NORMAS DE USO DE LOS SISTEMAS DE INFORMACIÓN

Sistemas de Gestión de Seguridad de la Información

Nombre:	NOR-SG-SI-02-03 Normas de uso de los sistemas de información
Título:	NORMAS DE USO DE LOS SISTEMAS DE INFORMACIÓN
Edición:	V.1
Clasificación:	Interno
Estado:	Publicado
Fecha:	24/02/2017
Página:	1/12
Editado por:	Responsable de seguridad
Revisado por:	Responsable de seguridad
Aprobado por:	Dirección

ÍNDICE

1. INTRODUCCIÓN

Este manual pretende que el usuario final conozca:

- Su situación respecto al uso de los sistemas de información de **AIXA CORPORE, S.L.** (En adelante **AIXA CORPORE**).
- Por qué la seguridad de la información es importante para **AIXA CORPORE**.
- Los riesgos que con llevan la inseguridad.
- Los requisitos legales actuales que obligan a garantizar la seguridad de datos.
- Las normas básicas implantadas.
- Recomendaciones y buenas prácticas a utilizar.

1.1. DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN

Un ordenador, un programa y unos datos constituyen los elementos básicos de un sistema de información. Los ordenadores de **AIXA CORPORE** están conectados por medio de equipos de comunicación a una red informática. Cada usuario con necesidades informáticas dispondrá de un ordenador personal conectado a red que llamaremos puesto de trabajo. Otros dispositivos como las impresoras, pueden conectarse a dicho ordenador o a la red.

El conjunto de esta estructura (puestos de trabajo, red informática, servidores, programas) sirve para almacenar, procesar y transmitir datos e informaciones. Todos estos elementos asociados forman un sistema automatizado de información, que llamaremos abreviadamente S.I. Dentro de este sistema tú eres el usuario de un puesto de trabajo.

Si un sistema de información deja de funcionar, se crea normalmente un gran problema; puede ser tan grave que lleve a la práctica paralización de la Entidad. Nuestra organización tiene una dependencia cada vez mayor de los sistemas informáticos, y estos sistemas son vulnerables a agresiones o fallos. La necesidad de la seguridad y del control es evidente.

1.2. PROBLEMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de un sistema de información consiste en preservar la disponibilidad, la confidencialidad y la integridad de datos y programas. Estos factores pueden ponerse en peligro por actos voluntarios o involuntarios de origen interno o externo. Una parte importante de la pérdida se debe a errores humanos y accidentes.

1.2.1. PROBLEMAS DE SEGURIDAD FÍSICA

- Catástrofes: incendios, terremotos, inundaciones.
- Fallos en los elementos físicos: cortes de fluido eléctrico, averías en los elementos de sistema (ordenador, discos, elementos de comunicaciones, líneas telefónicas).
- Fallos en el software de base o de aplicación: mal funcionamiento de los programas, o del sistema operativo, del control de las comunicaciones.
- Sabotajes: Destrucción de elementos físicos, daños al software del sistema, introducción de virus.

1.2.2. PROBLEMAS DE CONFIDENCIALIDAD

- Accesos no autorizados a informaciones confidenciales.
- Accesos no autorizados para obtener copias piratas de programas.
- Accesos no autorizados para modificar datos de aplicaciones, en provecho propio o como sabotaje (modificación de datos bancarios, nóminas, expedientes, destrucción de información).

1.2.3. UTILIZACIÓN INDEBIDA DEL ORDENADOR

- Juegos, trabajos particulares y/o para otra entidad, etc.

- Permitir por ingenuidad el acceso desde el exterior a usuarios maliciosos que adquieren el control remoto sobre un ordenador de la entidad.

En una sociedad sin tecnología informática se establecen mecanismos adecuados de seguridad para minimizar sus riesgos: se protegen los archivos para evitar su robo o destrucción, se elaboran leyes para proteger la intimidad, los datos de carácter personal y la propiedad intelectual.

Se pueden indicar cuatro niveles de protección:

1. Prevención de riesgos
2. Detección de problemas cuando han fallado los mecanismos de prevención
3. Limitación de pérdidas: si a pesar de los controles de prevención y detección, ocurre el problema, restringir las pérdidas en lo posible.
4. Recuperación: planes de contingencia totalmente probados y documentados para volver a disponer del sistema de información.

