INTERBEL S)

2014

La protección del correo electrónico en las Administraciones Públicas

Interbel S)

www.interbel.es

902 39 39 39

MEDIDAS DE SEGURIDAD SOBRE LOS CORREOS ELECTRÓNICOS EN LAS ADMINISTRACIONES PÚBLICAS

OBLIGACIONES

Las Administraciones Públicas españolas además de cumplir con la LOPD en cuanto a las obligaciones de almacenaje y normas de seguridad, están sometidas al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica

http://legislacion.derecho.com/real-decreto-3-2010-por-el-que-se-regula-el-esquema-nacional-de-seguridad-en-el-ambito-de-la-administracion-electronica

El plazo para la adecuación de las Administraciones Públicas a esta norma venció el pasado 30 de enero de 2014.

PARA CUMPLIR CON LA LOPD

El correo electrónico en una Administración Pública 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 Administración, sus correos electrónicos podrán incorporar datos personales más o menos sensibles.

Con este 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.

OTRAS OBLIGACIONES LEGALES SOBRE EL ARCHIVO DEL CORREO ELECTRÓNICO

El funcionamiento normal de las Administraciones Públicas conlleva que se envíen y reciban multitud de documentos, cosa que, cada vez con mayor frecuencia, se lleva a cabo a través correo electrónico. Muchas veces el propio cuerpo del mensaje del email contiene toda la información que se envía o recibe, sin incorporar documentos adjuntos.

En este sentido, existen múltiples disposiciones legales que obligan a conservar durante un determinado plazo de tiempo ciertos documentos y comunicaciones. A continuación se exponen otras obligaciones relevantes:

1. Documentos Contables:

   Código de Comercio, Ley General Tributaria, Ley del Impuesto de Sociedades

2. Relaciones Laborales:

   Orden del Modelo de Recibo Individual de Salarios, Ley sobre Infracciones y Sanciones en el Orden Social

3. Documentación Contractual:

   Código Civil

A continuación se detallan las MEDIDAS DE SEGURIDAD DEL CORREO ELECTRÓNICO PARA LAS ADMINISTRACIONES PÚBLICAS, las CONDICIONES DE ALMACENAMIENTO DEL CORREO ELECTRÓNICO para cumplir con la LOPD, y OTRAS NORMAS de obligado cumplimiento. Este es un informe elaborado por Derecho.com con el patrocinio de Interbel.

1. LAS ADMINISTRACIONES PÚBLICAS Y EL CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

Las Administraciones públicas españolas están sometidas al cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (en adelante, "**Esquema Nacional de Seguridad**"), que determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos previstos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

> En el supuesto de que una Administración pública incumpla lo dispuesto en el Esquema Nacional de seguridad, se derivarán las responsabilidades pertinentes de conformidad con lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Básicamente, el Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos que permiten una protección adecuada de la información, asegurando el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que las Administraciones públicas gestionan en el ejercicio de sus competencias.

Con dicha finalidad, el **Anexo II** del Esquema Nacional de Seguridad establece toda una serie de medidas de seguridad que las Administraciones públicas deben aplicar proporcionalmente a las dimensiones de seguridad relevantes en el sistema a proteger y a la categoría del sistema de información a proteger.

Así, por ejemplo, las medidas de seguridad tendentes a proteger el correo electrónico resultan aplicables a todas las dimensiones de seguridad existentes, es decir, en todos los casos. Dichas medidas de seguridad son (apartado 5.8.1 del Anexo II):

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.

b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1.º Correo no solicitado, en su expresión inglesa «spam».

2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.

3.º Código móvil de tipo «applet».

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1.º Limitaciones al uso como soporte de comunicaciones privadas.

2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

INTERACCIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD CON EL RLOPD:

Además de adecuarse a lo establecido en el Esquema Nacional de Seguridad, cuando el sistema/servicio/tratamiento también esté sometido al RLOPD deberá adecuarse de forma independiente a sus exigencias.

En este sentido, debe tenerse en cuenta que las denominaciones *básico/medio/alto* que utilizan ambas normas no hacen referencia a lo mismo. Así, en el caso del RLOPD el nivel de seguridad aplicable se determina en función de la concreta naturaleza del dato personal tratado, mientras que en el Esquema Nacional de Seguridad el nivel de seguridad se determina en función del impacto que un incidente de seguridad podría tener en relación con la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto a la legalidad y a los derechos de los ciudadanos.

SUJECIÓN DEL PROVEEDOR EXTERNO DEL SERVICIO DE MENSAJERÍA AL ESQUEMA NACIONAL DE SEGURIDAD:

Cuando una Administración pública contrate la prestación del servicio de mensajería a un proveedor externo, deberá asegurarse de que dicho proveedor cumple con los requisitos establecidos por el Esquema Nacional de Seguridad. En este sentido, dicha obligación para el proveedor se incluirá en el preceptivo contrato que ambas partes formalicen, reservándose además la Administración pública la facultad de auditar al proveedor para verificar tal circunstancia.

