Política de tratamiento de datos personales en ERCROS S.A.

Tratamiento de datos de carácter personal en ERCROS S.A.

INFORMACIÓN DEL DOCUMENTO	
Nombre del documento	Política de tratamiento de datos personales en ERCROS S.A.

REGISTRO DE REVISIONES		
Versión	**Fecha**	**Resumen y motivos de la modificación**
1.0	03-03-2019	Versión inicial

ÍNDICE DE CONTENIDOS

1. Introducción

El objetivo de este documento es *definir las directrices generales de seguridad de la información en el tratamiento y almacenamiento de datos de carácter personal* sobre la sociedad ERCROS S.A.

Afecta a directrices tanto técnicas como administrativas en el tratamiento de información de clientes, proveedores, empleados, usuarios de sistemas de información, personal con acceso a datos, y en general cualquier otra persona identificable cuyos datos personales estén contenidos en sistemas de información y/o locales de tratamiento de la organización en sus dependencias o bien de terceros cuya responsabilidad y finalidad sea otorgada a la sociedad ERCROS S.A.

De la misma manera afecta a todos aquellos tratamientos de los que la organización bien sea RESPONSABLE DEL TRATAMIENTO o bien ENCARGADO, (aquellos relacionados directamente con la prestación de los diferentes servicios que puede realizar la organización)

La responsabilidad manifestada desde la dirección en ERCROS S.A. se basa en los siguientes puntos relevantes que marcan el contenido de dicho documento

1. Identificación legal de los requerimientos.
2. Establecimiento de principios relativos a los datos personales y los niveles de seguridad objetivos según la naturaleza de los mismos.
3. Establecimiento mediante políticas, procedimientos e instrucciones técnicas de las medidas de seguridad que garanticen el nivel de seguridad objetivo.
4. Direccionamiento, concienciación y formación a usuarios, empleados y terceras partes que accedan a información de la cual las sociedades son responsables
5. Dotar de una infraestructura de recursos para poder implementar el programa integral
6. Evaluación, análisis y mejora continua de los procesos y controles establecidos.
7. Comunicación a las partes interesadas de los logros y metas alcanzados por el sistema de gestión

Este documento, como política y conjunto de directrices inicial sobre el tratamiento de datos de carácter personal, marca el nivel de seguridad que la sociedad ERCROS S.A. define para toda su organización, denominado en este documento como *nivel de seguridad base*, de manera el presente documento contiene la base de mínimos construida a partir de los requerimientos legales aplicables a la organización.

2. Alcance jurídico

Además, dicha política está también dirigida a proveedores y otras terceras partes de dichas organizaciones que presten servicios o productos que traten datos de carácter personal, y que deberán tener en cuenta para la definición y despliegue de los mismos a la organización.

La dirección de la organización será la encargada de asegurar y velar por la actualización de esta política y dirigirla hacia el personal apropiado, así como a terceros, en el caso que se necesario.

El presente documento de seguridad tiene como alcance los tratamientos declarados en el registro de actividades de ERCROS S.A., aquellos en los que la organización es responsable del tratamiento o bien encargado de tratamiento.

3. Referencias legales y normativas

- 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 (Reglamento general de protección de datos)
- Ley Orgánica de Protección de datos y garantía de derechos digitales, Ley 3/2018 de 5 de diciembre.

4. Definiciones

1. **Datos de carácter personal**, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
2. **Data Privacy**. Concepto que engloba a la protección de datos de carácter personal (confidencialidad, disponibilidad e integridad de la información que contenga datos de carácter personal)
3. **Tratamiento de datos**, Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
4. **Niveles de seguridad base.** Nivel de seguridad que se establece para los ficheros, sistemas de información y locales de tratamiento, en función del contenido en sus bases de datos y ficheros documentales y del tratamiento que se realice sobre los mismos.
5. **Responsable del fichero o tratamiento**, Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento de datos.
6. **Responsable de seguridad**, Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
7. **Persona identificable:** toda persona cuya identidad puede determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
8. **Derechos ARSOLP**: Son los derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento y portabilidad.

