



Sistema de Gestión de la Seguridad de la Información

Obligaciones generales para las personas usuarias

Honek onartua
Aprobado por

Comité de Seguridad y Privacidad
Corporativa

Erreferentzia
Referencia

Obligaciones generales para las
personas usuarias

Data
Fecha

10/06/2025

Jasotzaileak
Distribución

A todo el personal

Dokumentu honen jabea Eusko Jaurlaritza da eta, bere edukia, barnekoa. Eusko Jaurlaritzako langileen artean besterik ezin da zabaldu, ezin zaio zabalkunde publikorik eman eta ezin da sortu zenerako helburuetatik at dauden bestelako helburuekin erabili. Hirugarren batzuei ematen bazaie, emateko baldintzak betez besterik ezin izango da erabili. Eusko Jaurlaritzari ezin izango zaio leporatu dokumentu honen argitalpenean egiten den akatsik edo huts egiterik.

Este documento es propiedad de Eusko Jaurlaritza – Gobierno Vasco y su contenido es **interno**. Su difusión debe limitarse al personal de Eusko Jaurlaritza – Gobierno Vasco, no debiendo ser difundido públicamente ni utilizado para otros propósitos que los que han originado su creación. En el caso de ser facilitado a terceros su utilización deberá limitarse exclusivamente a las condiciones bajo las cuales ha sido facilitado. Eusko Jaurlaritza – Gobierno Vasco no podrá ser considerado responsable de eventuales errores u omisiones en la edición del documento.

SEGURTASUN SAILKAPENA / CLASIFICACIÓN DE SEGURIDAD									
Erabilgarritasuna Disponibilidad	BAJA	Osotasuna Integridad	BAJA	Konfidentzialtasuna Confidencialidad	BAJA	Benetakotasuna Autenticidad	BAJA	Trazabilitatea Trazabilidad	BAJA

Control de versiones

Versión	Fecha	Cambio respecto a anterior versión	Elaborado por	Revisado por	Aprobado por
v.1	29/11/2018	Versión inicial	Oficina técnica de seguridad	Comité Técnico de Seguridad	Comité de Seguridad y Privacidad Corporativa del Gobierno Vasco
v.2	17/11/2021	Se incluyen medidas para la seguridad desde el exterior (uso de VPN). Se actualiza apartado de gestión de soportes extraíbles. Se hace mención a las consecuencias por incumplimiento de las obligaciones	Oficina técnica de seguridad	Comité Técnico de Seguridad	Comité de Seguridad y Privacidad Corporativa del Gobierno Vasco
v.3	15/11/2023	Cambio formato, corrección de erratas y actualización de normativa derogada. Se quitan menciones a la Política de protección de datos personales y al manual de seguridad de Platea.	Oficina técnica de seguridad	Comité Técnico de Seguridad	Comité de Seguridad y Privacidad Corporativa del Gobierno Vasco
v.4	10/06/2025	Actualización del título principal. Modificación del nombre del departamento DTIC a DED por nueva estructura organizativa.	Oficina técnica de seguridad	Comité Técnico de Seguridad	Comité de Seguridad y Privacidad Corporativa del Gobierno Vasco

Contenido

Apartado / Sección	Página
I. Introducción	4
1.1 Objetivo del documento	4
2. Visión general	5
2.1 Definición	5
2.2 Alcance	5
2.3 Objetivos	5
2.4 Ámbito de aplicación	5
2.5 Excepciones	6
3. Obligaciones generales de las personas usuarias	7
3.1 Clasificación y tratamiento de la información	7
3.2 Tratamiento de datos personales	11
3.3 Identificación y autenticación	12
3.4 Uso apropiado de recursos	12
3.5 Puesto de trabajo	13
3.6 Equipo informático de la persona usuaria	14
3.7 Seguridad en el exterior	15
3.8 Recursos de red	16
3.9 Correo electrónico	16
3.10 Internet	18
3.11 Webs corporativas	19
3.12 Gestión de soportes	20
3.13 Compras	21
3.14 Gestión de incidencias	22
3.15 Deber de secreto	22
4. Anexos	23
4.1 Anexo I: Documentos y procedimientos relacionados	23
4.2 Anexo II: Glosario de términos y abreviaturas	23

I. Introducción

Estas normas vienen derivadas de las obligaciones legales aplicables en materia de protección de datos personales (RGPD) y de seguridad de los servicios electrónicos (ENS). De este modo, estas normas se encuentran recogidas en la regulación de seguridad de la Administración Pública de la Comunidad Autónoma de Euskadi (en adelante Administración Pública de la CAE) desarrollada en GureSeK, plasmada en el documento «**Política de Seguridad y Privacidad de la Información**».

1.1 Objetivo del documento

El objetivo de este documento es determinar las obligaciones generales que las personas usuarias de la Administración Pública de la CAE deben observar a la hora de manejar datos personales, información o documentación relacionada con los servicios electrónicos de la Administración.

Con este documento se pretenden establecer las directrices generales que todo el personal debe cumplir en materia de seguridad de la información y privacidad de los datos personales.

Este documento es aplicable a cualquier dato personal, así como a toda la documentación o a cualquier otro tipo de información, estructurada o no, existente en torno a los servicios prestados por la Administración Pública de la CAE y, en particular, en torno a la prestación electrónica de los mismos.

2. Visión general

2.1 Definición

Las «Obligaciones generales para las personas usuarias» es el documento que establece las directrices a cumplir, desde el punto de vista de la seguridad de la información y de la privacidad de los datos personales, a la hora de manejar cualquier tipo de documentación, datos personales o información en general relacionada con la prestación de servicios por parte de la Administración Pública de la CAE.

