Excmo. Colegio Oficial
de Graduados Sociales
de Santa Cruz de Tenerife

SISTEMA DE TRATAMIENTO DE DATOS

PROTECCIÓN DE DATOS

Índice

ANEXO I
Descripción de los sistemas de información y recursos protegidos

El sistema de tratamiento de datos de carácter personal está compuesto por los siguientes elementos:

1. Estructura del sistema de información, indicando las características generales que afectan a la seguridad e integridad de los datos.
2. Programas que acceden a los datos.
3. Sistema de almacenamiento de datos en papel.
4. Listado de terminales desde los que se puede acceder a los datos de carácter personal.
5. Procedimientos para la copia de seguridad.
6. Procedimientos para la gestión de brechas de seguridad

De cada uno de los siguientes apartados es importante matizar las características de la información almacenada en cada campo.

CONTROL DE ACCESO

Indicación de si existen medidas que controlen el acceso físico a las instalaciones o sistemas donde se tratan datos. Estos controles pueden ser:

- **Control de acceso a servidores:** se indica si al espacio físico donde están almacenados los servidores, existe algún control de acceso, como llave a la habitación / rack donde están ubicados.
- **Alarma**: si existe un sistema de alarma.
- **Rejas**: indicación de si se cuenta con rejas, portal u otro medio que dificulte el libre acceso a las instalaciones.
- **Control de acceso a las instalaciones** mediante clave, carnet…
- **Llaves**: si existe más de una persona con copia de las llaves de las instalaciones.
- **Videoportero**: si la entrada a las instalaciones es previo la visión de que persona accede a las mismas mediante un sistema de videoportero.
- **Armarios con llave:** los armarios que contengan datos especialmente sensibles deben contar con una llave para controlar el acceso a esa información.
- **Cámaras**: si las instalaciones cuentan con algún sistema de videovigilancia, en este caso se debe indicar:
  - Empresa de alarmas a las que está conectado el sistema en caso de existir.
  - Tiempo de conservación de las imágenes, el cual no puede superar los 30 días.
  - Personas autorizadas al visionado de imágenes.

SISTEMA (hardware /software)

Se determina las generalidades del sistema de tratamiento de datos, en los apartados que afectan a la seguridad o integridad de los datos, de esta forma se contempla información sobre:

SAI

Indicación de que los terminales cuenta con un Sistema de Alimentación Ininterrumpida que impida apagones bruscos del terminal ante la falta de corriente, o daños en casos de picos de la misma. En caso de tener un servidor central en la estructura de red, debe contar con este sistema, ya que puede ocasionar que si se falta la alimentación cuando varios usuarios están grabando datos, estos se corrompan y no sean íntegros.

DESTRUCCION DE PAPEL

Indicación de si se cuenta con un sistema adecuado para la destrucción de papel con datos personales, acorde al nivel de los mismos. Se indica si cuenta con destructoras de papel, una empresa externa que presta ese servicio o ambos.

ANTIVIRUS

Indicación de si el terminal cuenta con un programa antivirus que impida la infección del mismo. En la medida de lo posible se debe escoger uno para todos los terminales de la red.

FIREWALL

Indicación de si el terminal cuenta con un cortafuegos que impida la intrusión externa en el sistema. En la medida de lo posible, se debe escoger uno para todos los terminales de la red.

IMPRESORAS COMPARTIDAS

Indicación de si las impresoras están compartidas por varios usuarios. También se indica si la impresora cuenta con un sistema de bloqueo de impresión, que permita garantizar que solo la persona que ha imprimido el documento tenga acceso al mismo.

CONTRASEÑAS

Explicación de qué puntos del sistema cuentan con contraseña, y las características de la misma en cuanto a:

- Su longitud
- Complejidad
- Cada cuanto tiempo debe modificarse
- El límite de intentos de acceso, si se alerta de errores en el acceso.
- Si el sistema se bloquea la sesión

Este apartado debe compararse con el recomendado en las medidas de seguridad de este documento.

TRANSMISIONES TELEMÁTICAS

Indicación de si se transmiten datos de carácter personal por medios telemáticos asiduamente. O si se conocectan a plataformas de terceros para procesar datos

DATOS DE RED

Explicación de la estructura de red, indicando si es un dominio o un grupo de trabajo, en determinados casos se complementa con información del esquema de red. Este es un apartado crucial en la seguridad de la red, ya que las ventajas del Dominio son elevadas a la hora de garantizar el acceso del usuario/a datos y/o permitir una configuración rápida de todos los terminales.

