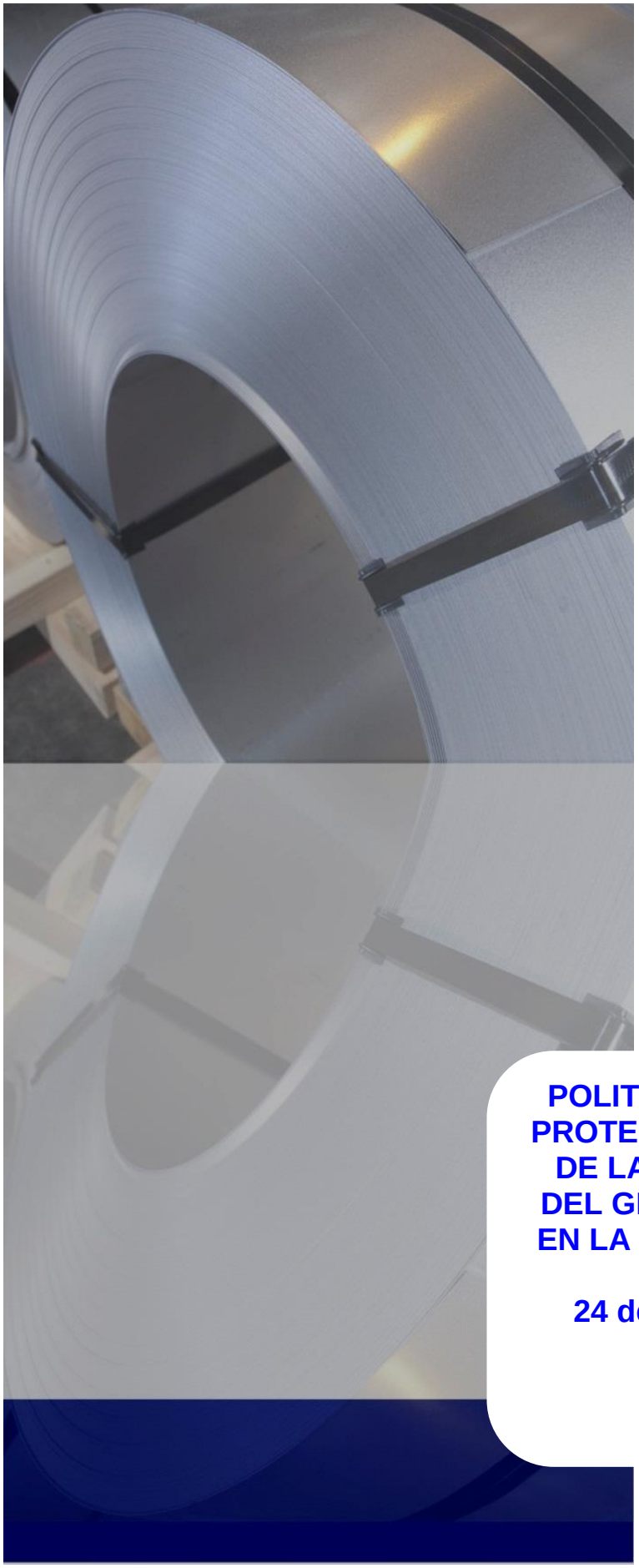

POLITICA INTERNA DE PROTECCION DE DATOS DE LAS SOCIEDADES DEL GRUPO ACERINOX EN LA UNION EUROPEA

24 de mayo de 2018

POLITICA INTERNA DE PROTECCION DE DATOS DE LAS SOCIEDADES DEL GRUPO ACERINOX EN LA UNION EUROPEA

INDICE

1. INTRODUCCIÓN

El 4 de mayo de 2016 se publicó en el Diario Oficial de las Comunidades Europeas, el 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 datos y por el que se deroga la Directiva 95/46/CE (en adelante el Reglamento).

Esta norma cuya entrada en vigor es el 25 de mayo de 2018, es de aplicación directa en todos los Estados miembros de la Unión Europea, no requiriendo transposición.

El Reglamento incorpora una serie de novedades significativas en lo relativo a las obligaciones que, hasta la fecha, venían soportando las empresas en la materia. A las novedades regulatorias, que incorporan nuevos derechos de los ciudadanos, nuevos requisitos para justificar los tratamientos, medidas de seguridad etc., se añaden mayores competencias a las autoridades de control y un régimen sancionador más exigente.