2.2 Alcance

Las obligaciones generales de las personas usuarias recogidas en el presente documento deben ser cumplidas por todo el personal de la Administración General de la CAE, tanto en el tratamiento de datos personales como en el ámbito de la Administración Electrónica, así como por todo el personal perteneciente a empresas externas subcontratadas que tenga acceso a la documentación o información asociada a alguno de los servicios de la Administración.

2.3 Objetivos

Los objetivos del documento de obligaciones generales de las personas usuarias son los siguientes:

- Constituir un recopilatorio del conjunto de obligaciones a las que está sujeta cualquier persona que participe de algún modo en el tratamiento de datos personales o en la prestación de los servicios de la Administración Pública de la CAE.
- Establecer las pautas generales de comportamiento a seguir a la hora de tratar con datos personales o con información o documentación relacionada con la prestación de los servicios de la Administración Pública de la CAE.

2.4 Ámbito de aplicación

Las presentes obligaciones generales de las personas usuarias deberán ser aplicadas por todo el personal de la Administración Pública de la CAE o subcontratado por ésta en el ámbito del tratamiento de datos personales o en el ámbito de la Administración Electrónica en torno a cualquiera de los aspectos que se describen a continuación:

- Utilización del equipo informático de la persona usuaria.
- Utilización de los medios electrónicos móviles proporcionados por la Administración Pública de la CAE.
- Acceso a cualquiera de los recursos y servicios provistos por la Administración Pública de la CAE para el desarrollo de la actividad profesional.
- Utilización de la documentación de la Administración Pública de la CAE, tanto en formato electrónico como impresa.
- Gestión de la información relacionada con la provisión de servicios por parte de la Administración Pública de la CAE.
- Tratamiento de datos personales por parte de la Administración Pública de la CAE.

2.5 Excepciones

No se permite ningún tipo de excepción al cumplimiento de las obligaciones aquí recogidas. Cualquier incumplimiento de las mismas será expresamente analizado por el Comité de Seguridad y Privacidad Corporativa del Gobierno Vasco.

Queda excluida la aplicación de la presente normativa sobre aquella información consumida, tratada o generada por parte del Servicio Vasco de Seguridad Pública que, por su condición, quede fuera del alcance del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y pasa a estar al amparo de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/AI del Consejo.

3. Obligaciones generales de las personas usuarias

Las personas usuarias deberán conocer y asumir el contenido de este documento. Por lo tanto, todas ellas podrán acceder a una copia del mismo, y desempeñarán las funciones que se les encomienden de conformidad con lo dispuesto en este documento.

Para garantizar la seguridad de la información, las personas usuarias estarán obligadas a observar las normas de actuación que se recogen a continuación.

3.1 *Clasificación y tratamiento de la información*

#	Clasificación y tratamiento de la información
1	Todas las personas usuarias deberán conocer los niveles de seguridad en los que está clasificada la información y documentación con la que trabajan (si así fuese el caso), y manejarla de acuerdo a las directrices establecidas para el tipo de información en cuestión.
2	La clasificación de la información vendrá determinada por las directrices establecidas en la Política de Clasificación de la Información de la Administración Pública de la CAE.
3	En general, se considerará información no clasificada aquella cuyos niveles de seguridad no hayan sido establecidos, así como aquella cuya seguridad haya sido catalogada como SIN VALORAR. Por el contrario, se considerará información clasificada toda aquella información y documentación cuyos niveles de seguridad hayan sido establecidos como BAJO, MEDIO o ALTO, así como toda aquella información y documentación asociada a cualquier servicio cuyos niveles de seguridad hayan sido establecidos como BAJO, MEDIO o ALTO.

#	Clasificación y tratamiento de la información
4	Las medidas de comportamiento que se deben observar a la hora de manejar cualquier información o documentación clasificada son las siguientes: - A la hora de desarrollar documentación, siempre se deberá hacer uso de las plantillas oficiales y de los formatos estandarizados dentro de la Administración Pública de la CAE. - Será obligatorio cumplimentar todos los metadatos y campos complementarios de las plantillas y formatos utilizados, indicando expresamente como no aplicables aquellos campos cuya cumplimentación no sea pertinente - Para la gestión de la información y documentación se deberán seguir los procedimientos y protocolos establecidos, garantizando en todo momento el cumplimiento de los procedimientos administrativos asociados - Sólo la documentación formalmente aprobada podrá ser publicada en entornos abiertos (intranet, extranet o internet), siendo necesario garantizar que la gestión de la información y documentación en fase de modificación no sale de los entornos administrativos hasta que las modificaciones hayan sido aprobadas - Antes de publicar cualquier información y documentación en un entorno abierto (intranet, extranet o internet) se deberá asegurar que dicha información no incorpora ningún metadato ni campo oculto que no sea pertinente para los destinatarios de los documentos, para lo cual se deberá hacer uso de las utilidades de limpieza de documentos establecidas - Tras la aprobación pertinente se deberá llevar a cabo la actualización de la información y documentación existente en los entornos abiertos, observando en todo momento la diligencia oportuna en cuanto a premura y cumplimiento de los procedimientos establecidos - Se procurará minimizar el número de copias existentes de una determinada información o documento, debiendo considerarse el carácter temporal de las mismas - Se deberá prestar especial atención a no divulgar información clasificada de manera pública (en ponencias o exposiciones públicas, a través de Internet, etc.) a no ser que esté expresamente admitido. Así mismo, se deberá prestar especial atención a no manejar este tipo de información, ni de manera oral ni en formato electrónico o impreso, en entornos públicos ni fuera de las dependencias de la Administración Pública de la CAE. - Se deberá prestar especial atención a la pérdida de documentación impresa que pueda contener información clasificada.
5	Para el manejo de información clasificada cuya DISPONIBILIDAD haya sido valorada como MEDIA o ALTA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada, las siguientes medidas adicionales: Se deberán minimizar los cambios a llevar a cabo sobre la información o documentación publicada en entornos abiertos, realizándolos preferentemente en los periodos de menor acceso a dichos entornos, de acuerdo a las estadísticas de uso disponibles Cualquier incidencia asociada con la indisponibilidad de la información deberá ser inmediatamente reportada al CAU para su pronta resolución, de acuerdo a lo estipulado en el apartado 3.13 Gestión de incidencias