CIFRADO DE DATOS

Para las transmisiones de datos especialmente protegidos se establecerá un sistema de cifrado. Se indica en este apartado si el sistema cuenta con alguna herramienta que realice el cifrado de datos.

FIRMA ELECTRÓNICA

Si cuenta con algún sistema de firma electrónica para la verificación del autor de documentos y /o envíos telemáticos se indicará en este campo.

OTROS

AUDITORÍAS INTERNAS

Puede existir alguna auditoría interna específica en protección de datos, seguridad de la información o cualquier otra norma que tenga en cuenta parámetros de seguridad.

CERTIFICADO ISO 27001

En el caso de contar con esta certificación, se asume que el sistema de tratamiento de datos cuenta con ciertas garantías de seguridad.

PLAN DE CONTINGENCIA

Se indica si se cuenta con una evaluación extensa de riesgos y un plan de medidas para contrarrestarlos.

GARANTIA DE ACCESO A DOCUMENTOS

Está basada en la pseudonimización/ anonimización, el registro de documentos y la autorización para copias que garantiza que cualquier información en papel tiene un estricto control del acceso y contenido.

PROGRAMAS

NOMBRE

Nombre con el que se accede al programa.

TIPO

Indicación de la utilidad principal del programa.

ACCESO

Especificación desde donde se puede acceder al programa, esto puede ser desde equipos específicos, desde cualquier equipo de la red, desde una IP determinada o desde una dirección web (acceso independiente).

CONTRASEÑA

Indicación de exigencia de una contraseña para acceder al programa

PERFIL

Indica si dependiendo del usuario que se valida en el programa se restringen los datos a los que tiene acceso

ALMACENAMIENTO EN PAPEL

OBSERVACIONES

Explicación de las características generales del sistema de almacenamiento de datos en formato papel.

UBICACIÓN

Lugar donde se almacena.

TIPO RECURSO

Clasificación del recurso: carpeta, archivador, etc.

PERSONAL AUTORIZADO

Personal autorizado para manejar este recurso.

NIVEL DE SEGURIDAD

Indicación del nivel de seguridad que se debe aplicar.

INFORMACIÓN QUE CONTIENE

Tipo de datos almacenados en ese soporte.

EQUIPOS

NOMBRE EQUIPO

Nombre con el que se identifica al terminal dentro de la red, en su defecto anotar el usuario asignado.

SISTEMA OPERATIVO

Sistema operativo, para saber si puede implementar las medidas técnicas suficientes al nivel exigido.

Descripción del sistema

CONTROL DE ACCESO

Copias de llaves	✓	Control de acceso a instalaciones	
Alarma		Tipo de control de acceso	
Rejas		Control de acceso a servidores	✓
Videoportero		Armarios con llaves	✓
Cámaras/videovigilancia			
Empresa videovigilancia			
Tiempo conservación imágenes			
Usuarios/as autorizados/as			

HARDWARE

Impresoras compartidas	✓	Servidor	✓
Bloqueo de impresión		Sai en servidores	✓
Destrucción de papel	Destructora	Sai en equipos	

SOFTWARE

Contraseñas en equipos	✓	Datos de red	
Contraseñas en programas	✓	Antivirus	Si
Complejidad contraseñas	Alfanumérica	Firewall	✓
Caducidad de las contraseñas	180 días	Restricción de permisos en sistema	✓
Longitud contraseñas	8 Caracteres	Registro de acceso en sistema	✓
Límite de intentos contraseñas	5	Alerta de errores o accesos	
Cifrado de datos		Bloqueo de sesión en sistema	
Firma electrónica			

OTROS

Auditorías internas		Certificación ISO 27001	
Plan de contingencia		Pseudonimización / anonimización	
Registro de acceso/entrada/salida de documentos		Autorización para copias de documentos	

Software / programas informáticos

NOMBRE DEL PROGRAMA	BD COLEGIADOS
Tipo de programa	Base de datos
Descripción de tipo de programa	Software de almacenamiento de datos
Tipo de acceso	
Descripción del tipo de acceso	
Contraseña	
Perfiles de usuario/a	
Observaciones	BASE DE DATOS EN ACCESS PARA EL CONTROL DE LOS COLEGIADOS

NOMBRE DEL PROGRAMA	CONTANET
Tipo de programa	Contabilidad
Descripción de tipo de programa	Programa para generar y gestionar la contabilidad
Tipo de acceso	En el equipo
Descripción del tipo de acceso	El acceso a la aplicación está restringido al terminal donde se ha instalado.
Contraseña	✔
Perfiles de usuario/a	✔
Observaciones	