1.2.4. ¿CUÁLES SON ENTONCES LAS FUNCIONES REFERENTES A LA SEGURIDAD QUE DEBE REALIZAR EL RESPONSABLE DE UN PUESTO DE TRABAJO?

- El conocimiento de la propiedad de los datos a los que accede y quiénes pueden disponer de estos datos; quién está autorizado a pedirle una salida de impresora o a que se le facilite en pantalla una determinada información.
- Del conocimiento de la propiedad de los datos se deduce el nivel de importancia de la información que se maneja y en función de ello se tendrá cuidado para evitar que sea visualizada, fotocopiada, duplicada, con atención incluso de forma especial a la que se deposita en las papeleras.
- Especial atención merece el uso de contraseñas que se describe en este documento en la sección "Criterios de Buenas Prácticas en Seguridad de la información".

2. NORMAS DE USO DE LOS SISTEMAS DE INFORMACIÓN.

A continuación se indican las normas de seguridad que todo usuario de **AIXA CORPORE** debe satisfacer. Estas normas se han organizado en la siguiente estructura:

- Normas generales de seguridad
- Normas para el cumplimiento de la LOPD
- Normas aplicables al uso de Internet.
- Normas aplicables al uso del correo electrónico.
- Buenas prácticas en materia de seguridad de la información
  - Selección de contraseñas
  - Uso del correo electrónico

A continuación se detallan cada una de estas secciones.

2.1. NORMAS GENERALES DE SEGURIDAD

Son normas para el personal en relación a la seguridad de la información de **AIXA CORPORE** las siguientes:

- El personal de **AIXA CORPORE** y cualquier otro personal que trabaje bajo contrato para ésta deberá acceder exclusivamente a aquella información que sea estrictamente necesaria para el desempeño de sus funciones.
- El acceso a información residente en los sistemas de información de **AIXA CORPORE** deberá realizarse siempre haciendo uso de un identificador de usuario, personal e intransferible, y de su palabra de acceso (contraseña) que deberá permanecer en secreto en todo momento y sólo podrá ser conocida por el empleado a quien se entrega su custodia.
- Bajo esta filosofía, **queda expresamente prohibida** la utilización de un mismo identificador de usuario y de su palabra de acceso por personas distintas a las que hubiera sido asignado. Es responsabilidad de cada empleado de **AIXA CORPORE** mantener en secreto su palabra de control de acceso y confeccionarla de forma que no sea adivinable por terceros, ya que **cualquier acceso indebido con dicho identificador será responsabilidad de su propietario**. **AIXA CORPORE** informará sobre criterios de buenas prácticas para la selección de contraseñas.
- Queda prohibido comunicar a otra persona el identificador de usuario y las claves de acceso a los sistemas de información. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del Responsable de Seguridad, con el fin de que le asignen una nueva clave. En los casos de ausencia temporal del usuario, el responsable de su unidad directiva podrá solicitar al Responsable de Seguridad correspondiente la asignación de los permisos necesarios a la persona por él designada a efectos de evitar la obstaculización de los trabajos en curso.
- La protección de los activos de **AIXA CORPORE** es una tarea que afecta a todas las personas vinculadas directa o indirectamente con la misma. Por tanto, es responsabilidad de todos preservar la disponibilidad e integridad de la información, comunicando a las áreas competentes y por los cauces establecidos, cualquier evento o incidencia que afecte a los sistemas de información.
- El usuario está obligado a utilizar los sistemas de información de **AIXA CORPORE, S.L.** y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la Empresa o de terceros, o que puedan atentar contra las normas sociales.