#	Clasificación y tratamiento de la información
6	Para el manejo de información clasificada cuya INTEGRIDAD haya sido valorada como MEDIA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada, las siguientes medidas adicionales: a. Se deberán minimizar los cambios a llevar a cabo sobre la información o documentación publicada en entornos abiertos, verificando expresamente el contenido en fase de aprobación Se deberán respetar escrupulosamente los procedimientos de gestión de cambios y versiones establecidos en torno a dicha información o documentación
7	Para el manejo de información clasificada cuya INTEGRIDAD haya sido valorada como ALTA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada y las establecidas específicamente para la información de INTEGRIDAD MEDIA, la siguiente medida adicional: Se deberá aplicar la Política de Firma Electrónica para firmar la información clasificada con este nivel de integridad
8	Toda información cuya CONFIDENCIALIDAD haya sido catalogada como SIN VALORAR se deberá considerar información pública, debiendo observarse para su tratamiento las consideraciones realizadas en los puntos 5 y 6 del presente apartado, referidos a la información con especiales requisitos de disponibilidad e integridad, respectivamente. Para el manejo de esta información se deberán observar, aparte de dichas medidas, la siguiente: Sólo podrá publicarse en Internet aquella información o documentación que haya sido catalogada como información pública
9	Para el manejo de información clasificada cuya CONFIDENCIALIDAD haya sido valorada como MEDIA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada, las siguientes medidas adicionales: a. Se deberán respetar de forma escrupulosa las políticas de escritorio limpio detalladas en los apartados 3.4. Puesto de trabajo y 3.5 Equipo informático de la persona usuaria, junto con todas las pautas establecidas específicamente dentro de dichos apartados b. Las personas responsables de cada entorno en los que se ubique o trate información de este nivel de confidencialidad deberán ser informadas de las solicitudes de acceso a dichos entornos, de modo que sean ellas quienes autoricen dichos accesos y sus modificaciones c. Se deberán llevar a cabo revisiones periódicas de los permisos de acceso a los entornos en los que se ubica o trata información de este nivel de confidencialidad, con el fin de que las personas responsables correspondientes verifiquen dichos permisos de acceso d. Se intentará que la cantidad de información de este nivel de confidencialidad que tenga que utilizarse fuera de las dependencias de la Administración Pública de la CAE sea mínima. En los casos en los que deba utilizarse se deberán acentuar las medidas de seguridad establecidas, sobre todo en lo referente a pérdidas de confidencialidad de la misma Deberá prestarse especial atención a la necesidad de eliminar todas las copias de información de este nivel de confidencialidad que no sean necesarias, sobre todo las copias almacenadas de forma local en los equipos y mesas de las personas usuarias.

#	Clasificación y tratamiento de la información
10	Para el manejo de información clasificada cuya CONFIDENCIALIDAD haya sido valorada como ALTA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada y las establecidas específicamente para la información de CONFIDENCIALIDAD MEDIA, las siguientes medidas adicionales: - Toda la información de este nivel de confidencialidad se deberá cifrar tanto en su almacenamiento como en su transmisión. Para ello se utilizarán las utilidades de cifrado dispuestas por la Administración Pública de la CAE a tal efecto en los diferentes entornos: - Utilización de VPN en comunicaciones - Cifrado de disco en ordenadores portátiles - Herramientas de cifrado de archivos, carpetas y unidades en PC, medios removibles (CD, DVD, memorias USB, etc.) y servidores - Cifrado implementado por las propias aplicaciones que lo requieran - En casos en los que la información de este nivel de confidencialidad sea compartida, no se deberá hablar sobre ella en lugares públicos ni en zonas abiertas, ni siquiera dentro de las dependencias de la Administración Pública de la CAE. Estas conversaciones deberán tener lugar en departamentos convenientemente cerrados y privados, con el fin de que no se produzcan escuchas por parte de terceras personas - Durante el trabajo con información de este nivel de confidencialidad, se deberá prestar especial atención a que nadie ajeno a la misma puede ver dicha información. Por tanto, será necesario cubrir o proteger adecuadamente todos los documentos, en papel o electrónicos, con el fin de evitar «miradas indiscretas» - Los documentos electrónicos con información de este nivel de confidencialidad deberán estar convenientemente protegidos, de modo que sólo puedan acceder a ellos las personas usuarias expresamente autorizadas. - La información en papel deberá guardarse adecuadamente, en lugares donde como mínimo sea necesario poseer una llave o conocer una contraseña para acceder a ellos. Habrá que prestar especial atención a la realización de copias de la información de este nivel de confidencialidad, que deberán ser las mínimas posibles y tener las mismas medidas de protección que los originales
11	Para el manejo de información clasificada cuya AUTENTICIDAD haya sido valorada como MEDIA o ALTA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada, la siguiente medida adicional: Se deberá aplicar la Política de Firma Electrónica para firmar la información clasificada con este nivel de autenticidad
12	Para el manejo de información clasificada cuya TRAZABILIDAD haya sido valorada como MEDIA se deberá observar, además de las medidas de comportamiento generales establecidas para la información clasificada, la siguiente medida adicional: Esta información deberá ser tratada mediante plataformas de gestión de contenidos, gestión de documentos, gestión de versiones o similares que permitan el registro automático de los cambios sufridos por la información y de los distintos estados por los que va pasando

