEMA OPE-RATIVO	USO	FECHA
0001	PC					
0002	Portátil	...	...	...	...	...
...	...					
	...					
	...					
	...					
	...					
	...					
	...					
	...					
	...					
	...					
	...					

10.3. ANEXO III: Inventario de Software

- **Aplicaciones Informáticas**

El ANEXO III contiene la relación de aplicaciones informáticas que se emplean para el tratamiento de datos personales. Su actualización es responsabilidad del Departamento de Tecnologías de la Información.

Nº DE ORDEN	APLICACIÓN	FABRICANTE	VERSIÓN	CLIENTE/REMOTA	USO	FECHA
0001						
0002	...	...	...	...	...	...
...						

10.4. ANEXO IV: Inventario de Soportes

- **Armarios y Dispositivos de Almacenamiento de Datos en Soporte Papel.**

El ANEXO IV contiene la relación de armarios y dispositivos de almacenamiento. Su actualización es responsabilidad del Departamento de Servicios Generales de ICEX.

ALTAS						BAJAS		
Nº DE ORDEN	**TIPO DE SOPORTE**	**DESCRIP-CIÓN**	**FECHA COPIA**	**CONTENIDO**	**FICHERO**	**FECHA**	**REUTILIZA-CIÓN**	**DESTRUCCIÓN**
0001								
0002	...	...	...	...	...	...	...	
0003								
...								

- **Soportes y Dispositivos de Almacenamiento Digital que contienen datos de carácter personal**

Cada departamento llevará un inventario de estos dispositivos y será responsabilidad de los mismo la actualización del ANEXO IV en este apartado.

ALTAS						BAJAS		
Nº DE ORDEN	**TIPO DE SOPORTE**	**DESCRIP-CIÓN**	**FECHA COPIA**	**CONTENIDO**	**FICHERO**	**FECHA**	**REUTILIZA-CIÓN**	**DESTRUCCIÓN**
0001								
0002	...	...	...	...	...	...	...	
0003								
...								

- **Gestión de Soportes**

Cada departamento llevará el control de entrada y salida de soportes y será responsabilidad de los mismo la actualización del ANEXO IV en este apartado.

REGISTRO DE ENTRADA **DATOS DEL SOPORTE**					
Nº del Soporte:		Tipo del Soporte:			
Descripción:					
Fecha de copia:					
Contenido:					
Fichero:					
DATOS DE ENTRADA					
Responsable de Recepción:					
Fecha y Hora:		Periodicidad:		Nº de Soportes:	
Información que contienen:					
Forma de envío:					
DATOS DEL EMISOR					
Empresa:		Persona:			
Motivo:					
AUTORIZACIÓN					
Entrada autorizada por:					
Observaciones:					

REGISTRO DE ENTRADA DATOS DEL SOPORTE			
Nº del Soporte:		Tipo del Soporte:	
Descripción:			
Fecha de copia:			
Contenido:			
Fichero:			
DATOS DE ENTRADA			
Responsable de Recepción:			
Fecha y Hora:		Periodicidad:	Nº de Soportes:
Información que contienen:			
Forma de envío:			
DATOS DEL EMISOR			
Empresa:		Persona:	
Motivo:			
AUTORIZACIÓN			
Entrada autorizada por:			
Observaciones:			

10.5. ANEXO V: Circular personal LOPD

Madrid, a de de _____

CIRCULAR INTERNA

ASUNTO: Adaptación de formularios de recogida de datos a la normativa de protección de datos de carácter personal.

En cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), y en el Real Decreto 1720/ 2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en lo sucesivo, RLOPD), se indican una serie de medidas a adoptar en relación a los formularios de recogida de datos de carácter personal con el fin de adaptar cualquier recogida de datos por parte de ICEX a la normativa vigente en la materia.

Dichas medidas se traducen en la introducción de las siguientes cláusulas de información y consentimiento en todos los formularios a través de los cuales se recaben datos de carácter personal. De esta manera:

1.Deber de información.

Siempre que se tomen datos de un interesado, éste debe ser informado de lo establecido en el artículo 5 de la LOPD a través de una cláusula informativa. De ésta manera todos los formularios que recojan datos de carácter personal, ya sea de forma telemática o presencial, deben incluir una de éstas cláusulas, según el tipo de formulario de recogida.

- Cláusula informativa simple:

" Los datos de carácter personal que nos facilite mediante éste formulario quedarán registrados en un fichero de ICEX España Exportación e Inversiones, con la finalidad de [indicar la finalidad del fichero]. Por ello puede ejercitar los derechos de acceso, rectificación, cancelación y oposición ante ICEX España Exportación e Inversiones, Pº de la Castellana 278,28046 Madrid (España)."

NOTA: Dato de carácter personal es, según lo define la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), "cualquier información concerniente a personas físicas identificadas o identificables."

- Cláusula informativa para formularios que incluyan cuestionarios:

"En cumplimiento de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), ICEX España Exportación e Inversiones, Pº de la Castellana 278,28046 Madrid (España), le informa que los datos de carácter personal que nos proporcione a través del formulario de registro que aparece en ésta página se recogerán en ficheros cuyo responsable es ICEX España Exportación e Inversiones, con la finalidad de [indicar la finalidad del fichero].

Según lo establecido el artículo 15 y siguientes de la LOPD y en los términos que indica su Reglamento de Desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre, en cualquier momento el titular de los datos personales puede ejercer sus derechos de acceso, rectificación, cancelación y oposición, dirigiéndose por escrito a ICEX España Exportación e Inversiones, Pº de la Castellana 278,28046 Madrid (España).

El hecho de que no introduzca los datos de carácter personal que aparecen en el formulario de inscripción como obligatorios podrá tener como consecuencia que ICEX España Exportación e Inversiones no pueda atender su solicitud.

Usted reconoce que la información y los datos personales recogidos son exactos y veraces. Por tal razón le rogamos que comunique inmediatamente cualquier modificación ce sus datos para que la información que contienen nuestros ficheros esté siempre actualizada y no contenga errores."

NOTA: Dato de carácter personal es, según lo define la LOPD, "cualquier información concerniente a personas físicas identificadas o identificables."

2. Deber de consentimiento para envío de comunicaciones comerciales.

Una vez el interesado ha sido informado de que sus datos van a ser incorporados a un fichero, previamente registrado en la AEPD, para unos fines determinados, el tratamiento estará legitimado, pero únicamente para esa finalidad para la que se ha informado que se recogían. Para el supuesto en el que se quisiese que esos datos pudieran ser usados para el envío de comunicaciones comerciales, se está en el supuesto de un nuevo tratamiento, para el cual se necesita consentimiento del interesado de los datos.

El artículo 14 del RLOPD es el que establece la forma que la normativa determina para recabar dicho consentimiento, recogiendo que "el responsable podrá dirigirse al afectado, informándole en los términos previstos en el artículo 5 de la LOPD, y 12.2 del RLOPD y deberá concederle un plazo de treinta (30) días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal". Ésta será la regulación general para los envíos comerciales, a menos que se realicen de forma electrónica, ya que éstos poseen una normativa específica (Ley 34/20002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico) que les exige que el destinatario de la comunicación comercial consienta previamente de forma expresa.
De esta manera:

- *Cláusula para la obtención del consentimiento para el* ***envío de comunicaciones comerciales postales*** *en el mismo momento de la recogida de los datos:*

*"Sus datos personales serán incorporados al fichero "[indicar el nombre del fichero]", del que es responsable ICEX España Exportación e Inversiones y se utilizarán para [indicar la finalidad del fichero]. Asimismo, si Ud. no indica lo contrario en el plazo de treinta (30) días, presta su consentimiento para que sus datos personales se incorporen al fichero "Publicidad" de ICEX España Exportación e Inversiones para el envío de información y publicidad sobre las actividades de ésta. Puede ejercer los de*rechos de acceso, rectificación, cancelación y oposición ante ICEX España Exportación e Inversiones, Pº de la Castellana 278, 28046 Madrid (España)"

- *Cláusula para la obtención del consentimiento para el* ***envío de comunicaciones comerciales postales*** *para el caso de que en el momento de la recogida de datos no se contemplara:*

"Le informamos que sus datos de carácter personal que nos facilitó se encuentran registrados en el fichero "clientes" de ICEX España Exportación e Inversiones cuya finalidad es [indicar la finalidad del fichero]. Por ello, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición ante ICEX España Exportación e Inversiones, Pº de la Castellana 278,28046 Madrid (España). Asimismo, se le informa que sus datos van se incorporarán al fichero "Publicidad" de ICEX España Exportación e Inversiones para el envío de información y publicidad sobre las actividades de ésta. Si desea manifestar su negativa a este tratamiento tiene un plazo de treinta días para comunicárnoslo respondiendo a este email incluyendo en el Asunto la palabra "Baja", advirtiéndole de que en caso de no pronunciarse, se entenderá que consiente este tratamiento."

