ZURICH

POLITICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION

(V.NRD07)

PERSONAL EXTERNO

AIDE

Abril 2008

Política de Seguridad de los Sistemas de Información para "Aide Asistencia, Seguros y Reaseguros, S.A.", (en adelante la Compañía).

Autor: GITR-IT Spain
Fecha de efectividad: Abril de 2008

Nota: tanto esta Política como las otras que se hace referencia en este documento constituyen información propiedad de la Compañía y, por lo tanto, tienen carácter confidencial y únicamente está permitida su utilización y difusión por personal autorizado.

OBJETIVO

En toda organización existe Información altamente confidencial, cuya pérdida o uso indebido dañaría gravemente su reputación. Asimismo, el deterioro o indisponibilidad de los Sistemas de Información podría interrumpir el normal desarrollo de los procesos de negocio, produciendo efectos negativos en la calidad del servicio al cliente, la posición competitiva, o los beneficios de la Compañía.

El objetivo de esta Política es mitigar los riesgos asociados a los Sistemas de Información, describiendo lo que se espera del personal externo, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la Compañía.

La Política de Seguridad refleja requerimientos legales y éticos de la Compañía tanto en actuaciones informales de los empleados, como en la realización de los procesos de negocio. Por ello, concierne a todos los individuos de todos los niveles de la Organización.

Esta Política también contempla lo establecido en el artículo 89.1 del Real Decreto 1720/2007, de 21 de diciembre, con el objeto de dar el debido cumplimiento de sus obligaciones y que, al amparo de lo que establece el articulo 89.2, se pone en conocimiento de todo el personal externo de la Compañía la normativa de seguridad.

Se deberá firmar el formulario adjunto para verificar que han leído, comprendido y aceptado la Política de Seguridad antes de obtener acceso a la Red Corporativa y a los Recursos Informáticos de la Compañía.

Esta Política complementa en España a *"Zurinet Security Policy"* y al documento "*ZRPM: Riesgo de Reputación"* en los aspectos clave de confidencialidad de la información.

El alcance de esta Política cubre los Sistemas de Información y Redes de Comunicaciones con los que opera la Compañía, incluyendo hardware, software y componentes de datos.

POLÍTICA

Toda la información albergada en la red corporativa de la Compañía, de forma estática o circulando en forma de mensajes de correo electrónico, es propiedad de la Compañía y tiene el carácter de confidencial.

Tendrán el carácter de información especialmente reservada los secretos de negocio o comerciales de la Compañía, en los que se incluyen, sin carácter limitativo, los procedimientos, metodologías, código fuente, algoritmos, bases de datos de clientes, planes de marketing, y cualquier otro material que forma parte de la estrategia de negocio o comercial de la Compañía.

De forma rigurosa, todo el personal externo debe:

- Proteger los Sistemas de Información y Redes de Comunicaciones de la Compañía contra acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o robo.
- Proteger la Información confidencial, perteneciente o confiada a la Compañía, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso.
- Asegurar que las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.
- Asegurar la confidencialidad de la información almacenada en formato no electrónico.

Confidencialidad de la información

- Proteger la Información confidencial de la Compañía, evitando su envío al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.
- Los usuarios de los sistemas de información corporativos deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación contractual con la Compañía, y las Compañías pertenecientes al grupo, tanto en soporte material como electrónico. Esta obligación continuará vigente tras la extinción del contrato.
- Ningún personal externo deberá poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de la Compañía.
- En el caso de que por cualquier motivo, el personal externo entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, o titularidad o copia cobre la referida información. Asimismo, el personal externo deberá devolver dichos materiales a la Compañía, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización del contrato con la Compañía. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la Compañía, no supondrá, en ningún caso, una modificación de esta cláusula.
- El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos.

Propiedad intelectual e industrial

No está permitido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

Control de Acceso Físico

Para acceder a los locales, edificios/recintos donde se encuentren los sistemas informáticos de la Compañía se pasará por los sistemas de control de acceso físico, que impidan el acceso al personal no autorizado.

Solo al personal autorizado, le está permitido el acceso a lugares donde se almacena la información confidencial y los sistemas informáticos de la Compañía, y se le exige que lleven la tarjeta de acceso.

Sólo bajo la vigilancia de personal autorizado, el personal externo podrán entrar en lugares donde se almacena la información confidencial y los sistemas informáticos, y durante un corto periodo de tiempo.

Identificadores de Usuario y Contraseñas

Ningún Usuario recibirá un identificador de acceso a la Red de la Compañía, Recursos Informáticos o Aplicaciones, hasta que haya cumplimentado y firmado el formulario de aceptación y conocimiento de las Políticas de Seguridad actuales y lo haya remitido a Recursos Humanos.