#	Clasificación y tratamiento de la información
13	Para el manejo de información clasificada cuya TRAZABILIDAD haya sido valorada como ALTA se deberán observar, además de las medidas de comportamiento generales establecidas para la información clasificada y las establecidas específicamente para la información de TRAZABILIDAD MEDIA, las siguientes medidas adicionales: a. Esta información deberá ser tratada mediante plataformas de gestión de contenidos, gestión de documentos, gestión de versiones o similares que permitan el registro automático de la actividad de las personas usuarias en torno a ella, identificando para cada acceso a la información la persona usuaria que lo realiza, el instante en que se lleva a cabo, la tipología de dicho acceso y el resultado del mismo Esta información deberá ser tratada a través de la plataforma DOKUSI en forma de documento electrónico administrativo, utilizando las funcionalidades de firma electrónica con sellado de tiempo que ofrece dicha plataforma

3.2 *Tratamiento de datos personales*

#	Tratamiento de datos personales
1	Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado, respetando los principios de licitud, lealtad y transparencia.
2	Se respetará el principio de limitación de la finalidad, que requiere que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; salvo con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, que no se considerarán incompatible con los fines iniciales.
3	Se tendrá siempre en cuenta el principio de minimización de datos, que obliga a que los datos personales sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
4	Se atenderá al principio de exactitud, que requiere que los datos personales sean exactos y, si fuera necesario, se actualicen; adoptando todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
5	Se respetará el principio de limitación del plazo de conservación, de modo que los datos personales sean mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; salvo en los casos en los que dichos datos personales se conserven con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en cuyo caso podrán conservarse durante períodos más largos, pero siempre sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente documento a fin de proteger los derechos y libertades del interesado.

#	Tratamiento de datos personales
6	Se tendrá siempre en cuenta el principio de seguridad de los datos, que obliga a que los datos personales sean tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas desarrolladas por la Administración Pública de la CAE. Estas medidas deberán ser aplicadas tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento
7	Todas las actividades de tratamiento de datos personales deberán estar apropiadamente registradas en el Registro de Tratamientos. Cualquier nuevo tratamiento, modificación en el mismo o cese deberá suponer la correspondiente actualización de dicho Registro de Tratamientos
8	Cuando sea probable que un tratamiento nuevo o modificado, por su naturaleza, alcance, contexto, fines o tecnologías utilizadas, entrañe un alto riesgo para los derechos y libertades de las personas físicas, será necesario realizar, antes del tratamiento, una evaluación del impacto de las operaciones de dicho tratamiento en la protección de los datos personales asociados

3.3 **Identificación y autenticación**

#	Identificación y autenticación
1	La persona usuaria, para acceder a los sistemas de información, deberá disponer de un acceso autorizado, por regla general, en virtud de identificador de persona usuaria y contraseña.
	La contraseña deberá cumplir la Política de Contraseñas de SARgune disponible en JAKINA , en el apartado de « <i>Informática y Telecomunicaciones</i> »
	En el supuesto de que así lo establezca la persona responsable de la información o la persona responsable del tratamiento de los datos personales, deberá disponer de firma electrónica avanzada u otro medio de identificación adecuado a las características de la información de que se trate. En este caso, también le serán de aplicación, con las adaptaciones debidas, las normas de actuación a las que se refiere el número anterior (2)

3.4 **Uso apropiado de recursos**

Los recursos materiales, informáticos, de comunicaciones o de cualquier otro tipo provistos por la Administración Pública de la CAE únicamente se proporcionan para el cumplimiento de las funciones en el desempeño del trabajo de la persona usuaria. Esta consideración facultará a la Administración Pública de la CAE a

implementar sistemas de control destinados a velar por la protección y el buen uso de los recursos. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad de la persona empleada y su derecho a la intimidad.

Por este motivo, el personal viene obligado a:

#	Obligaciones
1	Utilizar los programas antivirus y sus actualizaciones, poniendo la diligencia necesaria para proteger los sistemas de información contra accesos y usos no autorizados y evitar la destrucción o cualquier otro perjuicio a la información que maneja
2	Utilizar únicamente las versiones de software facilitadas por la Dirección de Estrategia Digital (DED), EJE u otro proveedor debidamente autorizado, siempre siguiendo sus normas de utilización. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente
3	Sólo se introducirán datos identificativos y direcciones de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo, Outlook)

A tal fin quedan prohibidos:

#	Prohibiciones
1	El uso de los recursos para actividades no relacionadas con las funciones propias de cada persona usuaria
2	Las actividades, equipos o aplicaciones no autorizadas por el órgano competente en la Administración
3	Introducir en los sistemas de información o la red corporativa contenidos comprometedores para la Administración. Estos son contenidos obscenos, amenazadores, inmorales u ofensivos, pero caben también otras posibilidades
4	Introducir voluntariamente programas, virus, macros, applets, controles ActiveX, sniffers, crackeadores o cualquier otro dispositivo lógico o físico que cause o pueda causar cualquier alteración o daño a los SSII o robo de información
5	Intentar destruir, alterar o inutilizar de cualquier otra forma los recursos telemáticos de la Administración
6	Intentar distorsionar o falsear los registros de actividad (log) de los SSII

3.5 **Puesto de trabajo**

En su puesto de trabajo todas las personas usuarias deberán cumplir la siguiente política de escritorio limpio:

#	Política de escritorio limpio
1	Los puestos de trabajo deberán permanecer despejados, sin más documentación encima de la mesa que el requerido para la actividad que se está realizando en cada momento
2	Toda la documentación en papel, así como todos los soportes de información electrónica, se guardarán en un lugar cerrado cuando no se estén utilizando