Almacenamiento en papel

NOMBRE DE ARCHIVO	Armario cerrado
Descripción	Facturas, recibos y tickets emitidos
Ubicación	Instalaciones principales- oficina
Nivel de seguridad	Medio
Protegida	
Actividades de tratamiento	

NOMBRE DE ARCHIVO	Armario cerrado
Descripción	Laboral: nóminas y contratos de los empleados
Ubicación	Instalaciones principales- oficina
Nivel de seguridad	Medio
Protegida	
Actividades de tratamiento	

NOMBRE DE ARCHIVO	Armario cerrado
Descripción	Facturas, recibos y tickets recibidos y remesas de pago
Ubicación	Instalaciones principales - oficina
Nivel de seguridad	Medio
Protegida	
Actividades de tratamiento	

NOMBRE DE ARCHIVO	Armario cerrado
Descripción	Documentación legal y jurídica: contratos, escrituras, autorizaciones...
Ubicación	Instalaciones principales - oficina
Nivel de seguridad	Medio
Protegida	
Actividades de tratamiento	

NOMBRE DE ARCHIVO	Armario cerrado
Descripción	Documentación varia
Ubicación	Instalaciones principales - oficina
Nivel de seguridad	Medio
Protegida	
Actividades de tratamiento	

NOMBRE DE ARCHIVO	Armario cerrado
Descripción	Datos de los Colegiados/as
Ubicación	Instalaciones principales - oficina
Nivel de seguridad	Medio
Protegida	
Actividades de tratamiento	

Hardware / equipos informáticos

NOMBRE DEL EQUIPO	SERVIDOR
Procesador	
Sistema operativo	Windows Server 2003
Fecha de alta	2021-01-11
Fecha de baja	
Usuario/a asignado/a	
Observaciones	

NOMBRE DEL EQUIPO	TERMINAL 1
Procesador	
Sistema operativo	Windows 10 Profesional
Fecha de alta	2021-01-11
Fecha de baja	
Usuario/a asignado/a	
Observaciones	

NOMBRE DEL EQUIPO	TERMINAL 2
Procesador	
Sistema operativo	Windows 10 Profesional
Fecha de alta	2021-01-11
Fecha de baja	
Usuario/a asignado/a	
Observaciones	

NOMBRE DEL EQUIPO	TERMINAL 3
Procesador	
Sistema operativo	Windows 10 Profesional
Fecha de alta	2021-01-11
Fecha de baja	
Usuario/a asignado/a	
Observaciones	

ANEXO II

Brechas de seguridad que afectan a los datos

1. Se ha confeccionado un impreso de registro de BRECHAS DE SEGURIDAD que obra a disposición de todos los usuarios con acceso a los tratamientos de datos con el fin de que quede debidamente registrada cualquier brecha de seguridad que al producirse haya puesto en peligro o haya dañado los ficheros de datos.
2. El usuario que tenga conocimiento de la brecha de seguridad se responsabiliza directa y personalmente de notificarla para que el responsable de privacidad pueda registrarla en el citado impreso.
3. El responsable de privacidad tomará de inmediato las medidas oportunas para que, en el menor tiempo posible, se subsane la anomalía que haya generado la brecha de seguridad.
4. El responsable de privacidad entregará los impresos de registro cumplimentados al responsable del tratamiento, el cual los conservará numerados correlativamente. Se anotará esa brecha de seguridad además en el cuadro de control de BRECHAS DE SEGURIDAD.
5. No registrar una brecha de seguridad de la que se haya tenido conocimiento, o no entregar el impreso cumplimentado al responsable, será considerado una falta contra la seguridad de los ficheros que podrá constituir quebranto de la buena fe contractual.
6. En caso de que la brecha de seguridad afecte a datos de los cuales se es encargado de tratamiento se le comunicará al responsable del tratamiento en un lenguaje claro y sencillo y deberá incluir los elementos que en cada caso señale el responsable de privacidad, como mínimo.
    - La naturaleza de la violación de datos.
    - Datos del punto de contacto del responsable o del encargado donde se pueda obtener más información.
    - Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
    - Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

    En este caso valdría incluir el formulario que se indica a continuación acompañado con la información del punto 6.b

1. Se notificará a la Agencia Española de Protección de Datos dicha brecha de seguridad en el conforme lo marcado en la norma a **menos que sea improbable que la violación suponga un riesgo** para los derechos y libertades de los afectados
    - Notificación de brechas de seguridad en **menos de 72 horas:**
        - La naturaleza de la violación
        - Categorías de los datos y de interesados afectados
        - Medidas adoptadas por el responsable para solventar la quiebra
        - Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados
        - La AEPD debe decidir en qué casos también es necesario notificar la quiebra a los afectados.