El Grupo Acerinox ha acometido un proceso de revisión y actualización de su organización para garantizar su adecuación a estas nuevas exigencias legales, recogiéndose en esta Política Interna de Protección de Datos (en adelante la Política Interna) los aspectos esenciales de dicha adaptación, que serán objeto de desarrollo, en caso de ser necesario, mediante instrucciones internas anexas a esta norma básica.

2. OBJETO Y ÁMBITO

2.1. Objeto

La Política Interna recoge los aspectos esenciales de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y las normas relativas a la libre circulación de tales datos, definiendo la estructura de gestión y supervisión de la materia, las funciones y obligaciones de las personas y Departamentos involucrados, y las obligaciones que el Grupo tiene respecto de los datos personales y su circulación.

2.2. Ámbito material

Esta Política Interna se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2.3 Ámbito subjetivo

Esta Política Interna resulta aplicable a todas y cada una de las compañías integrantes del Grupo Acerinox a las que les resulta de aplicación el Reglamento y, por tanto, a todos y cada uno de los trabajadores, directivos, y miembros de los órganos de administración de las siguientes compañías:

- Acerinox, S.A.
- Acerinox Europa, S.A.U.
- Roldan, S.A.
- Inoxfil, S.A.U.
- Inoxidables de Euskadi, S.A.U.
- Inoxcenter, S.L.U.
- Inoxcenter Canarias, S.A.U.
- Metalinox Bilbao, S.A.U.
- Cedinox
- Acerinox Benelux SA-NV
- Acerinox Deutschland GmbH
- Acerinox France S.A.S.
- Acerinox Italia S.R.L.
- Acerinox Polska SP Z.O.O.
- Acerinox Scandinavia AB
- Acerinox UK, Ltd.
- Acerol – Comércio e Indústria de Aços Inoxidáveis, Unipessoal, Lda.
- Inoxplate - Comércio de Produtos de Aço Inoxidável, Sociedade Unipessoal, Lda.
- InoxRe S.A.

(en adelante, Sociedades o individualmente Responsable del Tratamiento o Responsable)

3. OBLIGATORIEDAD

Esta Política Interna tiene carácter normativo y por tanto todos los trabajadores y los directivos de las Sociedades quedan vinculados por ella en cuanto norma interna de conducta, y tienen la obligación de conocerla y de ayudar a su implantación y efectividad con independencia de la posición que ocupen dentro de la organización, y tengan o no contacto directo con las materias en ella descritas.

4. DEFINICIONES

Se adjunta como **Anexo I** una relación de definiciones.

5. ESTRUCTURA DEL SISTEMA DE PROTECCION DE DATOS

5.1 Estructura

Las siguientes personas y órganos asumen funciones específicas en materia de protección de datos:

- El Consejero Delegado
- El Delegado de Protección de Datos
- Los Responsables de los Procesos
- El Departamento de Sistemas de Información
- La Dirección de Riesgos corporativos
- El Departamento de Asesoría Jurídica
- El Departamento de Auditoria Interna

5.2 Consejero Delegado

El Consejero Delegado será el competente para el nombramiento del Delegado de Protección de Datos, que dependerá funcionalmente del primero, correspondiéndole además la supervisión y el seguimiento del cumplimiento de sus funciones. Igualmente le corresponderá la aprobación de las políticas, instrucciones internas de desarrollo y planes de formación en la materia.

5.3 Delegado de Protección de Datos

El Grupo Acerinox ha decidido nombrar un único Delegado de Protección de Datos (en adelante DPD) para todas las Sociedades, que contara en el desarrollo de sus funciones con el apoyo y asesoramiento del resto de la organización. Los datos de contacto del DPD se publicarán en la página web del Grupo, y el nombramiento será comunicado a las autoridades reguladoras.

Las Sociedades garantizarán que el DPD participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, y le respaldarán en el cumplimiento de sus funciones, facilitando los recursos necesarios para el desempeño de las mismas, y para el mantenimiento de sus conocimientos especializados.

Las Sociedades garantizarán que el DPD no reciba ninguna instrucción en lo relativo al desempeño de sus funciones.

Los interesados podrán ponerse en contacto con el DPD en lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.

El DPD estará obligado a mantener la confidencialidad en el desempeño de sus funciones, de conformidad con la normativa aplicable.

El DPD podrá desempeñar otras funciones y cometidos. El Responsable del Tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

El DPD tendrá las siguientes funciones:

- Informar y asesorar al Responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones de la normativa aplicable.
- Supervisar el cumplimiento de la normativa aplicable y de las políticas de las Sociedades en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

El DPD desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

5.4 Responsables de Procesos

Los Responsables de Procesos son las personas identificadas como tal en el inventario de registros de tratamiento de cada Sociedad.

