Prólogo

El correo electrónico es, hoy en día, un medio de comunicación utilizado frecuentemente entre empresas para el intercambio de información.

El grupo ALDI Supermercados mantiene contacto, a través del correo electrónico, con un gran número de interlocutores.

Generalmente la información que se intercambia por e-mail es confidencial, por lo que debe ser protegida contra el uso indebido y la manipulación de terceros. Si no se protegen correctamente los mensajes de correo electrónico, la transferencia de datos a través de internet entre remitente y destinatario se podría comparar con la seguridad de una simple postal enviada por correos. Es por ello que las medidas de seguridad adicionales resultan imprescindibles para proteger la comunicación por medio de e-mails de manera eficaz. Con este fin, ALDI Supermercados utiliza un procedimiento estándar para el intercambio de correos electrónicos codificados.

A través de este documento, el grupo ALDI Supermercados le quiere facilitar toda la información necesaria para garantizar un medio de comunicación seguro con nosotros.

A continuación le aclararemos los términos relevantes en relación con la codificación del e-mail y le explicaremos los pasos básicos para la configuración e instalación de un sistema de comunicación seguro.

Al final del presente documento presentaremos dos propuestas para que se pueda poner en contacto con ALDI Supermercados a través de un e-mail codificado. Las instrucciones para ello las encontrará en las últimas páginas de este archivo.

Para cualquier duda o cuestión en lo que concierne la codificación de los e-mails, rogamos se pongan en contacto con el departamento informático de su empresa.

Codificación

Con el fin de mantener la confidencialidad en la comunicación por correo electrónico, los e-mails se deben enviar de manera codificada.

La información necesaria para codificar/encriptar y descifrar los mensajes se halla contenida en lo que denominamos certificado; éste contiene a su vez las claves públicas para la codificación (para todos los contactos) así como la clave privada (solamente para el usuario del e-mail ALDI) para el descifrado de los e-mails en cuestión. Por ello, antes de que comience la comunicación segura, tanto destinatario como remitente deben disponer de las claves públicas el uno del otro.

Claves públicas y privadas

Un certificado se compone de dos partes: una clave pública y una privada. La clave privada se utiliza para firmar y descifrar los e-mails y no debe revelarse nunca.

Al interlocutor de ALDI debe proporcionársele una clave pública, para que pueda verificar la firma de un e-mail y para que pueda reenviar un e-mail codificado al propietario de la clave pública.

Antes de la primera codificación de un correo electrónico, el remitente debe haber recibido la clave pública. Este intercambio suele hacerse mediante el envío de un correo electrónico con firma en el que el destinatario puede ver la clave pública. Sólo entonces el remitente puede codificar el correo electrónico con la clave pública del destinatario.

Después de recibir el correo electrónico codificado, el destinatario podrá descifrarlo con su clave privada. Estas operaciones las realizan la mayoría de programas de correo electrónico de manera automática.

Firmas

Para verificar la autenticidad de una dirección de correo electrónico es necesaria una firma digital. El remitente de un correo electrónico puede identificarse a través de la firma.

De esta manera se garantiza la seguridad y la integridad de la dirección de correo, ya que en el caso de cambios posteriores la firma digital será destruida.

Es por ello que siempre se añade la clave pública del certificado al correo electrónico, para que el destinatario pueda verificar la autenticidad e integridad del correo.

Al firmar un correo electrónico, la información contenida no podrá ser cambiada sin que el destinatario se dé cuenta; no obstante dicho correo podrá leerse libremente. Para garantizar la confidencialidad durante el intercambio de información, el e-mail se tiene que codificar. El método más seguro para el envío de correos electrónicos es la combinación de una firma y la codificación.

S/MIME

(Secure/Multipurpose Internet Mail Extensions) es un método estándar utilizado a nivel mundial para el intercambio de información segura a través del correo electrónico con certificado. Los componentes necesarios para S/MIME ya están integrados en la mayoría de los programas para correo electrónico modernos, de modo la aplicación simple y transparente de éstos queda garantizada. Esto significa que mediante la activación de la correspondiente opción en el programa de correo electrónico, los e-mails se codificarán automáticamente al enviarse y, a su vez, automáticamente descifrados al recibirse.

ALDI Supermercados solamente aceptará el método S/MIME para la codificación de los correos electrónicos.

Proveedores de servicios de certificados/Trustcenter

El proveedor de certificados (p.ej.: Trustcenter) es una organización que emite certificados digitales y que asume la responsabilidad de su implementación, asignación e integridad.

Si Ud. dispone de un sistema de correo electrónico compatible con el S/MIME pero no dispone aún de un certificado, lo podrá solicitar a un proveedor de certificados. En el anexo encontrará una visión general y un listado de los proveedores de confianza de ALDI Supermercados.

Certificado raíz

Además del certificado de cada uno de los usuarios, la comunicación por correo electrónico con ALDI Supermercados también requiere de un certificado patrón. Con éste, se podrá verificar el estado de confianza de los certificados de ALDI. Esto significa que el sistema utilizado por Ud. podrá verificar si el certificado realmente proviene de ALDI Supermercados y si sigue siendo válido.