La Agencia Española de Protección de datos pone a disposición de los Responsables de tratamiento una herramienta para evaluar si una brecha de seguridad debe ser comunicada a los titulares de los datos

Se puede acceder en el siguiente enlace:

https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

Al final de este anexo dispone de un formulario que le puede servir de guia a la hora de notificar a la AEPD una brecha

Naturaleza de las brechas de seguridad

I. BRECHAS DE SEGURIDAD QUE AFECTAN A LA CONFIDENCIALIDAD

- **Lectura no autorizada de la información contenida en los ficheros o sistemas de información.**
  - Por parte del personal informático de la organización.
  - Por parte de otras personas de la organización.
  - Por parte de personas ajenas a la organización.
- **Copia no autorizada de la información.**
  - Por parte del personal informático de la organización.
  - Por parte de otras personas de la organización.
  - Por parte de personas ajenas a la organización.
- **Error en la distribución de Informes o Soportes.**
- **Obtención de información desde soportes desechados.**
- **Obtención de información desde equipos o soportes destinados a la reutilización.**
- **Descifrado de la información.**
  - Por descubrimiento de claves.
  - Por conocimiento directo de las claves.

II. BRECHAS DE SEGURIDAD QUE AFECTAN A LA INTEGRIDAD

- **Modificación no autorizada de la información directamente de los Ficheros o Sistemas de Información.**
  - Por parte de otras personas de la organización.
  - Por parte de personas ajenas a la organización.
- **Borrado no autorizado de la información.**
  - Por parte del personal informático de la organización.
  - Por parte de otras personas de la organización.
  - Por parte de personas ajenas a la organización.
- **Destrucción total o parcial de la información**.
  - Por fallos en los equipos.
  - Por fallos en las instalaciones ocasionados por desastres naturales.
- **Imposibilidad de reconstruir los datos, partiendo de las correspondientes Copias de Respaldo.**
- **Alteración o borrado de la información durante su tratamiento.**
  - Por fallos ocasionados en las Aplicaciones Informáticas.
  - Por fallos ocasionados en los Sistemas Operativos.
  - Por fallos ocasionados por el mal funcionamiento del Hardaware

III. BRECHAS DE SEGURIDAD QUE AFECTAN A LA DISPONIBILIDAD

- **Modificaciones no autorizadas de permisos de acceso lógico a los ficheros.**
- **Imposibilidad o limitación del uso de las instalacione**s.
  - Por fenómenos meteorológicos.
  - Por huelgas o manifestaciones
  - Por otros motivos.
- **Indisponibilidad de los sistemas informáticos.**
  - Por virus.
  - Por defectos de software.

- Por defectos de hardware.
- Por intrusiones (internas o externas).

IV. BRECHAS DE SEGURIDAD QUE AFECTAN A LA AUTENTICACIÓN

- Suplantación del usuario autorizado.
  - Por cesión de la clave de acceso.
  - Por conocimiento de la clave de acceso.
  - Por violación de los controles de acceso.
- Fallos en los programas o dispositivos de control de acceso lógico.
- Fallos de gestión de los controles de autenticación.
  - Por bajas no comunicadas de usuarios del sistema.
  - Por autorizaciones de acceso improcedentes.

Registro de brecha de seguridad

NÚMERO DE BRECHA		
Fecha	**Hora**	**Nº de afectados**

Naturaleza de la brecha de seguridad				
INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	AUTENTICACIÓN	OTRA

Categoría de datos afectados	

Descripción de la brecha de seguridad

Consecuencias de la brecha de seguridad

Medidas propuestas y/o adoptadas para su corrección

Persona que notifica la brecha de seguridad

Firma de la persona que notifica la brecha	**Firma del responsable de seguridad**

FORMULARIO NOTIFICACIÓN BRECHAS DE SEGURIDAD

Datos del recibo de presentación (se cumplimenta en la presentación telemática, con el certificado digital)

Oficina:

Fecha y hora de registro en:

Fecha presentación:

Número de Registro:

Tipo de documentación física: Documentación adjunta digitalizada

Interesado

CIF Razón Social

Pais Municipio

Provincia Dirección

Código Postal Correo

D.E.H Observaciones

Información del registro

Tipo Asiento

Resumen/ Asunto

Unidad de tramitación

Adjuntos (para aportar documentos extras)

Nombre Lo rellena automáticamente

Tamaño (Bytes) Lo rellena automáticamente

Validez

Tipo

CSV Lo rellena automáticamente

Hash Lo rellena automáticamente

Observaciones

Formulario Presentación

Título

Primera notificación o notificaciones sucesivas

¿Cual es su intención?

