INSTRUCCIÓN INTERNA SOBRE LA GESTIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES

Madrid 3 de noviembre de 2020

ÍNDICE:

INSTRUCCIÓN INTERNA SOBRE LA GESTIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES

1. INTRODUCCION

La buena gestión de las violaciones de seguridad es un tema de vital importancia, teniendo en cuenta el impacto que éstas pueden ocasionar en los derechos y libertades de los interesados afectados. Además, el Reglamento (UE) 2016/679 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 (en adelante, "**RGPD**"), también establece que estos incidentes de seguridad pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como la pérdida de control sobre sus datos personales, la restricción de sus derechos, usurpación de identidad, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de la confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social significativo.

De esta manera, el artículo 12 del Código de Conducta y Buenas Prácticas del Grupo Acerinox establece la confidencialidad de los datos de los empleados, clientes y proveedores y la obligación de comunicar cualquier fuga de los mismos.

Asimismo, el Grupo Acerinox aprobó su Política Interna de Protección de Datos en cuyo artículo 8.7 se recogen, entre otros, los aspectos esenciales de la gestión de las violaciones de seguridad que afectan a datos personales.

Esta Instrucción Interna desarrolla el contenido del Código de Conducta y Buenas Prácticas y Acerinox, S.A. y su Grupo de Empresas, así como de la Política Externa de Protección de Datos, concretando el procedimiento para llevar a cabo una correcta gestión de las violaciones de seguridad que tengan incidencia en los datos personales de las personas físicas.

2. OBJETO

Esta Instrucción Interna se aplica a las brechas de seguridad que afectan a datos personales automatizados o en papel. De esta forma se definen las funciones y obligaciones que el Grupo Acerinox debe cumplir ante una violación de seguridad que afecte a datos personales.

3. AMBITO Y OBLIGATORIEDAD

Esta Instrucción Interna resulta aplicable a todas y cada una de las compañías integrantes del Grupo Acerinox a las que les resulta de aplicación el RGPD 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 GmbG
- 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 Productos de Aço Inoxidável, Sociedade Unipessoal, Lda.
- InoxRe S.A.
- VDM Metals Holding GmbH
- VDM Metals International GmbH
- VDM Metals GmbH
- VDM Metals Austria GmbH
- VDM Metals Benelux B.V.
- VDM Metals France S.A.S.
- VDM Metals Italia S.r.l.
- VDM Metals U.K. Ltd.

4. DEFINICIONES

Dato Personal

Se entiende por “dato personal” toda información sobre una persona física identificada o identificable (**interesado**). A estos efectos, se considerará “persona física identificable” a 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 varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Violación de Seguridad de Datos Personales

De forma genérica, se entiende por “violación de seguridad” a un suceso inesperado o no deseado, que provoca consecuencias en detrimento de la seguridad del sistema de información en el que se produce. En relación con los datos personales, el RGPD define las violaciones de seguridad de los datos personales, más comúnmente conocidas como “quiebras de seguridad”, de una forma muy amplia. De esta manera, se entiende por “violación de seguridad” todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

5. SUCESOS QUE PUEDEN DAR LUGAR A VIOLACIONES DE SEGURIDAD

Los sucesos que pueden ocasionar una violación de seguridad podrán ser, entre otros:

- Accesos no autorizados al sistema (robo de contraseñas; suplantación de usuario, etc.)
- Accesos no autorizados a archivos de almacenamiento de documentos
- Fallos en la aplicación o desconexión del sistema (migración incompleta de datos, falta de bloqueo, error de funcionalidades, fallos de servidores, caída o fallos del sistema, averías de software o comunicaciones, falta de suministro eléctrico, etc.)
- Ataques informáticos y malware (ransomware, troyanos, virus, etc.)
- Divulgación de datos personales o cesiones no autorizadas de datos personales
- Robo, pérdida o sustracción de información en dispositivos portátiles (pendrives, CDs, etc.)
- Robo, pérdida o sustracción de una tarjeta de acceso a un área restringida con potencial de acceso masivo a datos personales (Centro de Procesos de Datos, archivos centrales de documentación, etc.)
- Desastres naturales (inundación, incendio, terremoto, etc.)
- Errores en el manejo o utilización de un archivo o software que trate datos personales y que pueda suponer una pérdida o ponga en peligro su integridad o disponibilidad
- Salida de documentación o soporte con datos personales no autorizada
- Cualquier otro incidente que ocasione la destrucción, pérdida o alteración de datos personales