- *Cláusula para* la obtención del consentimiento para el **envío de comunicaciones comerciales realizadas por medios electrónicos:**

"Sus datos personales serán incorporados al fichero "[nombre del fichero]", del que es responsable ICEX España Exportación e Inversiones, y se utilizarán para [indicar la finalidad]. Asimismo, si Ud. consiente en ello sus datos personales se utilizarán para [indicar la finalidad publicitaria].

Puede ejercer los derechos de acceso, rectificación, cancelación y oposición en cualquier momento mediante escrito, acompañado de copia de documento oficial que le identifique, dirigido a ICEX España Exportación e Inversiones, Pº de la Castellana 278,28046 Madrid (España).

□ Deseo recibir información sobre [indicar la finalidad publicitaria, por ejemplo, recibir información sobre las actividades de ICEX España Exportación e Inversiones]."

Se cita como única excepción a la citada obligatoriedad de consentimiento previo y expreso de las comunicaciones comerciales electrónicas, el supuesto de no necesidad de cumplimiento de éstos requisitos cuando se haya mantenido una relación contractual previa con el mismo empresario y siempre que se trate de productos o servicios similares a los que inicialmente fueron objeto del contrato del que deriva dicha relación previa. De cualquier modo, también en éste supuesto es de obligatorio cumplimiento el facilitar al destinatario la posibilidad de oponerse al envío de publicidad incluyendo una dirección de correo electrónico en cada una de las comunicaciones comerciales que se realicen.

Reciban un cordial saludo.

10.6. ANEXO VI: Política de seguridad para usuarios.

OBJETIVO

En la Sociedad actual en la que nos encontramos, la información se ha convertido en uno de los activos más importante de las empresas y en el verdadero motor de sus procesos de negocio.

Paradójicamente, el uso universalizado de las nuevas tecnologías hace más vulnerables los métodos de manejo y custodia de información, sobre todo contra las agresiones procedentes del entorno.

En consecuencia, es imprescindible desarrollar una serie de medidas técnicas y organizativas, con el objeto de prevenir distintas amenazas externas o internas, que pudieran poner en peligro su disponibilidad, integridad y confidencialidad con el fin de minimizar al máximo los posibles pérdidas, daños y responsabilidades resultantes de la materialización de dichas amenazas.

Con el presente documento se persigue la salvaguarda de la confidencialidad de la información, el mantenimiento de la integridad de la misma, así como garantizar su disponibilidad en el momento en que cualquier usuario lo requiera.

En ICEX, la seguridad de la información es vital. Por ello, los recursos y herramientas de trabajo de ICEX deben ser protegidos en todo momento, para lo que es imprescindible la concienciación de las personas que traten estos activos al objeto de que procuren su protección de forma responsable.

En consecuencia, ponemos en su conocimiento que en ICEX se han llevado a cabo actuaciones con la finalidad de revisar nuestros procesos en materia de seguridad de la información.

A tal efecto se ha ejecutado el proyecto de adecuación a la normativa en materia de protección de datos de carácter personal de esta Entidad y es por ellos que se ha establecido la presente política de obligado cumplimiento para todo el personal que utilice los recursos o dispositivos de la Entidad que se exponen a continuación.

En cumplimiento de la normativa de protección de datos se hace necesaria la colaboración de todas las personas que trabajan y colaboran con ICEX y por tanto, te rogamos leas con atención e interés esta circular informativa.

CONTENIDO

Uso responsable de equipos informáticos propiedad de ICEX

ICEX dispone de equipos informáticos para que los empleados puedan desarrollar su actividad, facilitando el trabajo dentro y fuera de las instalaciones de la Entidad.

La asignación de estos recursos deberá ser debidamente controlada por la Dirección de Tecnología de la Información, para la efectiva gestión y notificación de las incidencias.

El usuario dispondrá en estos equipos de una cuenta y una contraseña de usuario, sin que esté permitida en ningún caso la instalación de aplicaciones por parte de los usuarios.

Todos los equipos dispondrán de las herramientas mínimas necesarias para el desempeño de las funciones del usuario. En concreto, y de cara a una posible verificación de los programas instalados, el usuario dispondrá de:

- Sistema Operativo
- Suite ofimática
- Navegadores de Internet
- Servicios de impresión

- Lector para ficheros en formato pdf
- Agente de antivirus y antimalware
- Firewall corporativo

El usuario no deberá vulnerar de ninguna forma los permisos de su cuenta, especialmente para instalar aplicaciones no relacionadas con el trabajo. En el caso de que el trabajador precise la instalación de una aplicación específica para llevar a cabo su labor, deberá solicitarlo a su responsable directo, quien, en caso de no disponer de potestad para autorizar la instalación de aplicaciones, escalará la petición hasta que alcance al Responsable de Seguridad por Departamento, que lo notificará a la Dirección de Tecnologías de la Información a través del procedimiento de notificación de incidencias.

Queda prohibida cualquier alteración del arranque o de su secuencia habitual para acceder a una cuenta sin disponer de contraseña.

El trabajador deberá velar por la seguridad y confidencialidad de la información contenida en los equipos, sobre todo cuando se encuentre fuera de las dependencias de ICEX. ICEX podrá imponer el cifrado de los datos personales que sean responsabilidad de ICEX y que sean almacenados en equipos portátiles deberán estar cifrados y el trabajador deberá gestionar dicha información utilizando los mecanismos que ICEX determine, sobre los que le informará y formará adecuadamente.

Sólo se podrán utilizar los soportes externos autorizados por ICEX, debiendo cumplir en todo caso las mismas normas que aplican a la información almacenada en equipos portátiles.

En caso de tener que viajar con el equipo, nunca se facturará con el equipaje. La pérdida del dispositivo informático portátil debe ser notificada inmediatamente a la Dirección de Tecnologías de la Información, con la denuncia correspondiente quien procederá a registrar la incidencia de acuerdo con el procedimiento establecido en el presente Documento de Seguridad.

Cuando el trabajador no haya obrado con la debida diligencia en la salvaguarda del dispositivo informático portátil, o incumpla repetidas veces las políticas aquí establecidas, podrá estar sujeto a acciones disciplinarias o compensatorias. A modo de ejemplo, será responsabilidad del usuario:

- Los desperfectos ocasionados como consecuencia de su traslado en dispositivos no adecuados (bolsas, maletas, etc.).
- Los desperfectos ocasionados como consecuencia de un uso inadecuado.
- La pérdida por olvido en lugares públicos.

Para verificar el cumplimiento de estas obligaciones, así como el correcto funcionamiento del equipo y el buen uso del mismo, podrán realizarse auditorías periódicas de los equipos de los usuarios con el objeto de examinar los siguientes aspectos:

- Aplicaciones instaladas y registro del sistema operativo.
- Información y archivos contenidos en el disco duro del equipo.
- Estado del antivirus.