- Toda actividad realizada sobre los sistemas de información de **AIXA CORPORE** es susceptible de ser auditada.
- **AIXA CORPORE** prohíbe la divulgación, duplicación, modificación, destrucción, mal uso, robo y acceso no autorizado a información propiedad de **AIXA CORPORE** o de otras empresas y personas que le haya sido confiada.
- La utilización de los servicios de Internet y correo electrónico se llevará a cabo teniendo en cuenta que asociado al usuario está el nombre de **AIXA CORPORE**. Consecuentemente se guardarán patrones ejemplares de cortesía, educación y ética en su uso.
- Se establece expresamente la prohibición del uso de los activos de **AIXA CORPORE** para finalidades distintas a las estrictamente profesionales relacionadas con el desempeño habitual de las funciones en la misma y que no hayan sido expresamente aprobadas por la Dirección o no tengan una justificación evidente. Esto incluye tanto recursos informáticos (correo electrónico, Internet, ofimática, espacio en disco, etc.) como la información (de ciudadanos, de terceros, etc.).
- Debido a los peligros que tiene la utilización de software dañino o no autorizado, queda prohibida la instalación de aplicaciones que no se encuentren debidamente autorizadas por la Organización mediante los circuitos establecidos.

2.2. NORMAS PARA EL CUMPLIMIENTO DE LA LOPD.

Son obligaciones de todo trabajador de **AIXA CORPORE**, en relación al cumplimiento de la legislación vigente en materia de protección de datos las siguientes:

- **Deber de secreto**
  - Todo empleado debe guardar secreto de la información de carácter personal que conozca en el desempeño de su trabajo, incluso después de haber abandonado la organización.
  - Todo empleado debe proteger los datos de carácter personal de **AIXA CORPORE** que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en clientes, en el propio domicilio o en otras instalaciones alternativas y tanto en equipos fijos como en portátiles.
- **Identificación y autenticación de usuarios**
  - Cada usuario es responsable de los accesos que se hagan con su identificación, por ello es necesario que la contraseña se mantenga en secreto, no comunicándola a otros usuarios.
  - Cada usuario es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, debe registrarse como incidencia y proceder a su cambio. El usuario debe comunicar al **Responsable de TI** el olvido o sospecha de conocimiento por terceros de la contraseña.
  - Cambiar la contraseña al menos **semestralmente.**
- **Gestión de soportes**
  - No sacar fuera de los locales del fichero ningún soporte sin ser usuario autorizado para ello por el responsable del fichero y sin el correspondiente permiso del mismo para esa extracción en concreto.
  - No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, aplicando las medidas de seguridad que se hayan establecido.
  - No introducir en los locales del fichero ninguna información de carácter personal sin ser usuario autorizado para ello por **el Responsable de TI o por Dirección**

- Los documentos, disquetes y otros soportes de información deben guardarse en armarios cuando no se usen y, especialmente, fuera del horario normal de trabajo.
- La información crítica o sensible debe encerrarse bajo llave cuando no se requiera especialmente o la oficina esté vacía.
- Los ordenadores personales y los terminales deben estar protegidos por llave, contraseñas u otras salvaguardas cuando no se usen.
- No tirar a la basura documentos con información de carácter personal o sensible sin la previa destrucción.
- No hacer copias de seguridad de ninguna información, especialmente si se trata de datos de carácter personal, salvo que sea siguiendo las instrucciones del **Responsable de TI**
- Si requiriese hacer copia en algún dispositivo de almacenamiento extraíble (Tarjeta de memoria, discos externos USB, etc.) o sobre soporte CD o DVD, debe notificarlo al Comunicar al **Responsable de TI** el olvido o sospecha de conocimiento por terceros de la contraseña para su adecuado inventariado y la aplicación de las medidas de seguridad que éste estime pertinente.

- **Control de los accesos físicos**
  - Cuando el usuario de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su horario laboral, debe dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse, desconectándose de la aplicación o a través de un protector de pantalla que impida la visualización de los datos. Es recomendable activar el protector con Ctrl+Alt+Supr + Bloquear Estación). La reanudación del trabajo implica la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
  - En el caso de las impresoras, fax y dispositivos similares, debe asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de los ficheros, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
  - Si es necesario enviar por correo convencional información especialmente protegida, usar un sobre opaco o doble sin indicaciones externas y hacer el envío por un canal seguro. Se requerirá confirmación fiable de recepción por parte del destinatario.
  - Los usuarios deben respetar la configuración fija de aplicaciones corporativas (ofimática, antivirus,...) de los puestos de trabajo desde los que se tiene acceso a los ficheros y sólo podrá ser cambiada bajo la autorización del **Responsable de TI**.
- **Control de accesos lógicos**
  - Acceder únicamente a aquellos ficheros para los que haya sido autorizado por el Responsable del fichero y actuar sobre los mismos solamente con el alcance que le haya sido fijado.
  - Comunicar al **Responsable de TI** cualquier anomalía en el sistema de control de accesos implantado.
  - No instalar ningún software o programa no autorizado por el responsable de seguridad.
- **Comunicación interpersonal**
  - Se deben tomar las precauciones adecuadas, por ejemplo, no revelar información sensible para evitar la escucha o interceptación de su llamada

por personas de su vecindad próxima, sobre todo cuando se usa un teléfono móvil.

