INTERBEL S)

2017

La LOPD y el archivo del correo electrónico

Interbel S)

www.interbel.es

902 39 39 39

INTERBEL

LAS OBLIGACIONES DE LA LOPD SOBRE EL ARCHIVO DEL CORREO ELECTRÓNICO

PARA CUMPLIR CON LA LOPD

El correo electrónico en una empresa incorpora contenido en el propio cuerpo del mensaje además de los documentos adjuntos que pueda llevar. En este sentido, **el email puede constituir en sí mismo un fichero de datos personales completo estando plenamente sujeto a la normativa de protección de datos.**

Dependiendo de la actividad de la empresa, sus correos electrónicos podrán incorporar datos personales más o menos sensibles.

La sanción que se aplica depende del nivel de seguridad exigible en función el tipo de información que contienen los correos electrónicos:

NIVEL SEGURIDAD EXIGIBLE	OBLIGADOS	TIPO DE INFORMACIÓN
ALTO	Clínicas, hospitales, consultas médicas, laboratorios, sindicatos, partidos políticos, abogados y procuradores, prisiones y comisarias.	Informes médicos, datos de salud, información de accidentes, datos sobre infracciones administrativas o penales, datos de afiliación sindical.
MEDIO	Administraciones tributarias, entidades financieras, entidades gestoras, aseguradoras, mutuas de trabajo y accidentes, empresas de gestión de cobro, empresas de selección de personal.	Datos económicos y financieros, información sobre la solvencia patrimonial y crédito o cobro deudas, datos derivados de procesos de selección de personal.
BAJO	Cualquier empresa u organismo público que trate datos personales.	Cualquier tipo de dato personal.

ASPECTOS TÉCNICOS

1. La empresa debe realizar copias de seguridad de su correo electrónico como mínimo semanalmente.
2. Deberá conservarse una copia de respaldo del correo electrónico y de los procedimientos de recuperación del mismo en un lugar diferente de aquel en que se encuentren los equipos informáticos que lo tratan.
3. El envío y acceso al correo electrónico debe realizarse cifrando los datos que contiene o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

LAS COPIAS DE SEGURIDAD

Las copias de seguridad (Backups) pueden no ser suficientes para llevar a cabo la protección que exige la ley:

1. Los procesos de Backup no realizan copias de los emails que hayan sido borrados entre copia y copia de seguridad.
2. Suele ocurrir que las copias realizadas se conservan durante un máximo de seis meses y se vuelven a reutilizar para copiar encima.
3. Con los Backups existen riesgos de vulnerabilidad y manipulación de datos.
4. Accesibilidad y permisos no quedan delimitados

LA SOLUCIÓN

Con un **sistema de archivo y control** de los correos electrónicos podrá cumplir con las medidas de seguridad clasificadas en nivel básico, medio y alto en función de la tipología de datos tratados.

1. Se realizan copias automáticas instantáneas.
2. Copia de todos los correos electrónicos entrantes y salientes incluidos los cuerpos del mensaje y los adjuntos (se realiza compresión de los datos para reducir hasta un 70% el espacio).
3. No son manipulables.
4. Permisos de alta seguridad.

A continuación se detallan las CONDICIONES DE ALMACENAMIENTO DEL CORREO ELECTRÓNICO para cumplir con la LOPD, un informe elaborado por Derecho.com con el patrocinio de Interbel.

CONDICIONES DE ALMACENAMIENTO DE LOS CORREOS ELECTRÓNICOS PARA CUMPLIR CON LA LOPD

El correo electrónico en una empresa puede constituir en sí mismo un fichero[1] de datos personales completo o bien parte de uno más amplio, estando en todo caso plenamente sujeto a la normativa de protección de datos. Esto implica que el correo electrónico debe almacenarse cumpliendo los siguientes requisitos legales:

1. **Conservación, localización y consulta:** La empresa debe almacenar sus correos electrónicos de forma que quede garantizada su correcta conservación, la localización y consulta de la información y se posibilite el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

> El que una empresa impida u obstaculice el ejercicio de los derechos de acceso, rectificación, cancelación y oposición que cualquier persona puede ejercitar ante ella, constituye una infracción tipificada como grave en el artículo 44.3.e) de la LOPD, sancionable con multa de 40.001 a 300.000 euros.

2. **Medidas de seguridad:** Dependiendo de la propia actividad de la empresa, sus correos electrónicos podrán incorporar datos personales de naturaleza más o menos sensible. En este sentido, el RLOPD (artículos 89 a 104) establece una serie de medidas de seguridad concretas, clasificadas en niveles **básico**, **medio** y **alto**, que la empresa debe cumplir en relación al almacenamiento de dichos correos.

   A continuación se enumeran las medidas de seguridad de índole técnica que deberán cumplirse:

[1] Art. 5.1.k) RLOPD: *"Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso."*

2.1. MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO:

Estas medidas de seguridad deben ser cumplidas por todas las empresas, independientemente del tipo de datos personales que contengan sus correos electrónicos.

a) Registro de incidencias

Debe existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal contenidos en los correos electrónicos, estableciendo un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

b) Control de acceso

La empresa debe dotar de acceso al correo electrónico sólo a aquellos empleados que lo precisen para el desarrollo de sus funciones. En este sentido, es obligatorio que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

De igual modo, el personal de la empresa con privilegios para conceder, alterar o anular el acceso autorizado al correo electrónico debe estar identificado en el Documento de Seguridad de la empresa.

c) Gestión de soportes y documentos

Si los correos electrónicos de la empresa se copiasen o almacenasen en algún soporte (cintas de backup, pendrives, unidades de disco duro externas, etc.), éste deberá permitir identificar el tipo de información que contiene, ser inventariado y sólo deberá ser accesible por el personal autorizado para ello en el Documento de Seguridad de la empresa.

