www.uning.es
info@uning.es

POLÍTICA DE RETENCIÓN DE DATOS	PRO-02
	Revisión 00

REV.	FECHA	DESCRIPCIÓN

ELABORADO POR: Carlos J. Pérez Aguilera	REVISADO Y APROBADO POR: DIRECCIÓN
FECHA: 08/05/2018	

POLÍTICA DE RETENCIÓN DE DATOS	PRO-02
	Revisión 00

ÍNDICE

1.-OBJETO

2.-ALCANCE

3.-RESPONSABILIDADES

4.-DESCRIPCIÓN

5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS

6.-DIAGRAMA DE FLUJOS

7.-ANEXO

ANEXO 1.-

POLÍTICA DE RETENCIÓN DE DATOS	PRO-02
	Revisión 00

1.-OBJETO

Esta política establece los periodos de retención requeridos para categorías específica de datos y establece los estándares mínimos que se aplicarán cuando se destruya cierta información dentro de la empresa.

Esta Política aplica a todas las unidades de negocio, procesos y sistemas en todos los países en los que la Empresa lleva a cabo sus negocios y realiza transacciones u otras relaciones comerciales con terceros.

Esta política aplica a todos los funcionarios, directores, empleados, agentes, afiliados, contratistas, consultores, asesores o proveedores de servicios de la Empresa que puedan recoger, tratar o tener acceso a datos (incluidos datos personales y / o datos personales sensibles). Es responsabilidad de todos los anteriores familiarizarse con esta política y garantizar el cumplimiento adecuado de la misma.

Esta política se aplica a toda la información utilizada en la Compañía. Ejemplos de documentos incluyen:

Correos
electrónicos
Documentos
en papel
Documentos
electrónicos
Vídeo y audio
Datos generados por los sistemas de control de acceso físico

2.-ALCANCE

Este procedimiento es aplicable a todo el personal de la empresa.

3.-DEFINICIONES

POLÍTICA DE RETENCIÓN DE DATOS	PRO-02
	Revisión 00

No aplica

4.-REGLAS DE RETENCIÓN

4.1. Principio general de retención

En el caso, para cualquier categoría de documentos no específicamente definidos en otra parte de esta política (y en particular dentro del Programa de retención de datos) y a menos que la ley aplicable disponga lo contrario, se considerará que el período de retención requerido para dicho documento se considerará de 6 años para documentos mercantiles desde la fecha de creación del documento.

4.2. Programa general de retención

El delegado de protección de datos determina el periodo de tiempo para el cual los documentos y registros electrónicos deben ser retenidos mediante el programa de retención de datos.

Como excepción, los periodos de retención dentro del programa de retención de datos pueden prolongarse en casos como:

- Las investigaciones en curso de las autoridades de los estados miembros, si existe la posibilidad de registros de datos personales necesarios para la Empresa para demostrar el cumplimiento de los requisitos legales;

o

- En el ejercicio de los derechos legales en los casos de demandas o procedimientos judiciales similares reconocidos por la legislación local.

4.3. Salvaguarda de datos durante el periodo de retención

Se considerará la posibilidad de que los medios utilizados para el archivo de datos se desgasten. Si se eligen medios de almacenamiento electrónicos, también se almacenarán los procedimientos y sistemas que garanticen que se pueda acceder a la información durante el período de retención (tanto con respecto al soporte de información como a la legibilidad de

formatos) para proteger la información contra pérdidas como resultado de futuros cambios tecnológicos. La responsabilidad del almacenamiento recae en el Responsable de Seguridad.

4.4. Destrucción de datos

Por lo tanto, la Empresa y sus empleados deben revisar periódicamente todos los datos, ya sea en formato electrónico en su dispositivo o en papel, para decidir si destruyen o eliminan cualquier dato una vez que el fin para el que se crearon esos documentos ya no sea pertinente. La responsabilidad general de la destrucción de datos recae sobre el Responsable de Seguridad.

Una vez tomada la decisión de llevar a cabo la eliminación de acuerdo con el Programa de retención, los datos deben eliminarse, triturarse o destruirse en un grado equivalente al del valor dado por los demás y su nivel de confidencialidad. El método de eliminación varía y depende de la naturaleza del documento. Por ejemplo, cualquier documento que contenga información sensible o confidencial (y, en particular, datos personales sensibles) debe ser eliminado como residuo confidencial y estar sujeto a una eliminación electrónica segura; algunos contratos que han expirado o han sido reemplazados sólo pueden garantizar la trituración interna. La sección del Programa de eliminación de documentos que se encuentra a continuación define el modo de eliminación.

En este contexto, el empleado deberá realizar las tareas y asumir las responsabilidades pertinentes para la destrucción de la información de manera adecuada. El proceso específico de eliminación o destrucción puede ser llevado a cabo tanto por un empleado o por un proveedor de servicios interno o externo que el Responsable de Seguridad subcontrata para este propósito. Se cumplirán todas las disposiciones generales aplicables según las leyes de protección de datos pertinentes y la política de protección de datos personales de la Empresa.