- Se comunicarán los identificadores y las contraseñas temporales a los usuarios de una manera segura.
- Durante la primera operación de entrada a los Sistemas de Información, el Usuario deberá cambiar la contraseña temporal que se le haya suministrado. En caso contrario, le será denegado el acceso y deberá contactar con el Centro de Atención a Usuarios para comunicar la incidencia.
- Los Usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable del fichero.
- Cada ordenador dispondrá de un protector de pantalla con contraseña que se activará a los diez minutos de inactividad.

- La posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información estará limitada mediante un sistema que impedirá realizar más de tres intentos fallidos de forma consecutiva.
- Los identificadores de usuario con más de 60 días en desuso, se desactivarán y al mes siguiente se borrarán del sistema.
- Un identificador de usuario se considerará expirado cuando el éste deja la compañía y se desactivará el último día de trabajo. Cuando se trate de personal contratado, él identificador de usuario se considera expirado y se desactivará el último día de trabajo como se declaró en el contrato.
- Los identificadores temporales deberán configurarse para un corto periodo de tiempo y siempre bajo demanda, desactivándose y borrándose de los sistemas una vez expirado dicho periodo.

Responsabilidades Personales

La seguridad de los datos es una tarea de equipo en la que los Usuarios juegan un papel fundamental.

Los Usuarios externos de los Sistemas de Información de la Compañía serán responsables de asegurar que los Datos, Aplicaciones y Recursos Informáticos de la Compañía sean usados únicamente para el desarrollo de los procesos de negocio y ciclos productivos.

El Usuario está obligado a utilizar la red corporativa y la intranet de la Compañía y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la Compañía o de terceros, o que puedan atentar contra la moral o las *normas de etiqueta de las redes telemáticas*.

Para obtener acceso a los Sistemas ofrecidos por la Compañía es necesario disponer de un identificador de usuario sobre el que se deben observar los siguientes procedimientos de actuación:

- Los Usuarios son responsables de toda actividad relacionada con el uso de su identificador.
- Los Usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona.
- Los Usuarios no deben utilizar ningún identificador de otro Usuario, aunque dispongan de la autorización del propietario.
- Los Usuarios no pueden conectarse más de una vez en más de una estación de trabajo.
- Si un Usuario tiene sospechas de que su identificador está siendo utilizado por otra persona, debe proceder a su cambio y contactar con el Centro de Atención a Usuarios para notificar el incidente.
- Si un Usuario tiene sospechas de que su contraseña está comprometida, deberá solicitar su cambio notificándoselo al Centro de Atención a Usuarios.
- El Usuario debe utilizar una contraseña segura compuesta por un mínimo de cinco caracteres. Como mínimo, uno de los caracteres debe ser un número o un símbolo, excepto al empezar y acabar. No es recomendable utilizar nombres propios, fechas destacables, palabras con algún sentido o fáciles de descubrir.
- Los Usuarios son responsables de cambiar su contraseña como mínimo una vez cada 30 días y deberá ser diferente de las últimas 12 utilizadas por el mismo usuario. En caso contrario, se les podrá denegar el acceso y deberán contactar con Centro de Atención a Usuarios para la obtención de una nueva.

Uso Apropiado de los Recursos

Los Recursos Informáticos, Software, Datos, Red Corporativa y los Sistemas de Comunicación Electrónica, son propiedad de la Compañía o sobre ellos tiene derecho de uso y están disponibles exclusivamente para cumplimentar las obligaciones contractuales y propósitos de negocio. Cualquier programa, base de datos, hoja de calculo o cualquier otro desarrollo creado por un usuario, será propiedad de la Compañía.

No está permitido:

- El uso de los recursos de la Compañía para actividades no relacionadas con el negocio, o bien la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del software o de los estándares de los Recursos Informáticos de la Compañía, o en su defecto de Home Office.
- Introducir contenidos obscenos, amenazadores, inmorales u ofensivos en la Red Corporativa de la Compañía.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos de la Compañía o de terceros.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de la Compañía o de terceros. (Estos actos pueden constituir un delito de daños).
- Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de soportes, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a *propiedad intelectual e industrial* y a control de virus.

Software

Los Usuarios deben utilizar únicamente las versiones de software facilitadas por la Compañía y siguiendo sus normas de utilización.

No está permitido:

- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar cualquiera de los programas instalados legalmente.
- Copiar ninguna aplicación de la Compañía para su uso en otro Recurso Informático de la Compañía o fuera de la misma, sin obtener antes consentimiento por escrito.
- Copiar ninguna aplicación o software que no sea propiedad de la Compañía a un Recurso Informático de la Compañía sin obtener antes consentimiento por escrito.