El papel de los Responsables de Procesos es esencial en la protección de datos, al constituir la primera línea de aplicación y respeto de la normativa y políticas internas en la materia.

Las obligaciones de los Responsables de Procesos son las siguientes:

- Asistir al DPD en el análisis y evaluación de los riesgos propios de los tratamientos, y los de los terceros que tratan datos por cuenta de las Sociedades en orden a establecer las medidas de seguridad correspondientes.
- Cumplir y hacer cumplir respecto de los tratamientos de datos de los que son responsables la normativa aplicable y las políticas internas.
- Asistir al DPD en las tareas de formación y concienciación en la materia de protección de datos.
- Notificar al DPD y evaluar las implicaciones de cualquier cambio en los tratamientos de los que es Responsable.

5.5 Departamento de Sistemas de Información

Obligaciones a cargo del Departamento de Sistemas de Información:

- Asistir al DPD en el análisis y evaluación de los riesgos propios de los tratamientos automatizados, y los de los terceros que tratan datos por cuenta de las Sociedades en orden a establecer las medidas de seguridad correspondientes.
- Aplicar, mantener y actualizar las medidas de seguridad informática asignadas a los registros.
- Aplicar, mantener y actualizar el actual plan de contingencia en lo referente a privacidad.
- Asistir al DPD en la gestión de los procedimientos de ejercicio de los derechos de los interesados y de los incidentes en materia de privacidad.
- Asistir al DPD en la elaboración de las instrucciones internas.
- Asistir al DPD en las tareas de formación y concienciación en protección de datos.
- Notificar al DPD y evaluar las implicaciones de cualquier cambio tecnológico que tenga incidencia en la protección de datos.

5.6 Dirección de Riesgos Corporativos

Obligaciones a cargo de la Dirección de Riesgos Corporativos:

- Asistir al DPD en el análisis y evaluación de los riesgos propios de los tratamientos, y los de los terceros que tratan datos por cuenta de las Sociedades en orden a establecer las medidas de seguridad correspondientes.
- Establecer una política de gestión de riesgos en privacidad alineada con las necesidades del negocio, definiendo también su apetito al riesgo.
- Monitorizar y controlar periódicamente los riesgos de privacidad existentes en las Sociedades.

5.7 Departamento de Asesoría Jurídica

Obligaciones a cargo del Departamento de Asesoría Jurídica:

- Monitorizar los cambios legislativos que se puedan producir en materia de protección de datos para su traslado al DPD.
- Asesorar y asistir al DPD en materia jurídica, en las investigaciones y requerimientos de autoridades, y en los procedimientos judiciales en materia de protección de datos.

5.8 Departamento de Auditoria interna

Obligaciones a cargo del Departamento de Auditoría Interna:

- Supervisar la aplicación de la Política Interna de acuerdo con el modelo de tres líneas de defensa establecido por el European Confederation of Institutes of Internal Auditing. Para ello, la Política Interna pasará a formar parte del Universo de Auditoría, y las auditorías tendrán como objetivo asegurar que las actividades, funciones y obligaciones descritas se realizan, y que garantizan los Principios Fundamentales de Protección de Datos.

- Se establecerá la periodicidad de la auditoría a través del Plan Anual aprobado por la Comisión de Auditoría.

6. PRINCIPIOS BASICOS DE LA PROTECCION DE DATOS

El principio básico que se protege con esta Política Interna es el respeto de los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la protección de los datos personales. Este derecho se concreta en los siguientes principios:

- Principios de licitud, lealtad y transparencia
- Principio de limitación de la finalidad
- Principio de minimización de datos
- Principio de exactitud
- Principio de limitación del plazo de conservación
- Principios de integridad y confidencialidad
- Principio de responsabilidad proactiva

7. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES

El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física solo es posible en las siguientes circunstancias:

- Consentimiento explícito del interesado salvo que la normativa lo prohíba.
- Que sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable del Tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social.
- Que sea necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

- Que se refiera a datos personales que el interesado ha hecho manifiestamente públicos.
- Que sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- Que sea necesario por razones de un interés público esencial.
- Que sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social. El tratamiento será realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, o por cualquier otra persona sujeta también a la obligación de secreto.

Los nuevos tratamientos de datos sensibles, así como el tratamiento de datos de menores de edad, de datos relativos a condenas e infracciones penales tendrá que ser consultado con carácter previo al DPD.