9. **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
10. **Responsable del activo de información:** según inventario de activos, el responsable interno del fichero.
11. **Encargado de Tratamiento**, Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
12. **Comunicación de datos** se considera comunicación de datos cualquier salida, entrega o acceso a datos por parte de un tercero, independientemente del medio de acceso o entrega, considerando como tercero cualquier entidad pública o privada y en particular, considerando como tercero a otras empresas del grupo."

    En el marco de las comunicaciones de datos que contengan datos de carácter personal (ligados al cumplimiento de la LOPD), se distinguen 2 tipos de supuestos con diferentes implicaciones legales:

    - **Prestación de servicios:** entrega o acceso de datos por parte de un tercero con la única finalidad de prestar un servicio por cuenta del Responsable del Fichero y conforme a las instrucciones dictadas por el mismo.
    - **Cesión de datos:** tratamiento de datos que supone su revelación a una persona distinta del interesado, cuando no concurran las características relativas a la prestación de servicios.
13. **Cesionario de los datos:** persona o entidad distinta del Responsable del Fichero a la que éste le revela datos para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y cesionario, en el marco de una cesión de datos.
14. **Sub-Encargado del Tratamiento:** persona o entidad que, sólo o conjuntamente con otros, trata datos personales por cuenta del Responsable del Encargado de tratamiento, como consecuencia de la existencia de relación jurídica que le vincula con el mismo y delimita su ámbito de actuación para la prestación de un servicio. (Estudios jurídicos AGPD)
15. **Aviso o política de Privacidad.** Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con los requerimientos legales relacionados con el deber de información.
16. **Disociación**: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.
17. **Medidas de seguridad administrativas:** Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.
18. **Medidas de seguridad físicas**: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados a preservar la confidencialidad, integridad y disponibilidad de la información.
19. **Medidas de seguridad técnicas**: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar la confidencialidad, integridad y disponibilidad de la información.

5. Principios de Protección de Datos Personales

a) **Licitud, lealtad y transparencia**. Los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.

b) **Limitación de la finalidad**. Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

c) **Minimización de datos**. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

d) **Exactitud**. Los datos personales deben ser exactos y, si fuera necesario, actualizados; se adoptarán 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.

e) **Limitación del plazo de conservación.** Los datos personales deben ser 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; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

f) **Seguridad**. Los datos personales deben ser 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 medidas técnicas u organizativas apropiadas.

6. Transparencia y deber de información hacia el interesado

a) **Deber de informar**. Los datos de carácter personal serán tratados de forma que se informe al afectado de la finalidad del tratamiento y de la identificación de responsables o responsables del tratamiento, de sus finalidades, del tiempo de retención o del criterio de archivo, de posibles cesiones, de posibles transferencias internacionales, de la posibilidad de reclamación y de los datos, si procede, del delegado de protección de datos. Estos mecanismos de información deben articularse mediante avisos legales, políticas o declaraciones de privacidad.

b) **Transparencia**. ERCROS S.A. tomará las medidas oportunas para facilitar al interesado toda la información indicada sobre el deber de información, de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

c) **Derechos de los afectados**. Los avisos de privacidad y las políticas de protección de datos deben permitir los ejercicios de los derechos de acceso, rectificación supresión, oposición, limitación al tratamiento y portabilidad. Los derechos se deben informar de manera sencilla y gratuita para los afectados. Para establecer estos ejercicios deberán desarrollarse controles de seguridad mediante normativas o procedimientos que direccionen hacia las partes interesadas la necesidad y la operativa de establecer textos legales de deber de información y sistemas y operativas técnicas para llevarlas a cabo. Los sistemas de información y procedimientos internos para operar dichos ejercicios deben definirse y desplegarse con la mayor homogeneidad e integración posibles dentro de la organización, de manera que se minimicen los riesgos de incumplimiento de los mismos.

7. Datos especialmente protegidos

Se entiende por datos especialmente protegidos aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, el tratamiento de datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, y los datos relativos a la salud o datos relativos a la vida sexual o la orientación sexuales de una persona física.

Se debe justificar la base jurídica de dichos tratamientos y desarrollar medidas de seguridad técnicas y organizativas para garantizar la confidencialidad y la integridad de los tratamientos, tanto en sistemas de información, en locales de tratamiento como en los procesos internos y con terceras partes. En los procesos de se deberá considerar estos tratamientos de manera particular.