Estas revisiones podrán ser aleatorias entre el personal de ICEX y efectuadas según su criterio cuantas veces la Entidad estime oportuno. Iguales consideraciones se aplican respecto de los equipos de sobremesa.
Una vez examinado el equipo del usuario, el contenido no autorizado será eliminado, así como el usuario informado de sus obligaciones respecto del equipo, y de las consecuencias del no respeto de estas directrices.
Los equipos serán entregados al usuario en perfecto estado y funcionamiento. Si el usuario detectase algún desperfecto, mal funcionamiento o contenido indebido al recibir el equipo, deberá ponerlo inmediatamente en

conocimiento de su responsable directo con el fin de que se pueda solucionar el incidente y que el usuario pueda exonerarse de toda responsabilidad.

Uso responsable de Internet

Los usuarios son los únicos responsables de las sesiones iniciadas en la red Internet desde sus terminales de trabajo. En ICEX, el uso de Internet tiene carácter laboral y no debe ser utilizado con fines personales, salvo circunstancias excepcionales, siempre que no afecte a la dedicación del empleado, ni a la capacidad de los sistemas de ICEX.

En ningún caso se pueden modificar las configuraciones de los navegadores del equipo ni la activación de servidores o puertos sin autorización de ICEX.
Está expresamente prohibido el uso de Internet con propósitos ilegales, inapropiados u obscenos. La definición del uso inapropiado es violar y/o cambiar el propósito y la finalidad del uso de Internet y de la redes de comunicación en el ámbito laboral. La definición de actividades obscenas es la violación de los estándares sociales que se han establecido para uso público.

En particular debe evitarse la utilización de imágenes (como los formatos GIF, JPG, BMP o TIFF entre otros), sonido (formatos WAV y MP3 principalmente) y vídeo (MPG, DivX, AVI, RAW o similares) para fines ajenos a la actividad laboral de la Entidad, debido a que el tamaño de estos archivos satura los canales de comunicación y disminuye la velocidad de transmisión perjudicando al funcionamiento de la red en su conjunto.

Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres; de los formatos de imágenes, sonidos o vídeo que a modo de ejemplo se enumeran en la norma anterior; de virus y códigos maliciosos y, en general, de todo tipo de programas y/o plug-in sin la expresa autorización de ICEX.

Asimismo, se prohíbe el uso de Internet o de la web mediante los recursos informáticos o de red de ICEX con fines recreativos, así como para obtener o distribuir material violento o pornográfico o con componente sexual, o para obtener o distribuir material incompatible con los valores de ICEX.

Los usuarios deberán identificarse y autenticarse individualmente antes de acceder a Internet.

ICEX se reserva el derecho a filtrar el contenido al que el usuario pueda acceder en Internet por medio del uso de sus recursos y servicios, así como a monitorizar y registrar los accesos realizados desde el equipo con el fin de comprobar el correcto uso laboral de Internet.

Descarga de material sujeto a derechos de autor

Por motivos de seguridad se recomienda que no se efectúe la descarga de software ejecutable desde Internet que no sea previamente aprobado por la Entidad. De igual modo, en ningún caso podrá descargarse software ni otros contenidos protegidos por derechos de autor con la finalidad de utilizarlo y/o distribuirlo posteriormente por los recursos informáticos y de red de ICEX sin la correspondiente licencia de uso y/o distribución de dicho material. Ante este tipo de necesidades, el usuario se dirigirá a su responsable directo con el fin de realizar la oportuna solicitud.

Los usuarios respetarán y darán cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet, haciendo uso de los recursos informáticos o de red de ICEX.

El listado siguiente no es de ninguna manera exhaustivo, pero procura proporcionar un marco para las actividades que son consideradas inaceptables:

- La violación de derechos de propiedad intelectual de cualquier persona física o jurídica, de derecho público o privado, incluyendo, pero no limitada a, la instalación o distribución de productos de software no licenciados apropiadamente para el uso por la Entidad.

- La violación de derechos de propiedad industrial de cualquier persona física o jurídica, de derecho público o privado, incluyendo, pero no limitada a, la utilización sin consentimiento de sus legítimos titulares de secretos comerciales, patentes, marcas, logos o rótulos.

Consideraciones de privacidad

Los usuarios respetarán en todo momento la privacidad de todos los individuos que utilizan Internet.
No buscarán, harán uso o se apoderarán de información personal, ni obtendrán copias del software, archivos, datos ni contraseñas pertenecientes a usuarios de Internet. No llevaran a cabo en ningún caso, la suplantación de forma voluntaria y consciente de otro usuario.

Los usuarios no modificarán ni eliminarán el software, los archivos, datos ni contraseñas de otros usuarios intencionadamente, salvo autorización expresa de dichos usuarios. Se requiere que los usuarios respeten la integridad de la información perteneciente a otros usuarios que hacen uso de Internet.

Se deberá obtener los permisos necesarios para obtener información personal u otros recursos de Internet que no sean de libre acceso al público. Se prohíben los intentos de acceder a la información privada u otros recursos de Internet sin haber obtenido la aprobación adecuada.

Uso responsable del correo electrónico corporativo

El correo electrónico es una herramienta valiosa para enviar y recibir mensajes, obtener y enviar información y hacer negocios. Sin embargo, cuando no se usa apropiadamente, puede ser también una fuente de problemas de seguridad y responsabilidad legal para ICEX.

El correo electrónico es una herramienta de productividad que ICEX pone a disposición de sus empleados, para el desarrollo de las funciones que les tiene encomendadas. Los usos ajenos a estos fines son, por tanto, considerados inapropiados y en el límite podrían configurar falta laboral.

El correo electrónico se empleará para aquellas comunicaciones requeridas como consecuencia del desarrollo de la actividad propia de ICEX con otras entidades o con otros usuarios. El acceso y uso de estos servicios por parte de los usuarios, así como los privilegios asociados a dicho acceso deben limitarse a los necesarios para realizar su actividad.

ICEX no permite el uso personal de este servicio, salvo de forma excepcional, siempre que no afecte al desempeño de sus funciones ni a los sistemas de ICEX. Los usuarios son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por ICEX. Asimismo, deben ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por ICEX. Los mensajes de correo transmiten información en sus cabeceras (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como daños a la imagen institucional) que podría acarrear una mala utilización de este recurso.

La violación de la seguridad de los sistemas puede generar responsabilidades civiles y/o criminales. ICEX colaborará al máximo de sus posibilidades en cualquier eventual investigación contra este tipo de actos o cualquier otra utilización ilegal, incluyendo la cooperación con la Justicia.

El sistema informático de ICEX se encuentra protegido contra virus informáticos por un antivirus. La responsabilidad sobre la comunicación a los responsables del sistema de cualquier anomalía suscitada en este sentido depende de cada usuario, así como la apertura de un correo sobre el que se tengan dudas o la emisión de un mensaje de virus por parte del antivirus.

No es correcto enviar correos electrónicos a personas que no desean recibirlo. En caso de reunir determinadas características, estos envíos podrían llegar a concebirse como spam, lo que configura una conducta prohibida por la legislación vigente en nuestro país. Si ICEX llegara a recibir reclamaciones por estas prácticas se tomarán las medidas sancionadoras pertinentes.

Cuando se establezca la necesidad de cifrar o firmar electrónicamente los correos electrónicos intercambiados con un cliente, proveedor u otra tercera parte, el Responsable de Seguridad por Departamento interesado consultará con el Comité de Seguridad los mecanismos dispuestos por ICEX para este tipo de operaciones.