Protección de datos personales

No está permitido:

- Crear ficheros de datos personales sin la autorización del responsable del fichero.
- Cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa.
- Realizar cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la Agencia de Protección de Datos.

Recursos de Red

No está permitido:

- Conectar a ninguno de los Recursos Informáticos de la Compañía ningún tipo de equipo de comunicaciones (p. ej. módem) que posibilite la conexión a la Red Corporativa.
- Conectarse a la Red de la Compañía a través de otros medios que no sean los definidos y administrados por los la Compañía.

- Conectar ningún dispositivo nuevo o Recurso Informático a la Red Corporativa sin obtener antes consentimiento por escrito.
- Intentar obtener otros derechos o accesos distinto a aquellos que les hayan sido asignados por la Compañía.
- Intentar acceder a áreas restringidas de los sistemas informáticos de la Compañía o de terceros.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Compañía.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos de la Compañía.

Correo Electrónico

Se considerará *correo electrónico* tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas, y en especial, Internet. Todos estos mensajes irán abiertos.

No está permitido intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o ficheros de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones).

- El servicio de correo electrónico debe ser usado únicamente para la comunicación de aspectos relacionados con el negocio y/o el cumplimiento de las obligaciones contractuales.
- La Compañía velará por el correcto uso del correo electrónico de los usuarios de la red corporativa y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Compañía como responsable civil.
- El sistema de correo electrónico de la Compañía no debe ser usado para enviar mensajes fraudulentos, obscenos, amenazadores, inmorales, ofensivos u otro tipo de comunicados similares.
- Los Usuarios no deben crear, enviar o reenviar mensajes de forma masiva o piramidales con fines comerciales o publicitarios (mensajes que se extienden a múltiples Usuarios).
- De manera excepcional, se podrá transmitir "datos de carácter personal" así como nombre, dirección, teléfono, etc., o los datos relativos a la salud, a entidades externas a la Compañía, a través del Sistema de Correo Electrónico, con el consentimiento expreso del afectado a quien se le indicará de forma detallada a quien se van a transmitir los datos y en todo caso cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Transmisión de datos a través de redes

- De manera excepcional, se podrá transmitir "datos de carácter personal" así como nombre, dirección, teléfono, etc., o los datos relativos a la salud, a entidades externas a la Compañía, a través de redes de telecomunicaciones, con el consentimiento expreso del afectado a quien se le indicará de forma detallada a quien se van a transmitir los datos y en todo caso cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Conectividad a Internet

La autorización de acceso a *Internet* se concede exclusivamente para actividades de trabajo. Todo el personal externo tienen las mismas competencias y responsabilidades en cuanto a *Internet* en sus campos normales de actividad, de acuerdo con los términos del contrato, y están obligados a cumplir siempre con las Guías Corporativas de la Compañía, Diseño Corporativo e Identidad Corporativa.

- El acceso a *Internet* se restringe exclusivamente a través de la red la Compañía, es decir, por medio del sistema cortafuego incorporado en la misma. No está permitido acceder a *Internet* vía módem (sea un módem individual o en pool).
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades, exclusivamente para cumplimentar las obligaciones contractuales
- Los Usuarios no deben hacer transferencia de datos de o a *Internet*.
- En caso de producirse la necesidad de una transmisión, esta deberá ser realizada por personal de la Compañía.

No está permitido:

- Utilizar el acceso a *Internet* para debates en tiempo real (Chat / IRC) siendo "*especialmente peligroso"*, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema.
- Visitar páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. que no sirvan como soporte al objetivo de negocio de la Compañía.
- La transferencia de ficheros no relativa a actividades de negocio - en particular la bajada de juegos de ordenador, ficheros de sonido y fotos, gráficos, etc.
- El uso del nombre, símbolo, logotipo o símbolo similar de la Compañía en ningún elemento de *Internet* (correo electrónico, páginas web, etc.) sin el previo consentimiento por escrito de la Dirección de la Compañía.
- Facilitar la accesibilidad desde *Internet* a ningún tipo de Información Corporativa sin obtener previamente consentimiento por escrito.
- Ocultar o manipular su identidad bajo ninguna circunstancia.

Ejemplos de actividades *no autorizadas*:

- Transmisión o recepción de material protegido por Copyright infringiendo la ley de Copyright y licencias.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración, mensaje o material clasificable como ofensivo o ilegal.
- Transferencia de ficheros a terceras partes. Por ejemplo, información:
  - sobre la Compañía; y/o
  - sobre entidades legales y personas, a quien la Compañía ha prometido confidencialidad.
- Transmisión o recepción de ficheros que infrinjan la ley de protección de datos o directrices de la Compañía.
- Transmisión o recepción de juegos o aplicaciones.
- Participación en actividades de Internet como grupos de noticias, debates en tiempo real, juegos u otras.