Sobre el tratamiento

¿Desde cuándo se viene realizando este tratamiento de datos?

Número aproximado de personas físicas sobre las que recoge, almacena o trata datos personales de otra forma; referido exclusivamente al tratamiento sobre el que se ha producido la brecha de datos personales:

El tratamiento sobre el que se ha producido la brecha incluye datos de personas

Sobre el tratamiento (incidente)

El incidente ha sido

El origen del incidente ha sido

¿Que pude haber ocurrido?Puede seleccionar varias opciones

Como consecuencia del incidente, se ha visto afectada la:

Referido específicamente a los datos afectados por la brecha de confidencialidad. ¿Están los datos cifrados de forma segura, anonimizados o protegidos de forma que son ininteligibles para quien haya podido tener acceso o no se puede identificar a las personas?

¿Que pude haber ocurrido?Puede seleccionar varias opciones

¿En qué grado podrían afectar las consecuencias identificadas a las personas físicas?

A fecha de esta notificación, ¿tiene constancia de que se hayan materializado alguno de los daños identificados, con el grado indicado en la cuestión anterior?

Como valora la probabilidad de que el daño anterior se materialice sobre las personas afectadas con la severidad indicada

*** Introduzca una breve descripción de lo ocurrido.** Evite incluir datos personales, fórmulas del tipo "Ver anexo" y en ningún caso lo aquí escrito podrá suponer una modificación sobre lo consignado en el resto del formulario.

Tipos de datos afectados

Seleccione los tipos de datos que se han visto afectados, exclusivamente de personas físicas, marque todas las opciones aplicables

Perfil de los afectados, referido exclusivamente a personas físicas

Entre las personas afectadas, hay menores:

Entre las personas afectadas, ¿hay miembros de colectivos vulnerables como supervivientes de violencia de género o en riesgo de exclusión social?

Las personas afectadas tienen los siguientes perfiles

En total, ¿cuántas personas han visto sus datos afectados por la brecha de datos personales? (Si desconoce el valor exacto, indique un valor aproximado)

¿Hay personas afectadas por la brecha en otros estados miembro de la UE?

Información temporal de la brecha

Indique la fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene la certeza de que se han visto afectados datos personales

¿Conoce la fecha en la que se inició la brecha?

Indique la fecha de inicio de la brecha

La brecha se ha detectado mediante:

Medidas de seguridad antes de la brecha

Marque las medidas de seguridad implementadas en la organización antes del suceso de la brecha (Deberá poder acreditar las medidas marcadas ante un eventual requerimiento de la autoridad de control)

¿Se podría haber evitado la brecha adoptando alguna medida de seguridad adicional?

¿Se ha producido el incidente por algún fallo deficiencia o inclumplimiento de medidas de seguridad implementadas?

¿Dispone de un análisis de riesgos documentado que justifique las medidas de seguridad adoptadas previamente al incidente?

Acciones tomadas tras el incidente

¿Ha actualizado su registro de incidentes con la información de esta brecha de datos personales?

¿Ha adoptado tras el incidente nuevas medidas de seguridad que podrían haber evitado la brecha?

¿Ha adaptado / mejorado sus procedimientos y políticas de seguridad?

Marque exclusivamente las nuevas medidas de seguridad y las que se hayan actualizado

¿Ha puesto el incidente en conocimiento de las autoridades policiales / judiciales por considerar que es constitutivo de delito?

¿Considera que ha tomado todas las acciones posibles y da por resuelta la brecha?

Comunicación a los afectados por la brecha de datos personales

¿Se ha comunicado la brecha a las personas afectadas en las condiciones anteriormente descritas?

A más tardar, las personas afectadas serán informadas en la siguiente fecha:

Medio por el que se informará

Delegado de Protección de Datos

¿Tiene designado un DPD el responsable del tratamiento?

NIF/NIE

Nombre

Apellidos

Cargo

Dirección

País

Localidad

Código Postal

Provincia

Correo electrónico

Responsable del tratamiento 1

Indique el tipo de organización

Tipo de organización

Sector de actividad del responsable del tratamiento

Nombre de la Organización

Nº Identificativo (NIF u otro)

Dirección

País

Código Postal

Provincia

Localidad

Correo electrónico

Encargado del tratamiento

¿Hay implicado un encargado del tratamiento?