Deben existir controles adecuados que impidan la pérdida permanente de información esencial de la empresa como resultado de la destrucción intencionada o no intencionada de la información– estos controles se definen en Políticas de Seguridad de la Información.

El Responsable de Seguridad documentará y aprobará por completo el proceso de destrucción. Los requisitos legales aplicables para la destrucción de información, en particular los requisitos de las leyes de protección de datos aplicables, deberán observarse plenamente.

4.5. Violación, ejecución y cumplimiento

La persona designada con la responsabilidad de Protección de datos (el Responsable de Seguridad) tiene la responsabilidad de garantizar que cada una de las oficinas de la Compañía cumpla con esta Política. También es responsabilidad del Responsable de Seguridad ayudar a cualquier oficina local con las consultas de cualquier autoridad de protección de datos local o gubernamental.

Cualquier sospecha de incumplimiento de esta Política debe informarse de inmediato a el Responsable de Seguridad. Se investigarán todas las instancias de supuestas infracciones de la Política y se tomarán medidas según corresponda.

El incumplimiento de esta Política puede tener consecuencias negativas, que incluyen, entre otras, la pérdida de confianza del cliente, litigios y pérdida de ventajas competitivas, pérdidas financieras y daños a la reputación, lesiones personales, daños o pérdidas de la Empresa. El incumplimiento de esta política por parte de empleados permanentes, temporales o contratados, o de terceros, a los que se haya otorgado acceso a las instalaciones o a la información de la Empresa, puede dar como resultado procedimientos disciplinarios o el cese de su empleo o contrato. Tal incumplimiento también puede conducir a acciones legales contra las partes involucradas en tales actividades.

5. Eliminación de documentos

5.1. Programa de eliminación rutinaria

Los registros que pueden destruirse de manera rutinaria a menos que estén sujetos a una investigación legal o reglamentaria en curso son los siguientes:

Anuncios y avisos de reuniones diarias y otros eventos que incluyen aceptaciones y disculpas;
Solicitud de información ordinaria como las direcciones de viajes;
Reservas para reuniones internas sin cargos/costes externos;

Documentos de comunicación como cartas, portadas de fax, mensajes de correo electrónico, hojas de ruta, hojas de felicitaciones y elementos similares que acompañan a los documentos pero que no agregan ningún valor;

Hojas con mensajes;
Lista de direcciones reemplazada, listas de distribución, etc.;

Documentos duplicados tales como copias CC y FYI, borradores sin cambios, impresiones de instantáneas o extractos de bases de datos y archivos diarios;

Publicaciones internas almacenadas que están obsoletas o reemplazadas; y

Revistas comerciales, catálogos de proveedores, folletos y boletines de vendedores u otras organizaciones externas.

En todos los casos, la eliminación está sujeta a los requisitos de comunicación que puedan existir en el contexto de un litigio.

5.2. Método de destrucción

Los documentos de nivel I son aquellos que contienen información que es de la más alta seguridad y confidencialidad y aquellos que incluyen cualquier dato personal. Estos documentos se eliminarán como residuos confidenciales (triturado de corte transversal e incinerado) y estarán sujetos a eliminación electrónica segura. La eliminación de los documentos debe incluir una prueba de destrucción.

Los documentos de nivel II son documentos privados que contienen información confidencial, como los nombres, firmas y direcciones de las partes, o que podrían ser utilizados por terceros para cometer fraudes, pero que no contienen ningún dato personal. Los documentos deben ser cortados transversalmente y luego colocados en contenedores de basura cerrados para su recolección por una empresa de eliminación aprobada, y los documentos electrónicos estarán sujetos a eliminación electrónica segura.

Los documentos de nivel III son aquellos que no contienen información confidencial o datos personales y son documentos publicados de la Empresa. Estos deben ser triturados en tiras o eliminados a través de una empresa de reciclaje e incluir, entre otras cosas, anuncios, catálogos, folletos y boletines informativos. Estos pueden ser eliminados sin una pista de auditoria.

POLÍTICA DE RETENCIÓN DE DATOS	PRO-02
	Revisión 00

5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS

Nombre del registro	Ubicación	Persona responsable de su almacenamiento	Controles para la protección de registros	Tiempo de retención
Programa de retención de datos	Carpeta RGPD	Responsable de Seguridad	Sólo personal autorizado puede acceder a estos contratos.	Permanente

Anexo– Programa de Retención de Datos

Categoría de registro de datos personales	Periodo de retención obligatorio	Propietario del registro
Documentos de afiliaciones, altas, bajas y cotizaciones en la Seguridad Social, así como los relativos a nóminas y contratos	4 años tras la relación laboral	Departamento de RRHH
Documentos mercantiles (clientes o proveedores)	6 años después de que el contrato se haya terminado, según el código de comercio A efectos fiscales 4 años	Dpto. Contabilidad
Datos de Videovigilancia Aquí se incluyen las grabaciones de imagen y/o sonido.	No hay	Resp. Seguridad
Documentación de salud	5 años contados desde la fecha del alta de cada proceso asistencial	Resp. Seguridad