3.6 *Equipo informático de la persona usuaria*

Durante el uso de los equipos de persona usuaria, se deberán observar las siguientes obligaciones:

#	Obligaciones
1	Proteger, en la medida de sus posibilidades, la confidencialidad de la información a la que tienen acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido, cualquiera que sea el soporte en que se encuentre contenida la información
2	Cada equipo informático de persona usuaria estará bajo la responsabilidad de alguna persona usuaria autorizada que garantizará que la información que muestran no pueda ser visible por personas no autorizadas
3	Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al equipo informático de la persona usuaria deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad
4	Cuando la persona responsable de un equipo informático abandone temporalmente su ubicación física, deberá dejarlo en un estado que impida la visualización de la información clasificada, por ejemplo, bloqueando el equipo. La reanudación del trabajo implicará la desactivación del desbloqueo mediante la introducción de la contraseña correspondiente. Si el abandono del equipo se produjera debido a la finalización de su turno de trabajo, la persona usuaria procederá al cierre completo de la sesión del sistema
5	Utilizar el menor número de informes en formato papel que contengan información clasificada y mantener los mismos en lugar seguro y fuera del alcance de terceras personas
6	No podrán guardar información clasificada, y en particular ficheros que contengan datos personales, en discos locales de los ordenadores personales (PC)
7	Las copias temporales de información y/o datos personales que se creen tendrán las mismas medidas de seguridad que correspondan a los ficheros maestros de los que proceden sus datos, siempre y cuando deba mantenerse dicho nivel de seguridad, considerando la tipología de los datos seleccionados, el origen y/o los usos previstos para los mismos. Una vez que estas copias hayan dejado de ser útiles para la finalidad con la que se crearon, serán borradas por la persona usuaria que las creó.

#	Obligaciones
8	En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan información clasificada. Si las impresoras son compartidas con otras personas usuarias no autorizados para acceder a información, las personas responsables de cada equipo deberán retirar los documentos conforme vayan siendo impresos o, si es posible, utilizar la impresión retenida (protegida por contraseña, ver documento « <i>Guía de buenas prácticas para configuración y uso de dispositivos multifunción (DMF)</i> »)
9	Los equipos informáticos de persona usuaria tendrán una configuración fija en sus aplicaciones, sistemas operativos, etc. que sólo podrá ser cambiada bajo la autorización del Responsable de la Información o de la persona responsable del tratamiento de datos personales o por personas administradoras autorizadas
10	Todas las personas usuarias deberán hacer un uso apropiado de las herramientas de seguridad instaladas en sus equipos informáticos (firewall, antivirus, antimalware, herramientas de cifrado de información, herramientas de VPN, etc.)
11	Está prohibido deshabilitar cualquier herramienta, programa, utilidad o software de cualquier tipo (con fines de seguridad) instalado en los equipos informáticos de la persona usuaria
12	Las personas usuarias de ordenadores portátiles evitarán, en la medida de lo posible, que estos equipos contengan claves de acceso remoto a recursos internos del Gobierno Vasco.
13	Toda la información cuya CONFIDENCIALIDAD esté clasificada como de nivel ALTO que pueda estar almacenada temporalmente en un ordenador portátil se deberá guardar cifrada, utilizando las herramientas dispuestas a tal efecto en el equipo

3.7 Seguridad en el exterior

Cuando alguna persona usuaria haga uso o acceda a cualquier tipo de información clasificada, estando fuera de las dependencias de la Administración Pública de la CAE, deberá seguir las siguientes normas de comportamiento:

#	Normas de comportamiento
1	Deberá acceder a la información con la máxima discreción posible, evitando que otras personas puedan acceder a ella (leyéndola del propio documento en papel o de la pantalla del equipo de la persona usuaria o escuchando la conversación) de manera casual
2	Se deberá prestar especial atención para impedir la pérdida o robo de cualquier documento en papel, soporte de información o equipo de la persona usuaria que pueda contener información clasificada o que pueda permitir el acceso a ella
3	Si se trabaja con información cuyo nivel de CONFIDENCIALIDAD haya sido clasificado como MEDIO o ALTO se deberán seguir con especial diligencia las directrices efectuadas a tal efecto en los puntos 9 y 10 del apartado 3.1 Clasificación y tratamiento de la información

#	Normas de comportamiento
4	En caso de pérdida o robo, o ante cualquier sospecha de que la confidencialidad de la información clasificada haya podido ser vulnerada de algún modo, se deberá notificar inmediatamente al CAU o a la persona responsable de la Información (según el caso) para que se proceda a la apertura del incidente de seguridad correspondiente, de acuerdo a lo estipulado en el apartado 3.13 Gestión de incidencias
5	En caso de tener que acceder a los sistemas de información desde fuera de las instalaciones de la Administración Pública de la CAE, se deberá acceder a través de una red VPN y se asignarán al usuario los mismos permisos que dispone para los accesos locales. Para solicitar acceso de manera remota, será el informático del departamento quién realizará la petición al Servicio de Seguridad de Usuarios quien validará dichos accesos. Si se necesita acceso a una aplicación concreta, el Servicio de Seguridad de Usuarios redirigirá la petición al responsable de la aplicación.