8. OBLIGACIONES DE LAS SOCIEDADES COMO RESPONSABLES DE TRATAMIENTO

8.1 Medidas de seguridad

Las Sociedades aplicarán medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de los datos personales es conforme con la normativa aplicable.

Las medidas organizativas, técnicas y físicas que se aplican en las Sociedades se han actualizado en base a la metodología de análisis de riesgos y están adecuadas al apetito de riesgo de la Compañía con el objetivo de a) asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios que intervienen en el tratamiento de datos personales, y b) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

Dichas medidas que se reflejan para cada tratamiento en el inventario de registros propio, se revisarán y actualizarán cuando sea necesario, y como mínimo una vez al año. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

Las personas que tengan acceso a datos personales de los que sean responsables las Sociedades solo podrán tratar dichos datos siguiendo instrucciones incluidas en esta Política Interna y en su normativa de desarrollo.

8.2 Evaluación de Impacto de la privacidad

Se realizará una Evaluación de Impacto de la privacidad (PIA) para los tratamientos actuales y nuevos tratamientos que supongan un alto riesgo para los derechos y libertades de las personas físicas, y en concreto en los siguientes casos:

- Cuando exista una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como, por ejemplo, la elaboración de perfiles.
- Tratamientos a gran escala de las categorías especiales de datos o de los datos personales relativos a infracciones o condenas penales.
- Observación sistemática a gran escala de una zona de acceso público.

Cuando se vaya a implantar un nuevo tratamiento de datos personales o se produzca un cambio en un tratamiento existente que requiera PIA, este deberá efectuarse y aprobarse formalmente por el DPD y el Responsable de Procesos.

Cuando un PIA relativo a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el Responsable no toma medidas para para mitigarlo, se consultara a la autoridad de control.

8.3 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, las Sociedades aplicarán, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, 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 de la normativa aplicable y proteger los derechos de los interesados.

Para ello los Responsables de Procesos respecto de los tratamientos ya identificados cuando estos vayan a modificarse, y el resto de los empleados de las Sociedades antes de iniciar un nuevo tratamiento de datos, deberán contactar con el DPD para regularizar el mismo con al menos un mes de antelación al inicio del tratamiento o realización de la modificación.

En cuanto al tratamiento de datos por defecto, las Sociedades aplicarán medidas para garantizar que solo sean objeto de tratamiento los datos personales (cantidad de datos, extensión de su tratamiento, plazo de conservación y accesibilidad) necesarios para cada uno de los fines del

tratamiento. Estas medidas garantizarán en particular que por defecto los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

8.4 Corresponsables del tratamiento

Cuando dos o más Sociedades o alguna de ellas con un tercero determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de sus obligaciones salvo, y en la medida en que, sus responsabilidades respectivas se rijan por la normativa aplicable. Dicho acuerdo podrá designar un punto de contacto para los interesados y reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados.

8.5 Registro de las actividades de tratamiento

Se ha elaborado un inventario de los registros de actividades de tratamiento de datos personales de los que son responsables cada una de las Sociedades, en el que se ha incluido la información obligatoria establecida en la normativa aplicable.

Estos inventarios están centralizados, son accesibles, completos y se mantendrán actualizados para incluir todas las actividades de tratamiento que en cada momento se lleven a cabo.

8.6 Encargados del tratamiento de datos de los que son responsables las Sociedades

Las Sociedades elegirán encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la normativa aplicable y garantice la protección de los derechos del interesado.

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo a la normativa aplicable, que vincule al encargado respecto del Responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del Responsable.

A tal fin todos los empleados de las Sociedades deberán informar al DPD de los nuevos tratamientos por cuenta de terceros que se quieran realizar para que se proceda a la regularización de los mismos.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del Responsable, se

impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo a la normativa aplicable, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el Responsable y el encargado. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el Responsable del Tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

8.7 Violación de la seguridad de los datos personales

Cualquier violación de la seguridad de los datos personales ha de ser comunicada inmediatamente al DPD para que este a su vez la notifique a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Las violaciones de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas serán recogidas es un registro que permitirá a la autoridad de control verificar el cumplimiento de la normativa aplicable.

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, este extremo se comunicará inmediatamente al DPD para que este a su vez se la comunique al interesado sin dilación indebida.

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

- Se han adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
- Se han tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.
- Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

8.8 Destrucción de datos y soportes

Se ha elaborado una política de destrucción de documentación y soportes automatizados y no automatizados que contengan datos de carácter personal

una vez expirada su fecha de conservación, que incluye instrucciones al personal del Grupo que tiene encomendada esa función.