8. Protección de datos desde el diseño y por defecto

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, ERCROS S.A. aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, de manera interna o direccionado hacia sus proveedores medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

ERCROS S.A. aplicará las medidas técnicas, organizativas y físicas apropiadas 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. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizaran en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

8.1 Registro Actividades de Tratamiento

Como base inicial del desarrollo de medidas técnicas y organizativas y como resultado del proceso de gestión de riesgos es necesario realizar y actualizar un registro de actividades de tratamientos a modo de inventario de datos personales de la organización. El registro de actividades debe elaborarse sobre la información que se realiza tanto como responsable como encargado de tratamiento, documentado como mínimo la finalidad, la base jurídica del tratamiento, las categorías de datos, los tipos de datos personales, las categorías de los destinatarios, las cesiones y transferencias y la información sobre la localización física de los datos y las medidas de seguridad asociadas al tratamiento.

Deberá definirse la operativa interna para la elaboración, mantenimiento de dicho registro de actividades.

8.2 Análisis de Riesgos

Se deben evaluar los riesgos para la seguridad de los datos personales que se tratan, adoptando de forma responsable y proactiva todas las pertinentes medidas para evitar y paliar los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas concernidas considerando para

ello, el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines de tratamiento.

En este proceso hay que identificar amenazas y/o vulnerabilidades, evaluar los riesgos y tratar los riesgos. El análisis de estos riesgos no sólo hay que abordarlo en un momento posterior a la puesta en marcha del producto, servicio o tratamiento que corresponda por parte de ERCROS S.A. De hecho, lo ideal en consonancia con los principios de privacidad desde el diseño y por defecto es abordarlos desde el mismo momento de la proyección de tal producto, servicio o tratamiento.

8.3 Análisis de impacto en la protección de datos

Deberá realizarse una evaluación de impacto relativa a la protección de los datos cuando exista un tratamiento que cumpla cualquiera de los siguientes supuestos:

- Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.
- Cuando se realice evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
- Cuando se realice un tratamiento a gran escala de las categorías especiales de datos a, o de los datos personales relativos a condenas e infracciones penales.
- Cuando se realice una observación sistemática a gran escala de una zona de acceso público.

Deberá definirse la operativa interna para la elaboración y documentación del análisis de impacto y la comunicación del resultado del mismo.

8.4 Desarrollo de medidas técnicas y organizativas

Como resultado de procesos de análisis de riesgos, análisis de impacto y otros procesos de responsabilidad proactiva deberá definirse un catálogo de medidas de seguridad que deberán ser comunicadas tanto a los departamentos de sistemas y desarrollo como en la contratación de servicios que conlleven el tratamiento de datos personales.

8.5 Gestión de quiebras o violaciones de seguridad

Debe definirse un procedimiento de notificación y gestión de las violaciones de seguridad que abarquen no sólo aquellas relacionadas con los sistemas de información, sino cualquier aspecto que haya ocasionado una pérdida, riesgo sobre la confidencialidad, integridad y disponibilidad de la información de carácter personal. Dicho procedimiento debe definir la comunicación interna, la comunicación a la Agencia Española de Protección de datos y en algunos casos hacia el interesado o bien hacia el cliente, si la violación atañe a un servicio prestado por la organización.

En sistemas de información de terceros, operados o no en la infraestructura tecnológica de ERCROS S.A. deben direccionarse estas directrices para que sean implementadas en el alcance del servicio realizado.

8.6 Normativas y procedimientos específicos de seguridad

En función del análisis de riesgos y de oportunidades deberán desarrollarse normativas específicas de tratamientos para definir los procesos a seguir para dar cumplimiento de la protección de datos en tratamientos que así lo requieran.

9. Catálogo de medidas de seguridad

9.1 Niveles de seguridad

ERCROS S.A. define DOS niveles de seguridad según el contenido de la información y el tratamiento que se realiza tanto si está contenida en sistemas de información de manera automatizada como en locales de tratamiento de manera documental o no automatizada.