Intercambio de certificados:

El intercambio de certificados entre los interlocutores sólo se llevará a cabo una primera vez, que es cuando se codifica el correo electrónico.

Sólo será necesario repetir este paso cuando uno de los certificados intercambiados pierda su validez.

Cómo enviar el certificado al grupo ALDI Supermercados:

Cuando su proveedor de servicios certificados (Trustcenter) le haya proporcionado su certificado personal del listado adjunto, y Ud. haya introducido su clave pública en el servidor de Trustcenter (véase instrucciones, punto 2.1), éste solicitará automáticamente su clave pública.

Si no hubiera guardado su clave pública en el servidor de claves del proveedor de certificados (Trustcenter), puede introducir dicha clave en el portal de certificación ALDI (www.aldi-nord.de/certportal).

Si su certificado de usuario hubiera cambiado, debido por ejemplo a una modificación del proveedor de certificados, se deberá repetir este proceso.

Recibir los certificados de ALDI Supermercados:

El certificado de usuario se recibe automáticamente con cada correo electrónico codificado enviado por su persona de contacto de ALDI. Además, también se pueden descargar los certificados de sus interlocutores a través del portal de certificación de ALDI (www.aldi-nord.de/certportal) , introduciendo la/s dirección/es exacta/s de la/s persona/s de contacto.

El certificado patrón, que también recibe automáticamente a través de un correo electrónico de ALDI, sólo se debe importar una vez a su ordenador.

El certificado de usuario se asigna al contacto correspondiente de correo electrónico (véase instrucciones, punto 2.5).

El certificado patrón de ALDI Supermercados se puede descargar a través del portal certificado ALDI (www.aldi-nord.de/certportal) , o bien puede recibirlo de manera automática con cada e-mail codificado (como archivo adjunto) que le envíe su persona de contacto de ALDI (Véase Instrucciones, punto 4).

Webmessenger:

Mediante el portal de Webmessenger, los interlocutores de ALDI reciben acceso a un "E-Mail-Cliente", siempre a través de una conexión a internet segura. Gracias a este mail de cliente, los proveedores de ALDI pueden enviar y recibir mails de los trabajadores de ALDI.

A continuación se explican de nuevo los procesos de comunicación segura con ALDI Supermercados. Para el óptimo uso de la comunicación segura a través de correo electrónico recomendamos la primera propuesta.

1ª Propuesta

Hasta ahora, Ud. no tiene ningún contacto de correo electrónico seguro con ALDI Supermercados (ni tampoco acceso al Webmessenger) y quiere establecer comunicación a través de correo electrónico codificado (intercambio de claves a través de la publicación de la clave pública en el servidor de claves del proveedor de certificados Trustcenter).

1. **Solicite** su certificado S/MIME personal de un Trustcenter del listado anexo (publique su clave pública en el servidor de claves del Trustcenter) (véase instrucciones, punto 2.1 y 2.2)

2. **Asigne** el certificado a su cuenta de correo electrónico personal, dentro de las opciones de su software para correo electrónico (véase instrucciones punto 2.4).

3. **ALDI Supermercados** consulta al servidor de claves de los Trustcenter indicados en el anexo y utiliza su clave pública (no se requiere ninguna acción por su parte).

4. **Recibirá** un correo electrónico codificado de un interlocutor de ALDI Supermercados. El correo incluye el certificado del interlocutor así como el certificado patrón

5. **Cree** un contacto para el interlocutor de ALDI Supermercados en el programa de correo electrónico y asigne el certificado correspondiente al contacto creado (véase instrucciones punto 2.5).

6. **Elija** la opción de codificación S/MIME cuando redacte un correo electrónico al colaborador de ALDI (véase instrucciones punto 2.4).

2ª Propuesta

Su persona de contacto de ALDI ya le ha facilitado el acceso a Webmessenger y ya puede enviar e-mails seguros a sus contactos de la empresa.

Listado de proveedores de certificados/Trustcenter de confianza:

Swiss Sign	https://www.swisssign.com/
Producto	Personal ID Silver
Certificados patrones de confianza son:	SwissSign Gold CA SwissSign Gold CA G2 SwissSign Gold Root CA SwissSign Gold Personal CA G3 SwissSign Silver CA G2 SwissSign Silver Root CA SwissSign Silver Personal CA G3

ALDI Nord patrones de confianza

1. ALDI Nord
   S/MIME certificado patron
   Válido a partir de 04.12.2015

   SHA1: `a06a c71d b800 e8d9 56c3 c3e5 9ed0 bc3f 0ce0 b6d3`
   MD5: `bfd1 22f4 f721 197c 0860 38fc eef2 0752`

2. ALDI Nord
   S/MIME certificado patron
   Expira el 06.01.2016

   SHA1: `e072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43`
   MD5: `542b b140 189c 0d0a d146 0007 e677 a6ed`