Tipo de organización

Nombre de la organización

NIF

Calle

Número

País

Código Postal

Provincia

Localidad

Introducir el correo electrónico del Encargado del Tratamiento

Enviar su notificación de brecha de datos personales

Marque la opción más adecuada a la situación del responsable en el momento de esta notificación:

Cláusula informativa

Declaraciones

DECLARO que los datos consignados en esta notificación de brecha de datos personales son ciertos y que no se ha omitido ni falseado información siendo fiel expresión de la verdad, asumiendo las obligaciones y responsabilidades que se derivan de la misma. Asimismo, que he leído la cláusula informativa que se expone a continuación.

Cláusula informativa sobre datos de carácter personal

Los datos de carácter personal serán tratados por la Agencia Española de Protección de Datos e incorporados a la actividad de tratamiento: Gestión de brechas de datos personales , cuya finalidad es la gestión y evaluación de la notificación de violación de seguridad.
Finalidad basada en el ejercicio de potestades públicas conferidas a la Agencia Española de Protección de Datos por el Reglamento General de Protección de Datos y la Ley General de Telecomunicaciones.
Los datos personales podrán ser comunicados al CERT (Computer Emergency Response Team) del Centro Criptológico Nacional, a las Fuerzas y Cuerpos de Seguridad del Estado, al Comité Europeo de Protección de Datos, a las Autoridades de Protección de Datos de la Unión Europea, y a la red de equipos de respuesta a incidentes de seguridad informática («red de CSIRT», por sus siglas en inglés de «computer security incident response teams»), creada por la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
Los datos serán conservados durante el tiempo necesario para cumplir con la finalidad para la que se han recabado y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación la normativa de archivos y patrimonio documental español.

Para solicitar el acceso, la rectificación, supresión o limitación del tratamiento de los datos personales o a oponerse al tratamiento, en el caso de se den los requisitos establecidos en el Reglamento General de Protección de Datos, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personal y garantía de los derechos digitales, puede dirigir un escrito al responsable del tratamiento, en este caso, la AEPD, dirigiendo el mismo a la Agencia Española de Protección de Datos, C/Jorge Juan, 6, 28001- Madrid o en el registro electrónico de la AEPD
Datos de contacto del DPD: dpd@aepd.es

ANEXO III
Procedimiento para la realización y recuperación de copias de seguridad

1. El responsable del tratamiento se encargará de verificar, contando con la colaboración del responsable de privacidad, la correcta aplicación de los procedimientos utilizados para la realización de copias de seguridad y recuperación de datos.
2. Los procedimientos de realización de copias de seguridad o recuperaciones de datos garantizarán, en la máxima medida posible, la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida.
3. **Las copias de seguridad se realizarán sobre soporte extraíble y con periodicidad mínima semanal.** Este plazo sólo podrá ampliarse en el caso de que en el citado período no se haya producido ninguna actualización o modificación de los datos.
4. No obstante la frecuencia mínima señalada en la norma anterior, se realizarán copias de seguridad adicionales previamente a la realización de cualquier intervención técnica en los recursos informáticos (p.e.: instalación o actualización de aplicaciones, instalación o sustitución de hardware, reparaciones, etc.).
5. Antes de proceder al almacenamiento de la copia de seguridad, se verificará que se ha realizado correctamente y sin ninguna incidencia, para lo cual se recomienda utilizar una herramienta de copias de seguridad que genere un informe final.
6. Todo programa o aplicación utilizada para el tratamiento de datos personales deberá proveer la función de realización de copias de seguridad, o bien permitir el almacenamiento de la informacion de tal forma que se garantice la recuperación de datos en los términos expuestos en las normas precedentes. (rutas concretas de almacenamiento de archivos)
7. Todo procedimiento de recuperación de datos deberá ser realizado por personal con los necesarios conocimientos técnicos.

   En el caso de que dicho procedimiento sea realizado por personal externo, el responsable de privacidad verificará que durante su ejecución se mantenga la más estricta confidencialidad sobre los datos de carácter personal obrantes en los ficheros.
8. Dicha recuperación debe **ser autorizada** expresamente por el responsable del tratamiento, mediante la ficha que se adjunta en esta documentación, siempre y cuando no se den los siguientes precedentes:
   - la recuperación de datos eliminados se encuentra entre los permisos habilitados al usuario/a
   - la recuperación de datos es realizada expresamente por el responsable de privacidad o informática, y ya existe un canal de comunicación para solicitar estas recuperaciones.

1. El sistema de backup no es del todo completo si no se incluye cierta rutina de trabajo, con una completa documentación y gestión de la copia de seguridad, que obtenga toda la potencia de esta herramienta de seguridad.
2. El sistema de copia de seguridad debe ser verificado como mínimo cada 6 meses, comprobando la integridad del dispositivo y la posibilidad de la correcta recuperación de datos. El responsable de establecer los métodos de prueba.