Nivel de seguridad base	Ficheros o tratamiento de datos
CONFIDENCIALES O ESPECIALMENTE PROTEGIDOS	• Datos de salud, ideología, afiliación sindical, religión, creencias, origen racial, vida sexual tanto de empleados, de usuarios de los servicios de ERCROS S.A. de sus familiares o de empleados, voluntarios u otros tipos colaboradores de la organización. • Datos de afinidad políticas o filosófica • Datos recabados con fines policiales sin consentimiento de las personas afectadas; y derivados de actos de violencia de género.
BÁSICO	• Datos de empleados y colaboradores respecto a sus retribuciones económicas, y beneficios sociales. • Imágenes obtenidas en cámaras de videovigilancia. • En general cualquier fichero o tratamiento que contenga alguna información por la que pueda identificarse a una persona.

9.2 Medidas de seguridad en sistemas de información automatizados

Las siguientes medidas de seguridad, procedimientos y controles deben desarrollarse en sistemas de información de tratamiento de datos, dichas medidas implican tanto al desarrollo de herramientas como la configuración y parametrización de aplicaciones comerciales y/o Opensource

Ámbito	Nivel Básico	Datos confidenciales
Control de Acceso lógico a aplicaciones	• Relación actualizada de usuarios y accesos autorizados. • Control de accesos permitidos a cada usuario según las funciones asignadas. • Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. • Concesión de permisos de acceso sólo por personal autorizado.	• Registro de accesos: usuario, hora, funcionalidad de la aplicación, tipo de acceso, autorizado o denegado. • Conservación del registro al menos 2 años. • Función de administrador para poder consultar el registro de accesos
Identificación y autenticación	• Identificación y autenticación personalizada. • Procedimiento de asignación y distribución de contraseñas que asegure la confidencialidad de las mismas. • Procedimiento de recuperación de la contraseña por parte del usuario que asegure la confidencialidad de la misma. • Almacenamiento ininteligible de la contraseña en base de datos o cualquier otro soporte de almacenamiento o distribución. • Función de administrador para la gestión de la periodicidad del cambio de contraseñas.	• Función de administrador para gestionar el límite de intentos reiterados de acceso no autorizado
Gestión de soportes	• Sistema de inventario de soportes, CMDB o similar. • Identificación del tipo de información que contienen, o sistema de etiquetado. • Acceso restringido al lugar de almacenamiento.	• Cifrado de datos en la distribución de soportes. • Cifrado de información en dispositivos portátiles

Ámbito	Nivel Básico	Datos confidenciales
	• Autorización de las salidas de soportes • Medidas para el transporte y el desecho de soportes.	
Copias de Respaldo	• ERCROS S.A. deberá realizará copias de seguridad de la información según el modelo de servicio de Backup realizado, cuota y planificación. • ERCROS S.A. deberá realizar operaciones de control general para verificar el correcto funcionamiento de la plataforma que proporciona el servicio de Backup. • ERCROS S.A. deberá almacenar las Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.	
Accesos remotos	• ERCROS S.A. deberá implementar y asegurar en la transmisión de datos a través de redes electrónicas cifradas mediante certificados digitales u otros mecanismos.	
Envío por correo electrónico (funcionalidades de aplicaciones informáticas)	• Registro o log de acceso de los emails enviados	• Encriptación de ficheros adjuntos
Seudonimización	• La seudonimización deberá ser realizada mediante desarrollos a nivel de aplicación o mediante otros mecanismos asegurando que la información ya no pueda atribuirse a un interesando sin utilizar información adicional, siempre que dicha información figure por separado y esté sujeta a las debidas medidas de seguridad.	
Desarrollo de software seguro	• Además de las medidas descritas previamente el desarrollo de software debe garantizar el todo el ciclo de vida de construcción de código la integración y confidencialidad de la información de carácter personal tratada, realizando pruebas con datos seudonimizados, en un entorno seguro de construcción, codificación segura, funcionalidades y construcción de código que proteja contra las amenazas y vulnerabilidades de los sistemas de información de repositorio y de interfaz de usuario (OWASP, COBIT, etc.), seguridad en el paso a producción, gestión de cambios, etc. En el caso específico de PROVEEDORES que desarrollen aplicaciones informáticas que traten datos personales deberán contar con políticas y procedimientos internos de desarrollo de software seguro.	

9.3. Medidas de seguridad en ficheros documentales

Las siguientes medidas de seguridad, procedimientos y controles deben implementarse en locales de tratamiento que almacenen información de carácter personal, en soportes digitales o automatizados o no.