Está completamente prohibido realizar cualquiera de las siguientes actividades:

- Utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno a las actividades laborales autorizadas por la Entidad.
- Utilizar en los equipos informáticos provistos por ICEX buzones de correo electrónico de otros proveedores Internet. Especialmente se prohíbe la utilización como encaminador de correo de otras máquinas que no sean las puestas a disposición por la Entidad, el envío de mensajes con direcciones no asignadas por los responsables de la Entidad y la manipulación de las cabeceras de correo electrónico saliente.
- Participar en la propagación de cartas encadenadas, esquemas piramidales o similares.
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la Entidad.
- Falsificar las cabeceras del correo electrónico o del remitente.
- Recoger correo de buzones de otro proveedor de Internet.
- Difundir mensajes de acoso, denigratorios, discriminatorios u ofensivos de cualquier modo.
- Difundir mensajes de humor, comentarios o imágenes que contengan insultos étnicos, epítetos raciales o cualquier otra comunicación que pudiera ofender, denigrar o avergonzar a otros debido a su raza, origen nacional, sexo, orientación sexual, edad, discapacidad, religión, creencias políticas u otras razones a las que el destinatario pueda ser sensible.
- Enviar correos desde cuentas ajenas sin consentimiento de su titular.
- Permitir la utilización de la cuenta y/o el correspondiente buzón a personas no autorizadas.
- Efectuar ataques con objeto de imposibilitar u obstruir sistemas informáticos (ataques de denegación de servicio), dirigido a un usuario o al propio sistema de correo, así como el envío de un número alto de mensajes por segundo (mail bombing), o cualquier variante, que tenga por objeto la paralización del servicio por saturación de las líneas, de la capacidad de CPU del servidor, del espacio en disco de servidores o terminales o cualquier otra práctica similar.
- Enviar mensajes que comprometan la reputación de ICEX a foros de discusión, listas de distribución y/o newsgroups.
- Queda prohibido el reenvío automático de mensajes (autoforwarding) de correo electrónico a direcciones que no sean de ICEX, estén vinculadas a ella o ésta haya autorizado expresamente su reenvío.
- Divulgación no autorizada de secretos comerciales de ICEX.
- Enviar información confidencial, privada o propiedad de ICEX o información sobre los clientes y/o proveedores.
- Enviar materiales externos con derechos de propiedad intelectual, de marca comercial registrada o patentados, incluyendo artículos o software, que no sean propiedad de ICEX o que no hayan sido autorizados para ser enviados, reenviados, almacenados o impresos por el propietario de los mismos.
- Mensajes relacionados con la operación de un negocio personal o actividades de negocios realizadas no relacionadas con el negocio de ICEX.
- Usar el sistema de forma que cause congestión de la red o rupturas de seguridad, tales como:
    - Descarga de archivos de tamaño excesivo.
    - Permitirle a personal no autorizado que use el sistema.
    - Suscribirse a servidores de listas o listas de correo electrónico para negocios no relacionados con ICEX.
    - La descarga de programas de mensajería instantánea, tipo Messenger, no autorizados expresamente por ICEX.
    -

Cuando se emitan mensajes de difusión a varios destinatarios, sin que exista la necesidad de que cada uno de los destinatarios conozca la identidad del resto, o sin que se espere una respuesta de uno de los destinatarios que deba ser conocida por el resto, deberán consignarse todos los destinatarios en el campo “Con Copia Oculta” (CCO) o, en inglés, “Blind Carbon Copy” (BCC).

Todas las comunicaciones enviadas, recibidas o almacenadas mediante la mensajería electrónica de ICEX se consideran propiedad de esta.

Al objeto de garantizar el cumplimiento de la presente política, ICEX podrá supervisar las comunicaciones y archivos remitidos por los usuarios por medio de los recursos y sistemas de la Entidad en el caso de que existan sospechas fundadas de que se está haciendo un uso indebido de los recursos de ICEX incumpliéndose los aspectos descritos en esta política. La supervisión o el acceso respetarán en todo momento los derechos de privacidad de los usuarios, incluyendo el cumplimiento de la legislación vigente.

La violación continuada de esta política o abuso del sistema podrá repercutir en la terminación de privilegios de correo electrónico y pueden ser referidos al responsable correspondiente, para mayor acción, incluyendo, si es adecuado, la extinción del contrato de trabajo.

Uso de la firma electrónica

Debido al gran número de comunicaciones con clientes vía e-mail, y a la importancia de securizar el contenido y el entorno de dichas comunicaciones, cada usuario de ICEX dispondrá, llegado el caso, de un certificado digital de firma electrónica ya configurado para su cuenta de correo, que deberá ser empleado en todas las comunicaciones electrónicas remitidas. El hecho de firmar un correo proporcionará las siguientes funcionalidades:

- Autenticidad, el o los destinatarios, no podrán dudar de la identidad del remitente del correo.
- No repudio, el remitente no podrá negar que ha mandado el correo.
- Integridad, el destinatario puede estar seguro de que el mensaje no ha sido modificado respecto al que envío el remitente.

Uso responsable del teléfono fijo, móvil y fax de ICEX

ICEX proporciona acceso y uso de las comunicaciones telefónicas y de fax para aumentar la productividad y mejorar el desarrollo de las actividades propias de la Entidad. El uso fraudulento del fax o del teléfono, fijo o móvil, puede poner en peligro la integridad de la Entidad y lesionar sus intereses. Esto puede acontecer mediante la realización de actividades consideradas ilícitas que atenten contra la moral o puedan resultar ofensivas o mediante el uso abusivo del mismo.

El uso personal de las comunicaciones telefónicas o por fax estará permitido si es fortuito o insignificante y no interfiere con las actividades laborales habituales. Cualquier uso personal:

- No debe conllevar coste alguno a la Entidad.
- No debe estar asociado a una entidad política.
- No debe promover la actividad de otra entidad.
- No debe potencialmente dañar la reputación y el nombre de ICEX.

Queda prohibido el uso del fax y de las comunicaciones telefónicas de ICEX cuando se haga un uso de ellas destinado a los aspectos especificados a continuación:

- Beneficio personal.
- Negocios personales.
- Actividades políticas personales.
- Comportamiento antisocial o inmoral.
- Actividades que violen la legislación local, autonómica, nacional o internacional.
- Actividades recreativas.
- Divulgación no autorizada de información confidencial de ICEX.
- Actividades incompatibles con los valores propios de la Entidad.

El acceso de los usuarios y los privilegios asociados a dicho acceso deben limitarse a los necesarios para llevar a cabo las labores correspondientes a sus tareas propias.

Queda prohibido y no se tolerará el uso del fax ni de las comunicaciones telefónicas de ICEX para transmitir o distribuir material inapropiado u ofensivo, o como ofensas por motivo de raza religión, o género.

Los usuarios del fax y de las comunicaciones telefónicas de ICEX no deberán hacerse pasar por otro usuario o entidad en el transcurso de cualquier comunicación.

ICEX se reserva el derecho de revisar la lista de llamadas realizadas y faxes enviados, para la verificación del cumplimiento de las normas ante cualquier sospecha o evidencia de uso fraudulento o abusivo del mismo.

Con respecto al teléfono móvil, deberá estar protegido convenientemente con un número PIN, el cual el trabajador no debe hacer público, con el fin de no poner en peligro la confidencialidad de los datos contenidos en el mismo y seguirá las mismas consideraciones que las expresadas anteriormente.

La asignación de estos recursos deberá ser debidamente controlada por el Departamento de Recursos Humanos, a través del procedimiento establecido en el presente Documento de Seguridad para la notificación y gestión de las incidencias.

Uso responsable de la impresora, fotocopiadora y escáner

Los recursos de reprografía, impresión y digitalización son herramientas de trabajo puestas a disposición del trabajador por parte de ICEX.

Estas herramientas generan unos gastos que serán asumidos por ICEX siempre que el uso del trabajador responda a las necesidades reales del trabajo. Cuando la Entidad detecte un uso excesivo e inadecuado de estos recursos por parte del trabajador, tomará las medidas disciplinarias oportunas.

En cualquier caso, el trabajador debe concienciarse del compromiso que tiene ICEX con el medio ambiente, por lo que deberá asimilar y hacer propio dicho compromiso.