PROCEDIMIENTO PARA COPIAS DE SEGURIDAD

1. Planificación de las copias de seguridad.
2. Documentar cuando se debe hacer la copia de seguridad:
   - nombre del proyecto de copia de seguridad y si será diferencial o incremental.
   - También se debe indicar el responsable de realizarla.
   - Soportes para las copias de seguridad: se debe indicar el tipo de soporte donde realizamos la copia de seguridad.
   - Origen y destino de los datos.

1. Garantizar que la copia de seguridad dispone de un sistema para impedir la apertura y acceso a la información no autorizada.
2. Almacenar la copia de seguridad en un lugar seguro, si no se almacena fuera de las instalaciones lo recomendado sería armarios ignífugos.
3. Destruir los soportes cuando se acabe su ciclo de vida, mediante un borrado seguro.
4. Supervisar el estado de los soportes, debido a la frecuencia o número de veces utilizado: cambiarlo cuando se detecten fallos o lentitud de acceso.
5. Comprobar cada **6 meses** que el sistema de copia y respaldo funciona. Utilizar la correspondiente ficha para documentar tal prueba.

Realización de copias de seguridad

NOMBRE DE LA COPIA	PRINCIPAL
Descripción	2 UNIDADES ALTERNATIVAS SEMANALMENTE. (ALMACENADAS EN DEPENDENCIAS SEPARADAS).
Tipo de copia	
Descripción tipo de copia	
Periodicidad	Diaria
Responsable de la copia	
DNI del responsable	
Origen de los datos	SERVIDOR
Destino de los datos	DISCO DURO EXTERNO
Protegida	✔
Genera informe	
Fuera de las instalaciones	

NOMBRE DE LA COPIA	SECUNDARIA
Descripción	QUE LO ALMACENE LA GERENTE
Tipo de copia	
Descripción tipo de copia	
Periodicidad	Semanal
Responsable de la copia	
DNI del responsable	
Origen de los datos	SERVIDOR
Destino de los datos	DISCO DURO EXTERNO
Protegida	
Genera informe	
Fuera de las instalaciones	✔

Recuperación de copia PRINCIPAL

NOMBRE DE LA COPIA	PRINCIPAL
Descripción	2 UNIDADES ALTERNATIVAS SEMANALMENTE. (ALMACENADAS EN DEPENDENCIAS SEPARADAS).
Tipo de copia	
Descripción tipo de copia	
Periodicidad	Diaria
Responsable de la copia	
DNI del responsable	
Protegida	✔
Genera informe	
Fuera de las instalaciones	
Origen de los datos	DISCO DURO EXTERNO
Destino de los datos	
Fecha de última copia	
Fecha de la recuperación	
Datos manuales	
Origen datos manuales	
Observaciones	

FIRMA DEL RESPONSABLE DE SEGURIDAD	FIRMA DEL RESPONSABLE DE LA COPIA

Recuperación de copia SECUNDARIA

NOMBRE DE LA COPIA	SECUNDARIA
Descripción	QUE LO ALMACENE LA GERENTE
Tipo de copia	
Descripción tipo de copia	
Periodicidad	Semanal
Responsable de la copia	
DNI del responsable	
Protegida	
Genera informe	
Fuera de las instalaciones	✔
Origen de los datos	DISCO DURO EXTERNO
Destino de los datos	
Fecha de última copia	
Fecha de la recuperación	
Datos manuales	
Origen datos manuales	
Observaciones	

FIRMA DEL RESPONSABLE DE SEGURIDAD	FIRMA DEL RESPONSABLE DE LA COPIA

ANEXO IV Procedimiento para la gestión de soportes y otros recursos informáticos

Estas medidas tienen por objetivo identificar los activos de la organización y definir las responsabilidades de protección sobre los mismos. Esto incluye desde la realización de un inventario, hasta la definición de los usos aceptables. Igualmente la gestión de activos incluye la clasificación de la información y la gestión de soportes.

IDENTIFICACION DE ACTIVOS

La gestión de los activos de una organización es uno de los aspectos más complicados y a la vez más claves en un departamento de informática. Son muchos los activos que gestionamos en una empresa (ordenadores personales, teléfonos móviles corporativos, tabletas, portátiles, proyectores, servidores, aplicaciones software, monitores, periféricos, etc.). Por ello es necesario que realicemos y mantengamos actualizado un inventario en el que los activos se encuentren clasificados y gestionados de la manera correcta.