Ámbito	Medidas de seguridad
Control de Accesos	• Control de accesos autorizados. • Identificación accesos para documentos accesibles por múltiples usuarios. • Mismas condiciones para personal ajeno con acceso a los recursos de datos.
Criterios de Archivo	• El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Supresión, Oposición, Limitación al tratamiento y portabilidad.
Almacenamiento	• Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura. • Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave, sistemas biométricos, tarjetas personales u otros mecanismos que garanticen el acceso nominativo y personal.
Copia o Reproducción	• Sólo puede realizarse por los usuarios autorizados. • Destrucción de copias desechadas. • Destrucción confidencial para tratamientos de datos especialmente protegidos.
Traslado Documentación	• Medidas que impidan el acceso o manipulación.

10. Funciones y obligaciones del personal

ERCROS S.A. clasifica el personal afectado por esta normativa en las siguientes categorías:

- **Responsable de privacidad** cuyas funciones serán las de coordinar y controlar las medidas definidas en este documento,
- **Administradores del sistema y áreas técnicas**, encargados de administrar o mantener el entorno operativo del Fichero.
- **Encargado del tratamiento**, es la persona física o jurídica, pública o privada, u órgano administrativo, que solo o conjuntamente con otros, trata datos personales por cuenta del Responsable del fichero como consecuencia de una relación. El tratamiento de los datos del fichero por un Encargado externo estará sometido en todo caso a las mismas medidas de seguridad contempladas en el Reglamento.
- **Usuarios de los tratamientos**, o personal que usualmente accede a la información para su tratamiento, y que también deben estar explícitamente relacionados contratos de acuerdo de confidencialidad y direccionamiento de normativas.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla. La organización deberá establecer mecanismos de información, comunicación y concienciación sobre las funciones, roles y riesgos relacionados con la protección de datos personales que deberán contener directrices sobre confidencialidad, gestión en el puesto de trabajo, soportes, notificación de incidencias, archivo y custodia de documentación en papel, contraseñas y uso de sistemas de información, trabajo fuera de las oficinas y oficinas y centros de trabajo de ERCROS S.A. y otras en general que se consideren necesarias para desplegar de manera divulgativa a todo el personal con acceso a información de carácter personal.

11. Acceso a datos por terceros

ERCROS S.A. deberá establecer procedimientos sobre cómo gestionar los contratos de encargo de tratamiento con terceros (básicamente proveedores y/ suministradores) a través de modelos base estableciendo responsables de realización del proceso e inventariando los diferentes tratamientos con sus potenciales accesos por terceros y derivando políticas específicas de tratamiento para direccionar las medidas de seguridad.

De igual manera las cesiones y transmisiones de datos personales entre países deberán ser identificadas en los registros de actividades de tratamientos, tanto de los responsables como de los encargados de tratamiento estableciendo los acuerdos y contratos necesarios entre ambas partes según la legislación específica de cada uno de los países emisores.

12. Responsabilidad proactiva. Evaluación y revisión continua

La organización a través de los procedimientos y proyectos del modelo de responsabilidad proactiva deberá realizar acciones de:

- **Seguimiento, medición y control** de la implementación de las políticas de seguridad, procedimientos y medidas técnicas definidas para garantizar la protección de datos personales definidos de esta política inicial de protección de datos personales.
- Realizar **procesos de auditoría externa** al menos cada dos años sobre los sistemas de tratamiento y locales de almacenamiento que traten datos de carácter personal de nivel de seguridad medio o alto, realizando además procesos de evaluación de riesgos sobre los activos y procesos de la información. Debe realizarse también ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. El proceso debe culminar en un Informe de detección de deficiencias y propuestas correctoras, que debe ser analizado por del responsable de seguridad y estableciendo conclusiones que deben ser elevadas al responsable del fichero: dirección o propiedad.
- Contar con un análisis de riesgos de datos personales que consiste en identificar vulnerabilidades y estimar los tratamientos a los riesgos identificados de manera que se mitiguen los mismos, acciones de decisión que deben establecerse en el marco de la gestión de la organización
- **Integrar los resultados de las evaluaciones de riesgos y auditoría internas** en los sistemas de gestión de la organización.
- **Mantener informado a la dirección** de los resultados de evaluaciones y auditorías determinando y resolviendo las decisiones y estrategias del *nivel de seguridad objetivo*.