En todo caso, el trabajador se asegurará de que no queden documentos impresos en la bandeja de salida o retenidos en la cola de impresión que contengan datos confidenciales, así como de retirar los documentos conforme vayan siendo impresos. Este mismo compromiso se ejercerá respecto de faxes, scanners u otros dispositivos de análoga funcionalidad.

Mesas limpias

Es crucial proteger la información confidencial de que sea publicada. Las oficinas de ICEX son visitadas frecuentemente por proveedores, consultores, clientes, personal de limpieza y otros compañeros de trabajo.
ICEX considera una buena práctica que los empleados mantengan su escritorio lo más limpio y organizado posible.
Durante el día, los empleados de ICEX y terceros relacionados:

- Deben almacenar los documentos con contengan información personal y confidencial, en los cajones bajo llave, usándolos exclusivamente cuando sea necesario para la labor que desempeñan.
- Deben bloquear y/o apagar el ordenador cada vez que se alejen físicamente del mismo.

Al terminar la jornada laboral el empleado:

- Debe recopilar y asegurar material confidencial.
- Cerrar bajo llave cajones y oficinas.
- Asegurar que los equipos informáticos así como cualquier otro equipamiento que esté bajo su responsabilidad, están debidamente apagados.

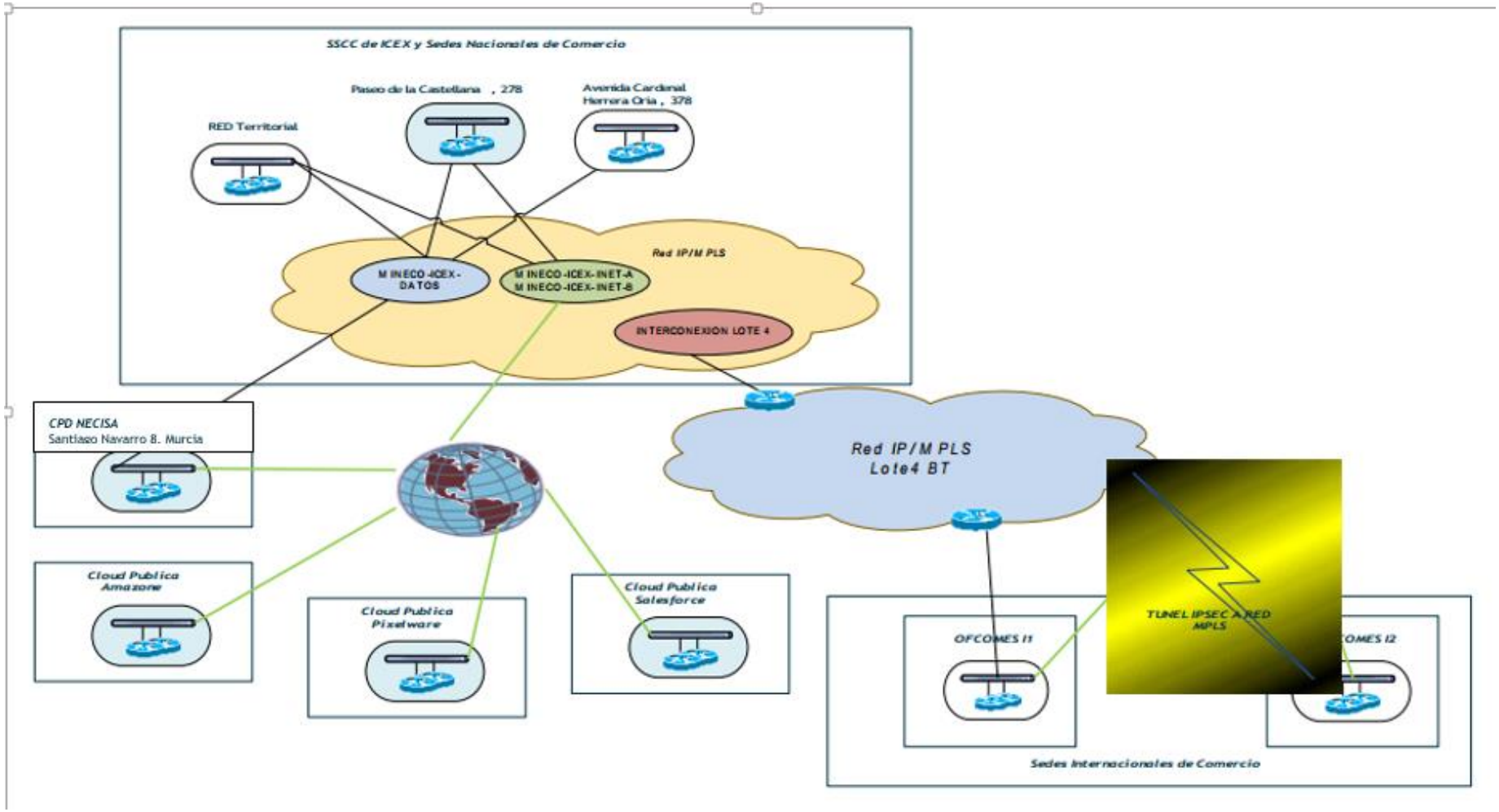
En ningún momento, se deberá publicar información confidencial de la Entidad ni de otros empleados, por ejemplo:

- Nombre de Usuario y Passwords
- Direcciones IP
- Contratos
- Números de Cuenta
- Listas de Clientes
- Propiedad Intelectual

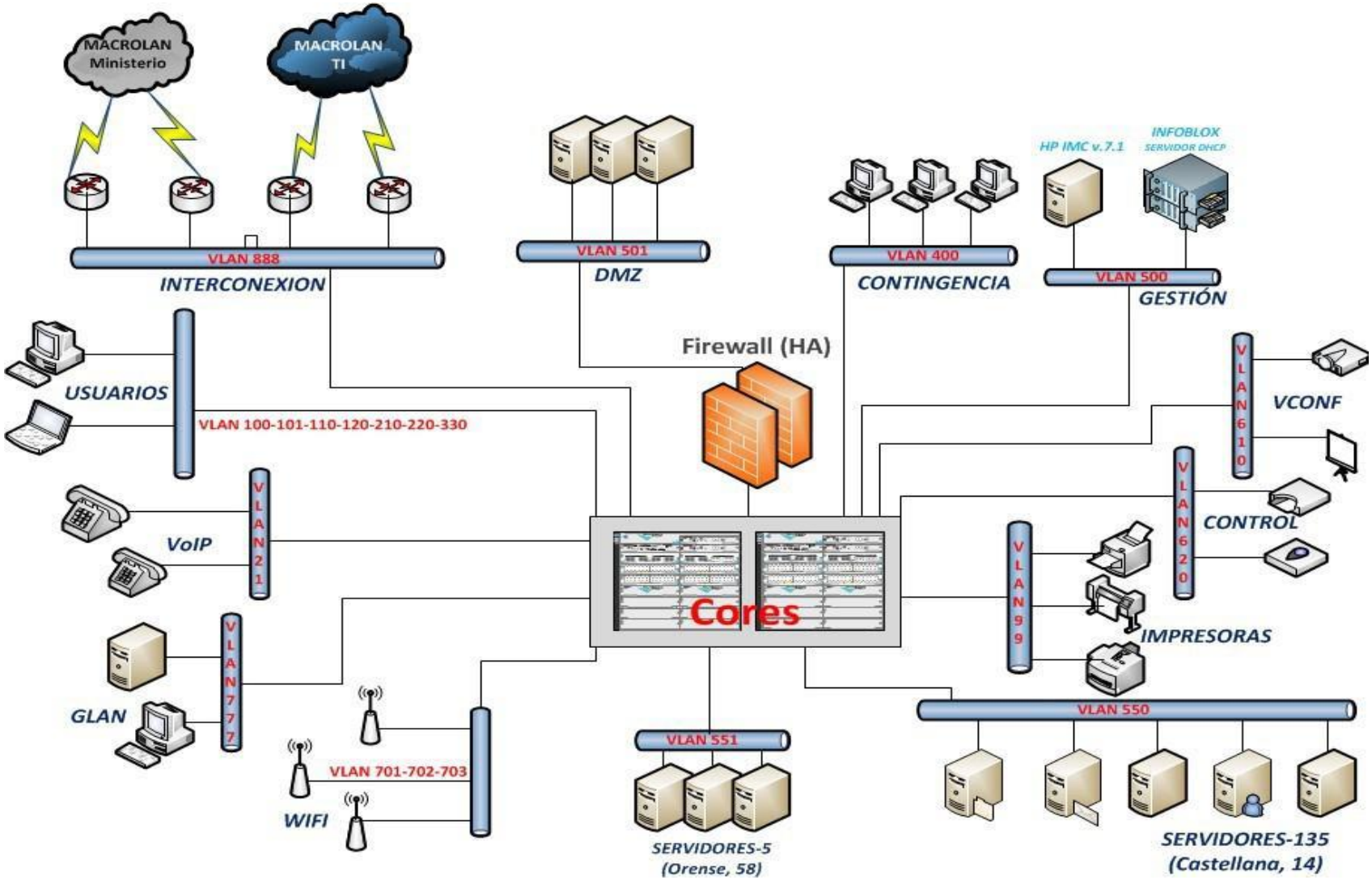
- Datos de Empleados
- …etc.