3.8 Recursos de red

Las personas usuarias son responsables, con carácter general, de asegurar que los datos, las aplicaciones y demás recursos informáticos puestos a su disposición, sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados. En este sentido, las personas con acceso a los SSII deberán cumplir las siguientes medidas de seguridad:

#	Medida de seguridad
1	No conectar, a ninguno de los recursos informáticos, ningún tipo de equipo de comunicaciones que posibilite la conexión a la red corporativa, sin la oportuna autorización
2	No conectarse a la red corporativa a través de otros medios que no sean los definidos y administrados por la DED, EJIE u otro Organismo o Entidad competente (cuando EJIE no actúe como encargado de tratamiento), sin perjuicio de lo dispuesto en la normativa que sea de aplicación
3	No intentar acceder a áreas restringidas de los sistemas de información propios o de terceros, ni otros accesos distintos a aquellos que les hayan sido asignados
4	No intentar descifrar claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos
5	No poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, ni dañar o alterar cualquiera de los recursos informáticos

3.9 Correo electrónico

En relación al uso del correo electrónico se establecen los siguientes principios:

#	Principio
1	Se considerará al correo electrónico como una herramienta más de trabajo provista a la persona usuaria con el fin de ser utilizada conforme al uso para el cual está destinada
2	El sistema de correo electrónico de la Administración Pública de la CAE no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares
3	Las personas usuarias no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples personas usuarias)
4	En relación al intercambio de información a través del correo electrónico, se considerarán no autorizadas las siguientes actividades: a. Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual b. Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal c. Transferencia a terceras partes no autorizadas de material de la Organización o material que es de alguna u otra manera confidencial d. Transmisión o recepción de ficheros que infrinjan el Reglamento General de Protección de Datos (RGPD) o las directrices de la Administración Pública de la CAE. Transmisión o recepción de cualquier tipo de dato e información no relacionadas con la actividad de la Administración Pública de la CAE.
5	Se atenderá expresamente a las disposiciones legales vigentes en materia de envío de información, limitando en la medida de lo posible el uso del correo electrónico a aquellos casos en los que no se determinan especiales exigencias en materia de protección de datos, trazabilidad, autenticidad, confidencialidad o no repudio. En caso contrario se utilizarán de manera preferente las vías oficiales establecidas por la Administración Pública de la CAE para el envío de comunicaciones y notificaciones electrónicas
6	Se deberán utilizar todas aquellas utilidades de seguridad dispuestas para la protección del correo electrónico: a. Uso de firma electrónica con aquellos correos electrónicos destinados al exterior cuya autenticidad e integridad se quiera garantizar b. Uso de cifrado con aquellos correos electrónicos cuya confidencialidad se quiera garantizar Uso de las utilidades del antivirus para verificar que los correos electrónicos no tienen virus
7	No se permitirá la transmisión vía correo electrónico de información cuya CONFIDENCIALIDAD esté clasificada como ALTA ni de datos personales de categorías especiales, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido
8	Se verificarán expresamente las direcciones de correo incluidas como destinatarias, con el fin de evitar, en la medida de lo posible, el envío de correos electrónicos a direcciones incorrectas o erróneas

#	Principio
9	Se prestará especial atención al uso de los campos CCO (con copia oculta) para definir las personas u organizaciones destinatarias de todos aquellos correos que se dirijan a grandes cantidades de persona usuarias u organizaciones, listas de distribución o destinatarias de diferentes organizaciones externas a la Administración Pública de la CAE.
10	Para la interacción con la ciudadanía y otras organizaciones se deberán utilizar cuentas de correo genéricas, limitando en estos casos el uso de las cuentas de correo personalizadas exclusivamente a aquellos casos en los que sea imprescindible

3.10 Internet

En relación con el acceso a Internet se tendrán en cuenta las siguientes directrices:

#	Directriz
1	Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Las personas usuarias no deben buscar o visitar sitios que no sirvan como soporte a los deberes y obligaciones de la Administración Pública de la CAE o al cumplimiento de su trabajo diario
2	El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporado en la misma. La utilización de otros medios de conexión deberá ser previamente validada, y estarán sujetos a las anteriores consideraciones sobre el uso de Internet
3	Las personas usuarias no deberán usar el nombre, símbolo, logotipo o símbolos similares a los de la Administración Pública de la CAE en ningún elemento de Internet (correo electrónico, páginas web, etc.) si no está justificado por actividades estrictamente laborales
4	Únicamente se permitirá la transferencia de datos «desde» o «hacia» Internet en relación con las actividades propias de la Administración Pública de la CAE. La transferencia de ficheros no relativa a actividades propias (por ejemplo, la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia, etc.) estarán prohibidas
5	Las personas usuarias no deben ocultar o manipular su identidad en ninguna circunstancia, salvo en los casos en los que se permita el uso de identificadores anónimos

#	Directriz
6	En relación con el uso de Internet se considerarán no autorizadas las siguientes actividades: - Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual - Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal - Transferencia a terceras partes no autorizadas de material de la Organización o material que es de alguna u otra manera confidencial - Transmisión o recepción de ficheros que infrinjan el Reglamento General de Protección de Datos (RGPD) o las directrices de la Administración Pública de la CAE. - Transmisión o recepción de cualquier tipo de dato e información no relacionadas con la actividad de la Administración Pública de la CAE. - Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con la actividad de la Administración Pública de la CAE. Realización de actividades que puedan dañar la buena reputación de la Administración Pública de la CAE, incluyendo actividades realizadas por personal de la Administración Pública de la CAE para su propio beneficio económico o de terceras partes, actividades de naturaleza política u otras similares
7	La participación del personal de la Administración Pública de la CAE en las redes sociales estará regulada por lo establecido en la «Guía de usos y estilo en las Redes Sociales del Gobierno Vasco» editada por el Departamento de Presidencia.