- No se deben mantener conversaciones confidenciales en lugares públicos o en oficinas abiertas o salas de tabiques finos.
- No se deben dejar mensajes en contestadores automáticos que puedan reproducirse por personas no autorizadas, grabarse en sistemas de uso público o grabarse incorrectamente como resultado de una equivocación en el marcado.
- En relación a las máquinas fax hay que tener en cuenta:
    1. El acceso no autorizado a los almacenamientos internos de mensajes para recuperarlos.
    2. La programación deliberada o accidental de las máquinas para enviar mensajes a números específicos.
    3. El envío de documentos y mensajes a un número equivocado, procedente de marcaje o de recuperación desde el almacenamiento de números.

- **Procedimiento de gestión de incidencias**
    - Cualquier usuario que tenga conocimiento de una incidencia de seguridad es responsable de su notificación mediante el procedimiento existente. El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del fichero por parte de ese usuario.

2.3. NORMA DE USO DE PORTATILES Y DISPOSITIVOS MOVILES

Dado el riesgo existente sobre este tipo de equipos, el usuario debe adoptar unas mínimas medidas preventivas de seguridad. Los equipos portátiles no deben:

- Abandonarse a la vista en coches particulares u otros medios de transporte utilizados.
- Dejarse a la vista en lugares públicos donde puedan ser sustraídos con facilidad.
- Los departamentos o áreas que utilicen equipos portátiles como puestos fijos deberán solicitar candados para fijar cada equipo a la mesa en donde vaya a ser utilizado.
- No se podrá utilizar un equipo portátil para trabajar con información de nivel CONFIDENCIAL en un lugar público.
- El usuario no podrá instalar software en equipo portátil entregado. Los equipos portátiles o puestos de teletrabajo homologados que vengan configurados, no podrán ser desconfigurados ni podrán instalarse en ellos ningún tipo de software no autorizado o realizar ningún tipo de manipulación cuyo objetivo sea inhabilitar cualquiera de las medidas de seguridad establecidas
- Cuando se vaya a dejar desatendido un portátil durante un periodo largo de tiempo, por ejemplo, por una reunión o ir a desayunar, el usuario debe:
    - Enganchar el portátil al candado disponible en su mesa. Si su despacho no dispone de uno, pero utiliza equipo portátil, deberá solicitarlo.
    - Cerrar la puerta de su despacho o área con llave si esta opción es posible.
    - En situaciones vulnerables como lugares públicos, salas de espera de aeropuertos, hoteles o salas de conferencia, el portátil no debe dejarse nunca desatendido.
    - No deben guardarse equipos portátiles en bolsas o maletas que puedan revelar que contienen elementos de valor en su interior para no atraer a ladrones.

- Cuando las medidas anteriores no puedan aplicarse por ser inviables o inapropiadas, el propietario del equipo es responsable de adoptar todas las medidas y precauciones que considere razonables con el objetivo de minimizar los riesgos de daño o robo del equipo.

2.4. NORMAS APLICABLES AL USO DE INTERNET.

Son normas aplicables al uso de Internet por parte de todo trabajador de **AIXA CORPORE**, las siguientes:

- Los sistemas de comunicación y acceso a la Internet son propiedad de **AIXA CORPORE** y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de **AIXA CORPORE** y nunca con fines no oficiales o para actividades personales o con ánimo de lucro.
- Las operaciones realizadas a través de la Internet pueden generar responsabilidad por parte de **AIXA CORPORE**, por lo que se reserva el derecho a auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso a la Internet y el contenido de lo accedido.
- El usuario debe respetar la legislación vigente (Ley de Propiedad Intelectual, Protección de Datos de Carácter Personal) y no utilizar el acceso a Internet con fines ilícitos o delictivos (acceso, uso y difusión de sitios de contenido ilegal: pornografía infantil, odio racial, terrorismo, etc.).