10.7. ANEXO VII: Centro de tratamiento y locales

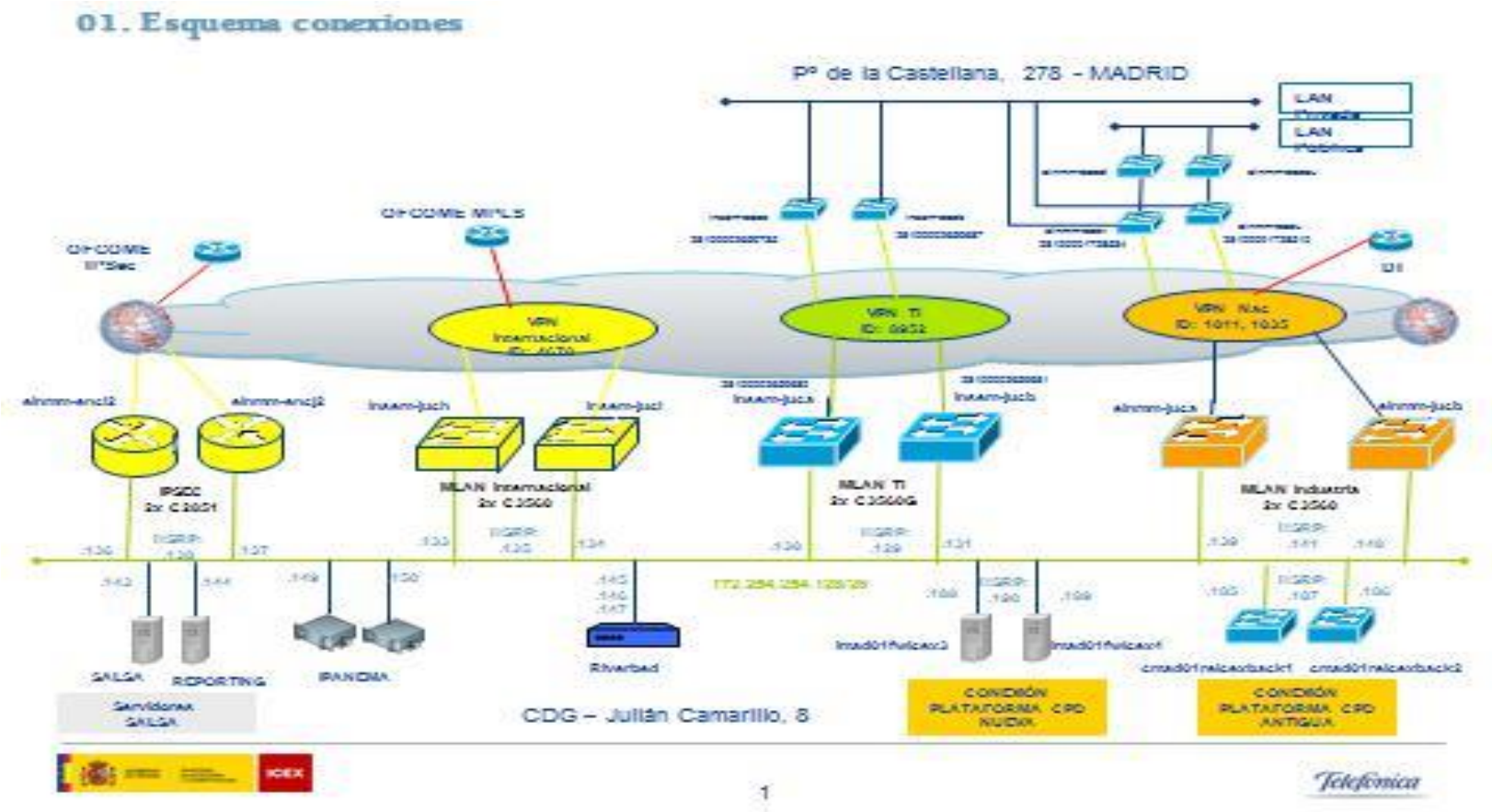
- **CPDs y elementos principales de comunicación**