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

El correo electrónico en una Administración Pública 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:

- **Conservación, localización y consulta:** La Administración 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.

- **Medidas de seguridad:** Dependiendo de la propia actividad de la Administración, 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."*

MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO:

Estas medidas de seguridad deben ser cumplidas por todas las Administraciones Públicas y 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.

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.

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.

3. OBLIGACIÓN DE CONSERVACIÓN DE LIBROS Y DOCUMENTACIÓN CONTABLE.

Si envía o recibe facturas por email, pedidos o cualquier otro tipo de documentación y justificantes tiene que tener en cuenta la siguiente normativa.

El **artículo 30 del Código de Comercio** establece que los empresarios conservarán los libros, correspondencia, documentación y justificantes concernientes a su negocio, debidamente ordenados, durante **seis años**, a partir del último asiento realizado en los libros. Esta obligación, que no desaparece aunque la empresa cese en el ejercicio de sus actividades, no sólo hace referencia a los libros oficiales.

El cese del empresario en el ejercicio de sus actividades no le exime del deber de conservación de libros y demás documentación, y si hubiese fallecido recaerá sobre sus herederos. En caso de disolución de sociedades, serán sus liquidadores los obligados a cumplir lo prevenido.

La legislación tributaria, sin embargo, define otros plazos. **La Ley General Tributaria** establece que prescriben a los **cuatro años**, la acción de la Administración para determinar la deuda tributaria, para exigir el pago de deudas e imponer sanciones. Por tanto, según la normativa tributaria, deben conservarse los libros, documentos y justificantes durante 4 años, que es el periodo de prescripción.

Así mismo, la **Ley del Impuesto de Sociedades** permite compensar bases imponibles negativas durante **15 años** para los periodos impositivos iniciados a partir de 1 de enero de 2002, y durante ese tiempo de compensación, la Administración puede exigir la acreditación de bases negativas mediante la exhibición de la contabilidad y soportes documentales.

- Ver artículo 30 del Código de Comercio.
- Ver artículos 66 y 67 de la Ley 58/2003, de 17 de diciembre, General Tributaria.
- Ver artículo 25 del R.D. Leg. 4/2004, de 5 de marzo, por el que se aprueba el Texto refundido de la Ley del Impuesto de Sociedades.

4. OBLIGACIÓN DE CONSERVACIÓN DE RECIBOS DE SALARIOS Y DOCUMENTOS DE COTIZACIÓN.

Si envía o recibe las hojas de salarios y/o las altas y bajas de la Seguridad Social por email, tiene que tener en cuenta la siguiente normativa.

El **artículo 3 de la Orden de 27 de diciembre de 1994 por la que se aprueba el Modelo de Recibo Individual de Salarios**, establece que las empresas deben archivar y conservar los recibos de salarios y boletines de cotización a la Seguridad Social durante un periodo mínimo de **cinco años**. En este sentido, hay que tener en cuenta que actualmente muchas empresas reciben los recibos de salarios elaborados por sus gestorías a través de correo electrónico.

Así mismo, tal y como recoge el art. 21 del Real decreto Legislativo 5/2000, de 4 de agosto, **Ley sobre Infracciones y Sanciones en el Orden Social**, no conservar durante cuatro años la documentación o los registros o **soportes informáticos en que se hayan transmitido** los correspondientes datos que acrediten el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran en relación con dichas materias, así como los documentos de cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones.

- Ver artículo 3 de la Orden por la que se aprueba el Modelo de Recibo Individual de Salarios.
- Ver artículo 21 del R.D. Leg. 5/2000, de 4 de agosto, Ley sobre Infracciones y Sanciones en el Orden Social.

5. OBLIGACIÓN DE CONSERVACIÓN DE LA DOCUMENTACIÓN CONTRACTUAL.

Cualquier email enviado o recibido en el que se llegue a un acuerdo entre dos partes, puede considerarse un documento contractual.

La documentación contractual enviada y/o formalizada con clientes y proveedores debería conservarse mientras duren las obligaciones contenidas en ella.

Además, no hay que olvidar que a pesar de haber finalizado la vigencia del contrato, los plazos de prescripción de las acciones civiles que pueden derivarse de los mismos, previstas en los **artículos 1.930 y siguientes del Código Civil**, pueden alcanzar los **30 años**.

> En conclusión, resulta importante dotar a la empresa de un sistema de retención del correo electrónico acorde con los diversos plazos de conservación documental legalmente establecidos. No hacerlo puede privar a la empresa de los elementos probatorios necesarios en un procedimiento judicial, arbitral o, incluso, ante una eventual inspección oficial de algún organismo de la Administración.

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 mejorar la Comunicación y la Productividad en empresas con soluciones de Email, cuenta con una experiencia de más de 18 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 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