Son **usos no autorizados** en relación a la utilización de Internet los siguientes:

- Navegar por páginas Web cuyos contenidos sean sospechosamente delictivos, ni acceder a sitios Web que proporcionen servicios de chat, consulta y envío de correo vía Web, juegos on-line y otros contenidos no autorizados o expresamente bloqueados por **AIXA CORPORE**.
- Descargar contenidos protegidos por la Ley de Propiedad Intelectual sin la respectiva licencia o autorización de uso o reproducción.
- Instalar programas descargados de Internet sin la debida verificación por parte del antivirus de la no existencia de código malicioso en el programa descargado.

2.5. NORMAS APLICABLES AL USO DEL CORREO ELECTRÓNICO

- El sistema de correo electrónico es propiedad de **AIXA CORPORE** y es parte íntegra de sus sistemas de información, por lo que el mismo se reserva el derecho a auditar el uso adecuado del mismo.
- El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de trabajo. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen de **AIXA CORPORE** o sus empleados.
- **El correo electrónico no puede emplearse como medio para enviarse documentación corporativa a una cuenta privada.**
- **AIXA CORPORE** es responsable de establecer las normas mediante las cuales se asignan las cuentas de correo electrónico, incluyendo las medidas de seguridad aplicables, como son los códigos de acceso y las contraseñas, los controles de acceso al servidor, los sistemas para auditar el uso del sistema, la integridad y seguridad de los datos y las comunicaciones enviadas.
- Durante horas laborables, los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de **AIXA CORPORE**, a menos que estén autorizados a tal uso.

Son **usos no autorizados** en relación a la utilización del correo electrónico los siguientes:

- Reenviar mensajes en cadena o rumores no fiables (Hoax). Dada la velocidad de retrasmisión de mensajes, circulan a menudo rumores falsos o correos con contenido difamatorio que solicitan al receptor que reenvíe el correo para dar a conocer el contenido. No participe reenviando con este tipo de mensajes.
- Enviar correos electrónicos cuyo contenido no se ajuste a actividades relacionadas con los objetivos y actividades de **AIXA CORPORE**. Son ejemplos de este tipo de contenidos los juegos, animaciones, tarjetas de felicitación, ficheros de música, videos, etc.
- Enviar correos electrónicos publicitarios sin el consentimiento expreso del receptor del mensaje.
- Queda terminantemente prohibido utilizar el correo corporativo como medio para el envío de documentación a una cuenta externa a la empresa salvo si se encuentra el empleado correctamente autorizado para ello.

2.6. CRITERIOS DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

2.6.1. SELECCIÓN Y UTILIZACIÓN DE CONTRASEÑAS

Se consideran criterios de buenas prácticas respecto a la selección y utilización de contraseñas los siguientes:

- Mantener la confidencialidad de las contraseñas;
- Evitar el guardar un registro de la claves (por ejemplo en papel, en un fichero de software o en un dispositivo manual), a menos que este pueda ser almacenado de forma segura;
- Cambiar las contraseñas siempre que haya cualquier indicación de posible compromiso en el sistema o en la contraseña;
- Cambiar las contraseñas temporales en la primera entrada;
- No usar la misma contraseña para propósitos profesionales que para no profesionales.
- Seleccionar contraseñas de calidad con al menos la mínima longitud establecida y además:
    - sean fáciles de recordar;
    - no estén basadas en algo que alguien más pueda fácilmente adivinar u obtener usando la información relativa a la persona, por ejemplo nombres, números de teléfono, y fechas de nacimiento etc.;
    - no sean vulnerables a ataques de diccionario (por ejemplo, que no consistan en palabras incluidas en diccionario);
    - no contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos. No utilizar caracteres repetidos, bien todo números o todo letras. Una muy usual es 123456, aaaaaaa, qwertyuiop, etc.
    - no deben estar basadas en algo que pudieran adivinar u obtener usando información relacionada con usted, como nombre de hijos, fecha de nacimiento, número de teléfono, etc.
- Como recomendaciones de contraseñas de calidad se sugieren las siguientes:
    - Reglas nemotécnicas: LleSeupm (**L**a **l**luvia **e**n **S**evilla **e**s **u**na **p**ura **m**aravilla)
    - Palabra cambiada de orden: aremlap (palmera al revés)