Por otro lado, tanto la salida de dichos soportes fuera de las instalaciones de la empresa, como el simple envío de correos electrónicos con datos personales desde la misma, deberá ser autorizada por la empresa o encontrarse debidamente autorizada en su Documento de Seguridad.

Siempre que vaya a desecharse alguno de los citados soportes, deberá procederse a su destrucción o borrado mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en ellos o su recuperación posterior.

d) Identificación y autenticación

La empresa debe adoptar las medidas que garanticen la correcta identificación y autenticación, inequívoca y personalizada, de los usuarios que tengan acceso al correo electrónico.

Así, cuando dichas medidas consistan en la existencia de contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Dichas contraseñas deben cambiarse con una periodicidad que no puede superar el año.

e) Copias de respaldo y recuperación

La empresa debe realizar copias de seguridad de su correo electrónico como mínimo semanalmente, estableciendo procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En este sentido, la empresa debe verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2.2. MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:

Estas medidas de seguridad, sumadas a las correspondientes al nivel básico que se han indicado anteriormente, deben ser aplicadas por todas aquellas empresas cuyo correo electrónico contenga datos relativos a la comisión de infracciones administrativas o penales. También debieran aplicar este nivel de seguridad las empresas dedicadas a prestar servicios de información sobre la solvencia patrimonial y el crédito de las personas o bien al cobro de deudas dinerarias; las Administraciones tributarias; las entidades financieras; las Entidades Gestoras y Servicios Comunes de la Seguridad Social y las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

a) Responsable de seguridad

En el Documento de Seguridad debe designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo para el correo electrónico.

b) Auditoría

Los sistemas de información e instalaciones de tratamiento y almacenamiento del correo electrónico deben someterse, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad que le son aplicables.

c) Gestión de soportes

Debe establecerse un sistema de registro de entrada de los soportes que contengan correos electrónicos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

Igualmente debe disponerse de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

d) Identificación y autenticación

La empresa debe establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al correo electrónico.

e) Control de acceso físico

Exclusivamente el personal autorizado en el Documento de Seguridad de la empresa puede tener acceso a los lugares donde se hallan instalados los equipos físicos que dan soporte al correo electrónico.

f) Registro de incidencias

En el registro de incidencias ya visto para el nivel básico de seguridad deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2.3. MEDIDAS DE SEGURIDAD DE NIVEL ALTO:

Estas medidas de seguridad, sumadas a los correspondientes niveles, básico y medio, que se han indicado anteriormente, deben ser aplicadas por todas aquellas empresas cuyo correo electrónico contenga datos relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, o bien datos derivados de actos de violencia de género.

a) Gestión y distribución de soportes

La identificación de los soportes que contengan correos electrónicos se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes identificar su contenido, y que dificulten la identificación para el resto de personas.

La distribución de los soportes se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

b) Copias de respaldo y recuperación

Deberá conservarse una copia de respaldo del correo electrónico y de los procedimientos de recuperación del mismo en un lugar diferente de aquel en que se encuentren los equipos informáticos que lo tratan.

c) Registro de accesos

Cada vez que alguien intente acceder al correo electrónico de la empresa se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

El período mínimo de conservación de los datos registrados será de dos años.

d) Telecomunicaciones

El envío y acceso al correo electrónico debe realizarse cifrando los datos que contiene o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Finalmente, hay que recordar que en caso de que exista personal ajeno a la empresa que tenga acceso a su correo electrónico (como por ejemplo el personal de un proveedor del servicio de mensajería) deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Tratar el correo electrónico de la empresa sin tener habilitadas las medidas de seguridad que se han indicado, constituye una infracción tipificada como grave en el artículo 44.3.h) de la LOPD, sancionable con multa de 40.001 a 300.000 euros.

Entre las soluciones que hay en el mercado para el Archivo del Email, en Interbel aconsejamos el Archivado de correo **Mailstore,** con el que podrá salvaguardar toda la información de su empresa que reside en el correo electrónico, ya sea en Outlook, Exchange, Gmail, Office365 o MDaemon, y encontrar cualquier email, por antiguo que sea, en un solo click, olvidándose de los archivos *pst. Su inmejorable relación calidad/ precio, lo convierte en el mejor Archivado de Correo del mercado.

Prueba GRATIS
30 días

Esta es una opinión legal, siempre y en todo caso sometida a mejor derecho.

SOBRE INTERBEL

Interbel, especialistas en Productividad para empresas y soluciones de Email Corporativo, cuenta con una experiencia de 20 años proporcionando software de calidad alrededor del correo electrónico y asesorando en la gestión del email, permitiendo ahorros de hasta un 70% de costes y un aumento de la productividad de más del 20%.

El Grupo Interbel tiene una red de 2.000 distribuidores y más de 4.000 clientes en España y Latinoamérica. Con presencia en Barcelona, Miami, Colombia, México y Argentina, y el respaldo de un gran servicio de asesoría y soporte técnico, garantiza soluciones de correo electrónico para que usuarios y empresas trabajen de modo más productivo con el email y la comunicación. Software, metodología y soluciones que proporcionan la seguridad, productividad y fiabilidad que las compañías buscan en el correo.

Contacto:

Vanessa Bosch
vanessa.bosch@interbel.es
marketing@interbel.es
Tfn: 902 39 39 39
Passeig de Gràcia, 120 3º 1ª
08008 Barcelona