Para la gestión del ciclo de vida completo de los activos debemos incluir dentro del inventario:

- identificador interno del activo;
- características básicas;
- clasificación de seguridad, si aplica;
- responsable del activo;
- proveedor, garantía y datos de mantenimiento;
- ubicación física;
- fecha de destrucción cuando sea el caso.

CLASIFICACIÓN DE LA INFORMACIÓN

Atendiendo a la importancia de los distintos activos de información para la empresa se ha de llevar a cabo una clasificación que permita aplicar a la misma las medidas de seguridad oportunas.

Para la clasificación se pueden considerar, además de su antigüedad y valor estratégico, las tres propiedades: confidencialidad, integridad y disponibilidad.

Lo más usual es clasificar la información teniendo en cuenta solamente una de estas tres dimensiones, la confidencialidad. Se clasifica la información en tres niveles: confidencial, de uso interno e información pública. Esta aproximación es la más aceptada pues uno de los riesgos más críticos para cualquier negocio es la fuga de información [4] que no es más que una pérdida de la confidencialidad de la misma.

Es importante identificar toda la información que se maneja, incluido el software, sin importar el soporte o su formato. Se ha de registrar su ubicación y la persona o equipo responsable y clasificarla según los criterios de seguridad que sean más adecuados, incluidas las

necesidades de cumplimiento legal que sean aplicables, según la actividad de la empresa. Esta clasificación será esencial para aplicar las medidas de seguridad adaptadas a la criticidad de cada «clase» de información para el negocio.

Una vez clasificada, aplicaremos las medidas necesarias para su protección. Estas medidas, que se concretarán en distintas políticas, se dirigen a definir:

- ubicaciones y dispositivos permitidos para el almacenamiento y uso de la información según su criticidad;
- cifrado de información crítica en tránsito o en almacenamiento;
- control de acceso a la información almacenada y a los servicios y programas para su tratamiento; permisos por roles, contraseñas robustas, etc.;
- control de uso de dispositivos externos de almacenamiento y de móviles o tabletas;
- control del uso de almacenamiento y servicios en la nube;
- destrucción segura de la información una vez terminada su vida útil;
- copias de seguridad y planes de recuperación;
- según la actividad de la empresa, archivado seguro de la información que se deba conservar y de los registros de actividad como

garantía del cumplimento legal o normativo que aplique.

GESTION DE RECURSOS

La gestión de soportes persigue evitar que se revele, modifique, elimine o destruya de forma no autorizada la información almacenada en los mismos.

Para ello el departamento de TI debe implantar procedimientos para la gestión de los soportes extraíbles, su eliminación y su protección frente a usos indebidos.

Debemos prestar especial atención los activos móviles usados en la organización. Estos dispositivos pueden almacenar información confidencial de la empresa y tienen una alta probabilidad de pérdida o de sufrir un robo.

Por ello deberán estar etiquetados e inventariados indicando como mínimo:

- tipo y marca del dispositivo;
- persona asignada al dispositivo;
- número de serie;
- dirección MAC si la tiene;
- tipo de uso.

ASIGNACIÓN DE: SOPORTE / RECURSO INFORMÁTICO

DATOS DE USUARIO	
NOMBRE Y APELLIDOS	
DNI	
EMPRESA	
FUNCION	

DATOS DEL RECURSO				
TIPO	DESCRIPCIÓN	ENTREGA	DEVOLUCION	CANTIDAD

DATOS DE INFORMACION (en el caso de memorias)	
ORIGEN DATOS	
DESTINO DATOS	
TIPO INFORMACIÓN	

OBSERVACIONES:

Condiciones de uso

- Debe garantizarse que los dispositivos tienen contraseña / pin de acceso seguros, en el caso de memorias deben ir encriptadas.
- El usuario es responsable del buen estado y conservación del recurso.
- El material y/o equipo entregado se destinará al desempeño de las funciones propias del puesto para los que el usuario autorizado ha sido contratado.
- El referido material deberá ser devuelto a la empresa en el momento de finalización de la relación laboral/mercantil establecida entre la empresa y el usuario.
- El usuario se compromete a utilizar y conservar el material entregado conforme a las exigencias de la normativa de LOPD y con la diligencia debida en el desempeño de sus funciones.
- **Es obligatorio conservar las cajas del material entregado hasta la devolución del mismo**, sobre todo en el caso de los móviles, los cuales tendrán que venir con todo lo suministrado (funda, cargador, cable de carga y auriculares si es el caso).
- **El material no podrá ser entregado hasta que este parte esté debidamente firmado por el destinatario y devuelto al remitente (RESPONSABLE TIC).**

En a de del

(FIRMA RESPONSABLE TI)	(FIRMA USUARIO/A)