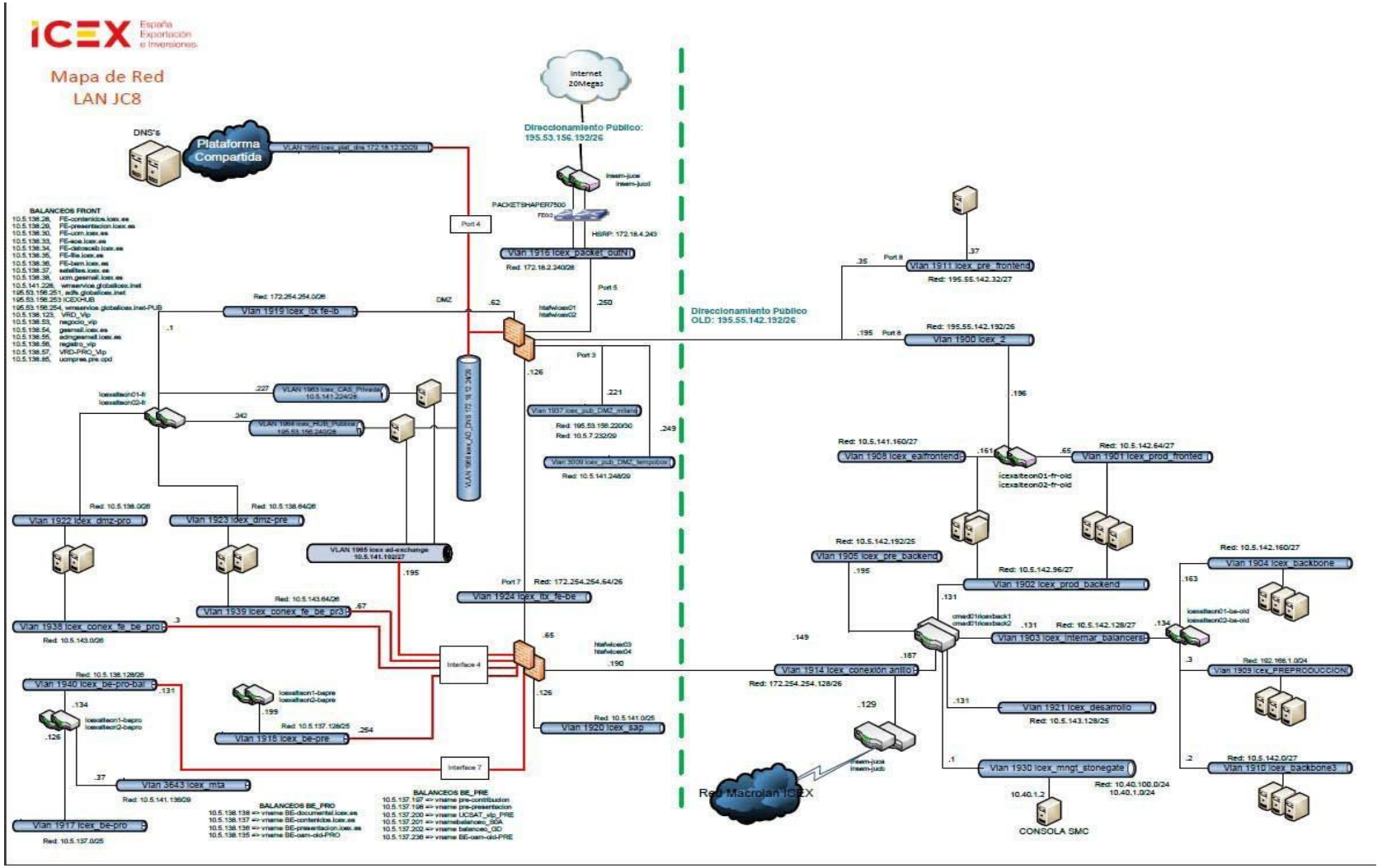
- **Estructura LAN de C278**



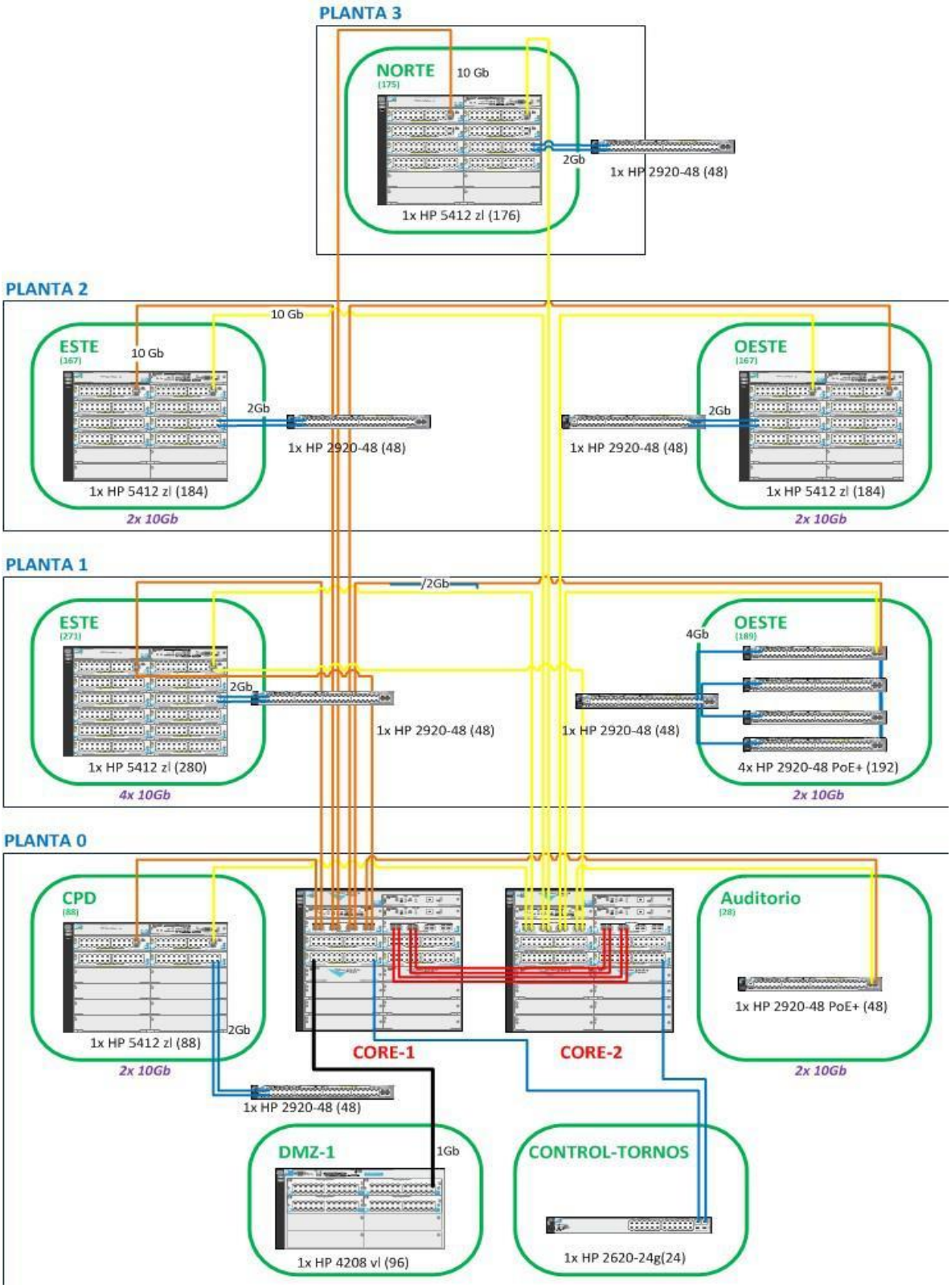
- **Esquema de Conexiones en C278**



- **Mapa de Red en Santiago Navarro, 8 (Murcia)**


Mapa de Red
LAN JC8
Internet
20Megas
Direccionamiento Publico:
195.53.156.192/25
DNS's
Plataforma
Compartida
PACKETSHAPER7500
HSRP: 172.18.4.243
Vlan 1916 Icex_packet_outN1
Red: 172.18.2.240/28
BALANCEOS FRONT
Red: 172.254.254.0/26
Vlan 1919 Icex_ltx fe-lb
DMZ
Direccionamiento Público
OLD: 195.55.142.192/26
Vlan 1911 Icex_pre_frontend
Red: 195.55.142.32/27
Red: 195.55.142.192/26
Vlan 1900 Icex_2
Vlan 1937 Icex_pub_DMZ_mitard
Red: 195.53.156.220/30
Red: 10.5.7.232/29
Vlan 3009 Icex_pub_DMZ_temporizar
Red: 10.5.141.248/29
Red: 10.5.141.160/27
Vlan 1908 Icex_ealfrontend
Red: 10.5.142.64/27
Vlan 1901 Icex_prod_fronted
icexalteon01-fr-old
icexalteon02-fr-old
Vlan 1922 Icex_dmz-pro
Red: 10.5.138.0/26
Vlan 1923 Icex_dmz-pre
Red: 10.5.138.64/26
VLAN 1995 Icex ad-exchange
10.5.141.192/27
Red: 10.5.142.192/25
Vlan 1905 Icex_pre_backend
Red: 10.5.142.96/27
Vlan 1902 Icex_prod_backend
Red: 10.5.142.160/27
Vlan 1904 Icex_backbone
Port 7
Red: 172.254.254.64/26
Vlan 1924 Icex_ltx_fe-be
Red: 10.5.143.64/26
Vlan 1939 Icex_conex_fe_be_pr3
Vlan 1938 Icex_conex_fe_be_pro
Red: 10.5.143.0/26
Interface 4
Vlan 1914 Icex_conexión anillo1
Red: 172.254.254.128/26
Vlan 1903 Icex_internar_balancers
Red: 10.5.142.128/27
Vlan 1909 Icex_PREPRODUCCION
Red: 192.168.1.0/24
Red: 10.5.138.128/26
Vlan 1940 Icex_be-pro-bal
Vlan 1918 Icex_be-pre
Red: 10.5.137.128/25
Vlan 1920 Icex_sap
Red: 10.5.141.0/25
Vlan 1921 Icex_desarrollo
Red: 10.5.143.128/25
Interface 7
Vlan 3643 Icex_mta
Red: 10.5.141.136/29
Vlan 1917 Icex_be-pro
Red: 10.5.137.0/25
Red Macrolan ICEX
Vlan 1930 Icex_mngt_stonegate
Red: 10.40.100.0/24
10.40.1.0/24
10.40.1.2
CONSOLA SMC
Vlan 1910 Icex_backbone3
Red: 10.5.142.0/27
BALANCEOS BE_PRO
BALANCEOS BE_PRE

- **Diseño físico LAN por plantas**



10.8. ANEXO VIII: Relación del personal autorizado

NOMBRE	NIF	CARGO	DEPAR TAMEN TO	ALTA	BAJA	CONTRAT O	E-MAIL	FICHERO	CARG O	PERMISOS	MODIFICACI ÓN	BORRADO	BLOQUEO

10.9. ANEXO IX: Identificación de Responsables

PERFIL	DEPARTAMENTO	NOMBRE Y APELLIDOS	FIRMA	FECHA
...	...	...	...	...