6. COMUNICACIÓN AL DPD DE VIOLACIONES DE SEGURIDAD

Cuando cualquier trabajador perteneciente al Grupo Acerinox, encargado del tratamiento o tercero, tenga conocimiento de una posible violación de seguridad (es decir, cuando se dé alguno de los supuestos señalados en el apartado anterior, o cualquier otro suceso que pueda desencadenar una violación de seguridad) deberá ponerlo en conocimiento del Delegado de Protección de Datos del Grupo Acerinox a través del correo electrónico dpo@acerinox.com, sin dilación indebida. No obstante, en caso de que se trate de una posible violación de seguridad ocurrido en VDM, se deberá informar al Delegado de Protección de Datos de VDM a través del correo electrónico datenschutz.vdm@acerinox.com

El Delegado de Protección de Datos del Grupo Acerinox deberá analizar qué impacto ha tenido la brecha de seguridad sobre los datos personales de los interesados. De esta manera, se trata de establecer hasta qué punto el incidente de seguridad, por sus características, el tipo de datos personales a los que se refiere o el tipo de consecuencias que puede llegar a tener para los afectados puede causar un daño en sus derechos o libertades. Los daños pueden ser materiales o inmateriales, e ir desde el posible uso indebido por quien ha accedido a ellos de forma no autorizada hasta la usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

7. COMUNICACIÓN A LA AUTORIDAD COMPETENTE DE VIOLACIONES DE SEGURIDAD

7.1. Cuándo se ha de notificar una violación de seguridad

En caso de que el Delegado de Protección de Datos del Grupo Acerinox decida que la violación de seguridad notificada puede suponer un riesgo para los derechos y libertades de los interesados, se realizará la notificación ante la autoridad competente en materia de protección de datos del país correspondiente.

A estos efectos algunas Autoridades competentes en materia de protección de datos tienen habilitado un canal específico que permite al responsable del tratamiento comunicar las violaciones de seguridad que han tenido.

El RGPD señala que puede no existir la obligación de notificar a la autoridad competente cuando el responsable del tratamiento pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que tal violación de seguridad entrañe un riesgo para los derechos y libertades de las personas físicas afectadas. Esta valoración se llevará a cabo por el Delegado de Protección de Datos del Grupo Acerinox.

7.2. Criterios de valoración de las violaciones de seguridad según la Agencia Española de Protección de Datos

La severidad de la pérdida de confidencialidad producida por esta brecha de seguridad se gradúa, siguiendo los criterios establecidos por la AEPD según el número potencial y el tipo de partes que pueden haber accedido ilegítimamente a la información.

De esta manera, la AEPD ha establecido los siguientes criterios para la valoración de las violaciones de seguridad:

VOLUMEN (números de registros completos e identificativos)

- Menos de 100 registros (1)
- Más de 1.000 (2)
- Entre 1.000 y 100.000 (3)
- **Más de 100.000 (4)**
- **Más de 1.000.000 (5)**

TIPOLOGÍA DE DATOS (Según RGPD y Sector)

- Datos no sensibles (x1)
- **Datos sensibles (x2)**

IMPACTO (Exposición)

- Nulo (2)
- Interno (dentro de la empresa - controlado) (4)
- **Externo (perímetro proveedor, atacante) (6)**
- **Pública (accesible en internet) (8)**
- **Desconocido (10)**

El cálculo del posible riesgo se podría obtener de la siguiente forma:

Riesgo = P (Volumen) x Impacto (Tipología x Impacto)

Se ha de notificar a la Agencia Española de Protección de Datos ante cualquier violación de seguridad que cumpla simultáneamente las siguientes circunstancias:

- Riesgo con valor cuantitativo en un umbral superior a 20
- Ante la coincidencia de dos circunstancias cualitativas (marcadas en **negrita**)

Asimismo, se procederá a comunicar a los interesados afectados cualquier violación de seguridad que cumpla simultáneamente las siguientes circunstancias:

- Riesgo con valor cuantitativo superior a 40
- Ante la coincidencia de dos circunstancias cualitativas (marcadas en **negrita**)

7.3. Plazo para realizar la notificación

La notificación de la violación de seguridad a la autoridad correspondiente en materia de protección de datos se hará efectiva sin dilaciones indebidas y, a ser posible, dentro de las 72 horas siguientes a que se haya tenido constancia de ella (teniendo en cuenta que el plazo se cuenta desde que el responsable del tratamiento tiene conocimiento de la violación de seguridad).