3.11 Webs corporativas

En relación a la publicación de información y documentación en cualquiera de las webs corporativas accesibles desde entornos abiertos (intranet, extranet e internet) se deberán tener en cuenta las siguientes directrices:

#	Directriz
1	Se tomarán medidas para la protección de la integridad de la información publicada en web, a fin de prevenir la modificación no autorizada que pudiera dañar la reputación de la Administración Pública de la CAE.
2	Se implementará un procedimiento de autorización formal antes de que la información se ponga a disposición del público objetivo

#	Directriz
3	Todos los sistemas de acceso público deberán tener en cuenta que: - La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la LOPDGDD y la LSSI/CE - La información que se publique, o aquella que se procesa, sea la correcta - La información confidencial sea protegida durante el proceso previo a su publicación - El acceso al sistema de publicación no permita el acceso accidental a otros entornos - Se identifique a la persona responsable de la publicación de información en la web pública Se garantice la validez y vigencia de la información publicada
4	En Internet sólo se podrá publicar la información pública, cuya CONFIDENCIALIDAD ha sido clasificada como SIN VALORAR. En este caso, el personal de la Administración Pública de la CAE tendrá la obligación de poner a disposición pública esta información
5	En el entorno de extranet sólo se podrá publicar aquella información cuyo nivel de CONFIDENCIALIDAD haya sido clasificado como BAJO o MEDIO, y en este segundo caso únicamente si las personas externas a las que se permite el acceso a la información y documentación deben tener acceso a ella
6	En el entorno de intranet general (<i>Jakina</i>) sólo se publicará aquella información cuyo nivel de CONFIDENCIALIDAD haya sido clasificado como BAJO. También se podrá publicar en los entornos de <i>Jakina</i> que incorporen control de acceso la información y documentación cuyo nivel de CONFIDENCIALIDAD haya sido clasificado como MEDIO, siempre limitando el acceso exclusivamente a los grupos de personas que deben tener acceso a ella
7	La información cuya CONFIDENCIALIDAD haya sido clasificada como ALTA no se publicará bajo ningún concepto en ningún entorno abierto

3.12 Gestión de soportes

Las personas usuarias están obligadas cumplir las siguientes medidas de seguridad relacionadas con la gestión de soportes de información extraíbles:

#	Medida de seguridad
1	Se debe evitar el uso de soportes extraíbles con información de la Administración Pública de la CAE, priorizando su compartición mediante el uso de las herramientas Office 365 corporativas (OneDrive, Sharepoint).
2	Se prohíbe expresamente el uso de soportes extraíbles para transportar información de nivel ALTO, CONFIDENCIAL, SENSIBLE, o de condición equivalente. Para el resto de las categorías de información, el soporte debe ir cifrado (consultar Guía de cifrado).
3	En caso de necesidades excepcionales, las Direcciones de Servicio de los departamentos, Organismos Autónomos o Entidades Públicas de Derecho Privado podrán proveer USBs de uso temporal.

#	Medida de seguridad
4	Es obligatorio devolver los soportes que contengan información, y en especial datos personales, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos
5	Guardar los soportes que contengan información en lugar seguro y siempre bajo llave cuando no sean usados, especialmente fuera de la jornada laboral. En cualquier caso, deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso de esa información
6	Durante el uso y almacenamiento de los soportes se deberán respetar las precauciones necesarias para su adecuada conservación, así como las exigencias de mantenimiento de la empresa que los fabrica en lo relativo a temperatura, humedad y otros agresores medioambientales
7	Los soportes que contengan información deberán estar claramente identificados con una etiqueta externa que indique (directa o indirectamente) el nivel más alto de clasificación de la información contenida en ellos.
8	Toda información contenida en soportes que sean reutilizables deberá ser borrada antes de una nueva utilización del soporte
9	Aquellos soportes de información que sean reutilizables, y en especial aquellos que hayan contenido copias de datos personales, deberán ser completamente formateados (no se podrá usar el formato rápido) antes de su utilización por una persona distinta a la persona usuaria anterior, de forma que los datos que contenían no puedan ser recuperados nuevamente. En estos casos será deseable el uso de alguna utilidad de borrado seguro (comúnmente denominado “wipeo”) a nivel físico
10	Se deberá registrar cualquier entrada de soportes que contengan información, identificando al transportista que realiza la entrega

3.13 Compras

Todas aquellas personas que realicen compras de productos hardware, software, y contratación de servicios deberán atender a las siguientes directrices:

#	Directriz
1	Se deberá aplicar la Guía de seguridad en la contratación de servicios o adquisición de productos TIC a la hora de llevar a cabo la adquisición de productos hardware y/o software en los que la seguridad tenga un papel determinante, así como en aquellos casos en los que dichos productos hardware y software vayan a tratar datos personales
2	Se deberá aplicar la Guía de seguridad en la contratación de servicios o adquisición de productos TIC a la hora de llevar a cabo la contratación de servicios de seguridad o de aquellos servicios en los que la seguridad tenga un papel determinante, así como en aquellos casos en los que dichos servicios vayan a tratar datos personales

3.14 **Gestión de incidencias**

Las personas usuarias están obligadas a favorecer la adecuada gestión de incidencias, para lo que deberán cumplir las siguientes medidas de seguridad:

#	Medida de seguridad
1	Deberán notificar al CAU cualquier incidencia que detecten y que afecte o pueda afectar a la seguridad de la información (sospecha de uso indebido del acceso autorizado por otras personas; recuperación de datos, etc.) La pérdida de listados o documentos en papel, la pérdida de soportes electrónicos de información –disquetes, CD, DVD, memorias USB o soportes electrónicos de cualquier otro tipo- deberá ser notificado a la persona responsable de la Información (según el Acuerdo de Consejo de Gobierno, de 30 de junio de 2015, en el que se aprueba la estructura organizativa y asignación de roles de seguridad)
2	El conocimiento y la no notificación de una incidencia por parte de una persona usuaria será considerado como una falta contra la seguridad de la información por parte de esa persona usuaria