- Mezcla de palabras: SagoCaos (Dos primeras letras y dos últimas letras de los nombres de los hijos/hermanos/padres) (Santiago y Carlos)
- Uso de caracteres para recordar frases: esto-es-solo-un-ejemplo, (otro-ejemplo).
- Sustituir números por letras como el 4 por la letra A, el 0 por la o y el 1 por la letra i: Buen4c0ntr4señ4.

2.6.2. USO DEL CORREO ELECTRÓNICO

Se consideran criterios de buenas prácticas en relación al uso del correo electrónico los siguientes:

- No abrir ni ejecutar ficheros que se reciban por correo electrónico especialmente si es un remitente desconocido, salvo que se tenga la total certeza de su inocuidad, y siempre después de revisarlo con el programa antivirus.
- No utilizar el correo electrónico para transmitir mensajes que contengan o lleven adjuntos datos de carácter que por sus características, volumen o destinatarios pudieran poner en peligro la confidencialidad.
- Ser profesional y cuidadoso en lo que escribe, sobre todo, cuando dichos correos electrónicos se dirijan a clientes o contactos de **AIXA CORPORE**. Para ello, lea cuidadosamente el texto del mensaje antes de enviarlo para evitar malas interpretaciones.
- Asegurar que los destinatarios de su correo son EXCLUSIVAMENTE las personas interesadas en el asunto del mismo.
- En el envío de correo hacia terceros, tratar de proteger su dirección de correo y la de sus compañeros siempre que esto sea posible. La difusión de virus y spam se realiza a partir de la exploración en PC infectados de direcciones de correo válidas. Evitar por tanto el reenvío de mensajes donde aparezcan las direcciones de correo de compañeros como parte del mensaje o en los campos de Copia. Siempre que sea posible, ocultar esta información utilizando el campo de copia oculta.
- En el reenvío de correo, revisar el cuerpo del mensaje, para no revelar a personas extrañas contenidos internos o confidenciales. El "reenvío de correo" debe siempre hacerse previa revisión del contenido íntegro del mensaje. En mensajes que hayan sido reenviados a usted, evitar que aparezca la secuencia de reenvíos en el texto del mensaje.
- Intentar no hacer pública tu dirección de correo. Además de las páginas Web esto es extensible a las listas de distribución, salas de chats, sitios Webs, etc. Si tiene que publicar tu dirección de correo utilice alguno de estos trucos:
    - Sustituir el símbolo @ por la palabra ARROBA (en mayúsculas) al dar la dirección de correo electrónico.
    - Añadir el texto "QUITALASMAYUSCULAS" después de la arroba si es obligatorio el carácter @
    - Leer y entender la política de privacidad cuando se suministre la dirección de e-mail en un sitio Web. Mirar si la política de privacidad permite a la compañía vender a terceras personas tu correo. Si esto fuera así, no envíe su dirección de correo a estos sitios. Si no existe Política de Privacidad, le parece sospechosa o no tiene claro quién es el responsable de un Web mejor no dar el e-mail.
    - Evitar el envío o almacenamiento en la cuenta de correo de ficheros que no estén relacionados con el trabajo. Normalmente correos con bromas, presentaciones PowerPoint o videos humorísticos consumen recursos corporativos en almacenamiento que no estén relacionados con el uso y

destino de los sistemas de información de **AIXA CORPORE**. Si se reciben este tipo de correos, eliminar el mismo una vez recibido o leído.

- El correo electrónico no es un sistema de almacenamiento de información sino de intercambio y comunicación. Por tanto, los documentos y archivos necesarios para el trabajo deben guardarse en carpetas de trabajo, no en el buzón de correo.
- Elimine periódicamente todos aquellos correos innecesarios o cuya información haya caducado y no sea útil. El buzón de correo tiene un tamaño limitado y por tanto, debe gestionar adecuadamente su uso.