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, debido a la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso. La información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

7.4. Contenido mínimo de la notificación

La información mínima que se debe notificar es la siguiente:

- La naturaleza de la violación de seguridad
- Las categorías de datos y de interesados afectados por la violación de seguridad
- El número aproximado de interesados afectados por la violación de seguridad
- Las consecuencias producidas, o que potencialmente se puedan producir, como consecuencia de la violación de seguridad
- Medidas adoptadas por Acerinox para solventar la violación de seguridad
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los afectados.

8. NOTIFICACIÓN A LOS INTERESADOS

En los casos en los que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad competente en materia de protección de datos deberá complementarse con una notificación dirigida a los afectados.

El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños considerables a los interesados en relación con sus datos personales. Por ejemplo, en casos en que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

La notificación a los interesados no será necesaria cuando:

- El responsable del tratamiento hubiera tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las medidas que hagan ininteligibles los datos para terceros, como sería el cifrado
- Cuando el responsable del tratamiento haya tomado con posterioridad a la quiebra de seguridad medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública

9. DEBER DE DOCUMENTAR TODAS LAS VIOLACIONES DE SEGURIDAD DE PROTECCIÓN DE DATOS

El RGPD establece la necesidad de que todas las violaciones de seguridad queden documentadas para poder tener evidencias de la gestión de las mismas, conservando las mismas por un plazo de 3 años.

Las violaciones de seguridad de los datos personales serán registradas y documentadas de conformidad con el modelo del **Anexo I** que contiene una relación de hechos, sus efectos y las medidas correctivas adoptadas.

Este registro quedará a disposición de las autoridades de control competentes.

10. REFERENCIAS

- 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.
- Guía para la gestión y notificación de brechas de seguridad publicada por la Agencia Española de Protección de Datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Política Interna de Protección de Datos de las sociedades del Grupo Acerinox en la Unión Europea, aprobada el 24 de mayo de 2018.

Órgano de aprobación: Consejero Delegado de Acerinox, S.A.

Fecha aprobación: 3 de noviembre de 2020

Realizado por: Departamento de Prevención y Cumplimiento

ID de la norma: PD-4

Versión: 1/21

Fecha de última versión aprobada: 22 de enero de 2020

ANEXO I.- MODELO DE INFORME DE VALORACIÓN DE VIOLACIONES DE SEGURIDAD

En fecha de [FECHA], se detectó por [_____] una violación de seguridad relativa a [DESCRIPCIÓN DE LOS HECHOS Y LOS EFECTOS QUE HA PROVOCADO LA INCIDENCIA DE SEGURIDAD].

Análisis de la Violación de Seguridad

VOLUMEN	[descripción]	[número]
TIPOLOGÍA DE DATOS	[descripción]	[número]
IMPACTO	[descripción]	[número]
RIESGO	**[ecuación]**	**[número]**

Teniendo en cuenta lo anteriormente mencionado y la Instrucción Interna sobre la gestión de violaciones de seguridad de datos personales, los hechos descritos constituyen una **violación de seguridad**.

Por tanto, una vez analizada la violación de seguridad producida, se entiende que la severidad de la misma es [**MÍNIMA, MODERADA, MÁXIMA**], puesto que [DESCRIPCIÓN DE LA JUSTIFICACIÓN].

Una vez se tuvo conocimiento del incidente de seguridad, se procedió inmediatamente a su solución y minimización del daño, [DESCRIPCIÓN DE LAS MEDIDAS ADOPTADAS].

Adicionalmente, se ha definido el siguiente plan de acción para la erradicación del problema que ha generado la violación de seguridad, a fin de evitar que se vuelva a producir dicha incidencia. [DESCRIPCIÓN DE LOS PLANES DE ACCIÓN]

Conclusión

Por todo lo anteriormente expuesto, se considera que la violación de seguridad producida en [FECHA] [NO/SI] tiene entidad suficiente como para que exista una comunicación de la violación de seguridad a la Autoridad competente en materia de protección de datos. [MOTIVAR]
Asimismo, la presente violación de seguridad [NO/SI] tiene entidad suficiente como para que sea comunicada al interesado. [MOTIVAR]