3.15 **Deber de secreto**

#	Medida de seguridad
1	Todo el personal deberá guardar, por tiempo indefinido, la máxima reserva, y no deberá utilizar para fines no autorizados ni emitir al exterior información clasificada ni datos personales salvo que esté debidamente autorizado, tal y como se establece en el Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
2	En el caso en que, por motivos relacionados con el puesto de trabajo, la persona usuaria entre en posesión de información confidencial contenida en cualquier tipo de soporte y a través de cualquier medio, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello otorgue derecho alguno de posesión, titularidad, copia o distribución sobre dicha información

4. Anexos

4.1 Anexo I: Documentos y procedimientos relacionados

#	Documento / Procedimiento
1	Guía de buenas prácticas para configuración y uso de dispositivos multifunción (DMF)
2	Guía de seguridad en la contratación de servicios o adquisición de productos TIC
3	Guía de usos y estilo en las Redes Sociales del Gobierno Vasco
4	Política de clasificación de la información
5	Política de firma electrónica
6	Política de Seguridad y privacidad de la Información
7	Procedimientos de gestión de cambios o versiones
8	Procedimientos para la gestión de la información y documentación
9	Utilidades de cifrado dispuestas por el Gobierno Vasco
10	Guía de limpieza de documentos
11	Guía de cifrado

4.2 Anexo II: Glosario de términos y abreviaturas

A continuación, se define una serie de términos que han sido empleados a lo largo de todo el documento y que facilitan el entendimiento del mismo.

#	Término	Definición
1	Activo	Componente, funcionalidad o recurso que tenga valor para la organización —información, datos, servicios, aplicaciones, equipos, comunicaciones, recursos administrativos, físicos y humanos...—
2	Amenaza	Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [UNE 71504:2008] Las amenazas siempre están presentes, pero se pueden intentar evitar o paliar los efectos de su materialización

#	Término	Definición
3	Análisis de Riesgos	Proceso para el análisis de las amenazas, vulnerabilidades, riesgos e impactos a los que está expuesto un sistema de información, teniendo en cuenta las medidas de seguridad ya presentes. Sirve como punto de partida para identificar las mejoras en las medidas de seguridad, tanto en lo que se refiere a la efectividad como a los costes
4	Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [ENS]
6	CAU	Servicio de atención a personas usuarias, orientado a atender incidencias relativas a los Sistemas Informáticos disponibles en el Gobierno Vasco (consultas, problemas o averías). Su actuación comprende la recepción, tratamiento y resolución de las incidencias detectadas (correo electrónico, aplicaciones, sistemas...)
7	Comité de Seguridad Corporativa	Organismo colegiado que asume la función de dirigir y coordinar los intereses de todas las entidades y personas afectadas por la Administración Electrónica en materia de seguridad
8	Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a personas, entidades o procesos no autorizados [ENS]
9	Conservación	Garantía de seguridad consistente en estabilizar y proteger la información del deterioro temporal a lo largo de todo su ciclo de vida
10	Dato personal	Toda información sobre una persona física identificada o identificable («el interesado»); considerando persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona [RGPD]
11	Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a estos cuando lo requieren [ENS]
12	DOKUSI	Sistema Integral de Gestión Documental (D okumentu K udeaketa Sistema Integrala) del Gobierno Vasco

#	Término	Definición
13	ENS	Esquema Nacional de Seguridad (RD 311/2022)
14	Gestión de incidentes o incidencias	Procesos orientados a recuperar el nivel habitual de funcionamiento del servicio y a minimizar en todo lo posible el impacto negativo en la organización, de forma que la calidad del servicio y la disponibilidad se mantengan
15	Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respeto a los riesgos [ENS]
16	Incidente de seguridad	Suceso inesperado o no deseado con consecuencias negativas para la seguridad del sistema de información [ENS], en particular cuando ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos [RGPD].
17	Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada [ENS]
18	Jakina	Nombre con el que se conoce la Intranet Corporativa del Gobierno Vasco
19	RGPD	Reglamento General de Protección de Datos - REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
20	LSSI/CE	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Se establecen las obligaciones, responsabilidades, infracciones y sanciones de aquellas empresas y particulares en general que tienen una página Web o que operan por Internet. También regula expresamente el envío de correos electrónicos con fines comerciales
21	Medidas de seguridad	Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, disuasión, protección, detección y reacción, o bien de recuperación [ENS]

#	Término	Definición
22	Metadato	Dato anexo o asociado a un determinado documento o fichero y que proporciona información adicional sobre él
23	Persona Usuaría	Cualquier persona con participación, directa o indirecta, en la prestación de servicios electrónicos o con acceso a la documentación o información relacionada con ellos
24	Política de seguridad y privacidad	Documento de alto nivel que especifica los objetivos en materia de seguridad de una organización y refleja el compromiso de la dirección para alcanzarlos
25	Proceso	Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y un fin delimitados, implica recursos y da lugar a un resultado [ENS]
26	LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
27	Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, con daños o perjuicios a la organización [ENS]
28	SARgune	Sistema de acceso a los servicios de la Red Corporativa del Gobierno Vasco, cuyo objetivo es mejorar la seguridad y la calidad, a la vez que facilitar el acceso a dichos servicios
29	Seguridad de la información	Protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas
30	Sellado de tiempo	El sellado de tiempo es un método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces
31	Sistema de información	Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir [ENS]
32	SSII	Sistemas de Información (en plural)
33	Soporte	Medio físico de cualquier tipo (papel, DVD, discos portátiles, etc.) utilizado para almacenar información

#	Término	Definición
34	Tratamiento de datos personales	Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción [RGPD].
35	Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad [ENS]
36	VPN	Red Privada Virtual (por sus siglas en inglés « <i>Virtual Private Network</i> »)
37	Vulnerabilidad	Una debilidad en un activo que puede ser aprovechada por una amenaza [ENS]