9. OBLIGACIONES DE LAS SOCIEDADES COMO ENCARGADAS DE TRATAMIENTO DE DATOS

Las Sociedades han elaborado y mantienen un registro de actividades de tratamiento por cuenta de terceros que esta centralizado, es accesible, completo y que se mantendrá actualizado para incluir todas las actividades de tratamiento por cuenta de terceros que en cada momento se lleven a cabo.

Las Sociedades notificarán sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tengan conocimiento.

10. POLITICA EXTERNA DE PROTECCIÓN DE DATOS

Se ha elaborado una política externa de protección de datos que está disponible para cualquier interesado, en la que se reflejan los derechos de los titulares de los datos personales y todos los elementos de información que establece el Reglamento en un formato fácilmente comprensible y estructurado, de acuerdo con las indicaciones que han elaborado las autoridades reguladoras en este sentido.

Esta Política permite dar a conocer a los terceros de forma detallada el funcionamiento de las Sociedades en materia de recogida, uso, conservación, divulgación o destrucción de datos personales.

La Política está disponible en la página web de Acerinox.

11. TRANSFERENCIAS INTERNACIONALES DE DATOS

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, el Responsable y el encargado del tratamiento cumplen las condiciones establecidas por la normativa aplicable, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

Cuando se plantee efectuar una transferencia internacional de datos no contemplada en el inventario de registros de tratamiento, se deberá contactar con el DPD con carácter previo.

12. DIVULGACIÓN Y FORMACIÓN

12.1 Divulgación de la Política Interna

La aprobación de la Política Interna se comunicará a todos los empleados de las Sociedades.

El DPD decidirá sobre las distintas acciones de comunicación que se deben realizar para transmitir el compromiso adoptado por el Grupo Acerinox en materia de protección de datos, el mensaje específico que se quiere transmitir, los emisores y receptores, el canal de comunicación y el calendario de las actuaciones.

12.2 Formación en privacidad y protección de datos

Como cierre de la Política Interna, el Grupo Acerinox ha considerado fundamental que los empleados de las Sociedades reciban una formación adecuada en protección de datos y en especial en las siguientes materias:

- Privacidad en el diseño acorde con los diferentes roles o perfiles de los empleados.
- Medidas de seguridad a aplicar a los tratamientos de datos personales en los que intervienen: minimización, cifrado, anominización, plazos de conservación de la documentación,
- Gestión del ejercicio de los derechos de los interesados.

La mencionada formación se estructurará a tres niveles:

- Formación general en protección de datos para todos los empleados.
- Formación específica para áreas relevantes en la interacción con empleados y clientes.
- Formación específica para el DPD, el personal del Departamento de Cumplimiento y los Responsables de Procesos.

La formación en materia de protección de datos se tramitará internamente como cualquier otra formación, con la ayuda de los respectivos departamentos de recursos humanos.

En el supuesto de nuevas incorporaciones a las Sociedades o promociones a puestos de trabajo que requieran formación específica en materia de protección de datos, el DPD identificará los cursos o iniciativas formativas individuales que se pueden llevar a cabo.

Sin perjuicio de lo anterior, si a través del sistema de control interno o de cualquier otra forma se detectaran necesidades de formación adicional o extraordinaria en materia de protección de datos, el DPD gestionará dicha formación.

13. APROBACIÓN

Esta Política Interna ha sido aprobada por el Consejero Delegado de Acerinox, S.A. con fecha 24 de mayo de 2018.

ANEXO I: DEFINICIONES

A efectos de esta Política Interna se entenderá por:

1) **«datos personales»:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará 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.

2) **«tratamiento»:** 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.

3) **«limitación del tratamiento»:** el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

4) **«elaboración de perfiles»:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

5) **«seudonimización»:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

6) **«fichero»:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

7) **«responsable del tratamiento» o «responsable»:** la persona física o jurídica que, solo o junto con otros, determine los fines y medios del tratamiento.

8) **«encargado del tratamiento» o «encargado»:** la persona física o jurídica, que trate datos personales por cuenta del responsable del tratamiento.

9) **«destinatario»:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

10) **«tercero»:** persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

11) **«consentimiento del interesado»:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

12) **«violación de la seguridad de los datos personales»:** toda violación de la seguridad que 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.

13) **«datos genéticos»:** datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

14) **«datos biométricos»:** datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

15) **«datos relativos a la salud»:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.