10.10. ANEXO X: Nombramiento Responsable de Seguridad

A: _____

De:_____

Fecha:__

Asunto: Nombramiento Responsable Seguridad

Con fecha ___ de ___ de ____, se constituye en ICEX España Exportación e Inversiones (ICEX) el Comité de Seguridad para el nombramiento de los Responsables de Seguridad por Departamentos, indicados a continuación:

- • D./Dña. xxx
- • D./Dña. xxx
- • D./Dña. xxx

Las funciones y responsabilidades de este puesto abarcan toda la seguridad de la información de ICEX, incluyendo seguridad informática, aspectos organizativos, y legislativos (tratamiento de datos personales). Ello incluye garantizar la seguridad de las instalaciones y de los datos en general y velar por el cumplimiento de los principios de la LOPD, estableciendo las medidas necesarias para su cumplimiento.
Del mismo modo acredita el conocimiento y cumplimiento de lo establecido en el Documento de Seguridad, así como de guardar secreto sobre los datos de carácter personal y cualesquiera otras informaciones o circunstancias que conociera o a las que haya tenido acceso en el ejercicio de las funciones que le hubiesen sido asignadas por ICEX.
Las anteriores obligaciones se extienden a cualquier fase del tratamiento de los citados datos y subsistirán aun después de concluidas las funciones en el marco de las cuales ha tenido acceso a los datos o concluida su relación laboral con la sociedad.

Firmado:

10.11. ANEXO XI: Copias de Seguridad.

INFORME DE RECUPERACIÓN DE DATOS

RECUPERADOR DE LOS DATOS	**Nombre y Apellidos:**	
SOLICITANTE DE LA RECUPERACIÓN	**Nombre y Apellidos:**	
BASE DE DATOS A RECUPERAR		
MÁQUINA DESDE LA QUE SE RECUPERAN LOS DATOS		
GRABACIÓN DE INCIDENCIAS NECESARIAS PARA LA RECUPERACIÓN		**GRABACIÓN DE DATOS MANUAL**

TIEMPO (en horas y minutos)	**INICIO (1)**	**FINALIZACIÓN (2)**	**TOTAL (2-1)**
INCIDENCIAS (T1)			
RECUPERACIÓN (T2)			
	TIEMPO TOTAL (T1+T2)		

VERIFICACIÓN DE LA RECUPERACIÓN	
OBSERVACIONES	

10.12. ANEXO XII: Gestión de Incidencias.

Tipo Incidencia	Descripción	Datos Restaurados	Datos restaurados a mano	Fecha Autorización	Firma / Autorización	Persona que atendió la incidencia.
0001						
0002	...	...	...	...	...	...
0003						
...						

10.13. ANEXO XIII: Ficheros con acceso de terceros.

TERCERO	FICHERO	FECHA DE ALTA	FECHA DE BAJA
0001			
0002	...	...	...
0003			
...			

10.14. ANEXO XIV: Modelo de solicitud del derecho de Acceso.

EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / Razón social: .....
Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso:
C/Plaza.....nº.....C.Postal.....
Localidad.....Provincia.....Comunidad Autónoma.....C.I.F. /D.N.I.....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D. / Dª. ....., mayor de edad, con domicilio en ....., nº....., Localidad ..... Provincia..... C.P. ..... Comunidad Autónoma..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 12 y 13 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Segunda de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia.

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un (1) mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez (10) días a contar desde la resolución estimatoria de la solicitud de acceso.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En.....a.....de.....de 20.....

Firmado:

10.15. ANEXO XV: Modelo de solicitud del derecho de Rectificación.

EJERCICIO DEL DERECHO DE RECTIFICACIÓN DATOS DEL RESPONSABLE DEL FICHERO

Nombre / Razón social: .....
Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso:
C/Plaza.....nº.....C.Postal.....
Localidad.....Provincia.....Comunidad Autónoma.....C.I.F. /D.N.I.....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D. / Dª. ....., mayor de edad, con domicilio en la.....,C/Plaza....., nº....., Localidad..... Provincia..... , C.P....., Comunidad Autónoma.....con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de rectificación sobre los datos anexos, aportando los correspondientes justificantes, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el artículo 15 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Tercera de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez (10) días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde, dentro del plazo de diez (10) días, que no procede acceder a practicar total o parcialmente las rectificaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la citada Ley Orgánica 15/1999.

Que si los datos rectificados hubieran sido comunicados previamente se notifique al responsable del fichero la rectificación practicada, con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En.....a.....de.....de 20.....

Firmado:

10.16. ANEXO XVI: Modelo de solicitud del derecho de Cancelación.

EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / Razón social: .....
Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso:
C/Plaza.....nº.....C.Postal.....
Localidad.....Provincia.....Comunidad Autónoma.....C.I.F. /D.N.I.....

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D/ Dª. ....., mayor de edad, con domicilio en la C/Plaza..... nº....., Localidad..... Provincia..... C.P..... Comunidad Autónoma..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de cancelación, de conformidad con lo previsto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en los artículos 15 y 16 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, vigentes al amparo de la disposición transitoria tercera de la citada Ley Orgánica 15/1999, y en la Norma Tercera de la Instrucción 1/1998, de 19 de enero, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, y en consecuencia,

SOLICITA,

Que se proceda a acordar la cancelación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez (10) días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la cancelación practicada.

Que en caso de que se acuerde dentro del plazo de diez (10) días que no procede acceder a practicar total o parcialmente las cancelaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del artículo 18 de la citada Ley Orgánica 15/1999.

Que si los datos cancelados hubieran sido comunicados previamente se notifique al responsable del fichero la cancelación practicada con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

En.....a.....de.....de 20.....

Firmado:

10.17. ANEXO XVII: Modelo de solicitud del derecho de Oposición.

EJERCICIO DEL DERECHO DE OPOSICION DATOS DEL RESPONSABLE DEL FICHERO

Nombre / Razón social: .....
Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso:
C/Plaza.....nº.....C.Postal.....
Localidad.....Provincia.....Comunidad Autónoma.....C.I.F. /D.N.I.....

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D. / Dª. ....., mayor de edad, con domicilio en la Calle/Plaza..... nº..... Localidad

..... Provincia..... C.P..... Comunidad

Autónoma..... con D.N.I....., del que acompaño copia, por medio del presente escrito ejerzo el derecho de oposición, de conformidad con lo previsto en los artículos 6.4, 17 y 30.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y en consecuencia,

EXPONGO,

.....
(Describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)
.....
.....

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

.....
(Enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)
.....
.....
.....

SOLICITO,

Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.
En.....a.....de.....de 20.....

Firmado:

10.18. ANEXO XVIII: Control de Auditorías.

AUDITOR	AÑO	FECHA DE ALTA
	...	...
...		