Todas las actividades que puedan dañar la buena reputación de la Compañía están prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas el personal externo para su propio beneficio económico o de terceras partes, y a actividades de naturaleza política.

¿ QUIÉN ES RESPONSABLE DE LA SEGURIDAD ?

La protección de los recursos y de la información es una necesidad básica para la buena marcha del negocio de la Compañía. Para ello, todos los niveles de Dirección tratarán de:

- Identificar y proteger los Recursos Informáticos del área bajo su responsabilidad.
- Asegurar que todos los Usuarios comprenden y están sensibilizados sobre su responsabilidad en la protección de los Recursos Informáticos.
- Llevar a término los procedimientos y prácticas de seguridad vigentes en la Compañía.
- Revisar el cumplimiento de los criterios establecidos e iniciar las acciones correctoras pertinentes en aquellos casos que se considere oportuno.

La siguiente matriz define los roles de seguridad y las responsabilidades dentro de la Compañía.

Rol_	Partes Responsables	Responsabilidad	Políticas y Estándares
Responsables de la Seguridad	• Personal Directivo • Comité de Seguridad • Comité de Control de Riesgos • Dirección de Sistemas • Dirección Capital Humano	• Asegurar la Seguridad de los Recursos Informáticos bajo su control • Aprobar actuaciones	• Revisar, Aprobar y Publicar las Políticas • Fomentar el cumplimiento de las Políticas
Gestión y Administración de la Tecnología	• Dirección de Sistemas	• Proporcionar y Asignar los Recursos Informáticos • Administrar los Sistemas de Información • Controlar el uso de los Sistemas de Información	• Asegurar el cumplimiento de las Políticas
Usuarios y Otros	• Personal de la Compañía • Mediadores • Peritos • Personal Subcontratado • Proveedores	• Cumplir las directrices respecto al uso de los Sistemas de Información	• Conocer y aplicar las Políticas

MONITORIZACIÓN

Todas las aplicaciones y datos ubicados en los Recursos Informáticos, Sistemas de Comunicación Electrónica de la Red Corporativa de la Compañía son de su propiedad o de posibles proveedores. Las aplicaciones de los proveedores serán tratadas de acuerdo a los contratos establecidos con los mismos.

Con el fin de velar por el correcto uso de las mencionadas aplicaciones y recursos, la Dirección de la Compañía y la Dirección de Sistemas, comprobará, de forma periódica, o cuando por razones del servicio resulte conveniente, utilizando los medios técnicos apropiados, la correcta utilización de los mismos por los técnicos y por los usuarios.

En caso de apercibir que un técnico o un usuario utiliza incorrectamente las aplicaciones y/o datos, le comunicará tal circunstancia; facilitará, en su caso, la formación necesaria para el correcto uso de las aplicaciones con el fin de evitar la causación de daños.

En caso de apreciarse mala fe en la incorrecta utilización de los datos y recursos, la Compañía ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

INCIDENCIAS

Es obligación de todo el personal externo, comunicar al responsable del sistema cualquier *incidencia* que se produzca en los Sistemas de Información a que tengan acceso.

- Se entiende por *incidencia* cualquier anomalía que afecte o pueda afectar a la seguridad de los datos.
- Dicha comunicación deberá realizarse inmediatamente y, en cualquier caso, en un plazo de tiempo no superior a una hora (1) desde el momento en que se conozca dicha *incidencia*, al Departamento de Proveedores quienes pasarán la correspondiente nota al centro.

ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, la Compañía se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a los representantes de las Empresas Proveedoras utilizando los medios que se consideren pertinentes. Es responsabilidad de cada Usuario la lectura y conocimiento de la Política de Seguridad de los Sistemas de Información más reciente de la Compañía.

Aide Asistencia, Seguros y Reaseguros, S.A.

Notificación de Aceptación de la Política de Seguridad para Personal Externo y Proveedores

De: _____
<Nombre de la empresa>

A: Dirección Sistemas de la Compañía

D. …… DNI …….. Domicilio ……. actuando en su propio nombre, declaro que conozco el contenido del documento POLITICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION de la Compañía y me comprometo a que en el uso de la Red Corporativa y los Recursos Informáticos de la Compañía, observaré lo establecido en dicho documento.

_____ _____
Nombre Firma

_____
Fecha

ANEXOS

POLITICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION

DEFINICIONES

- ActiveX – Los denominados controles ActiveX son componentes adicionales que se pueden incorporar a las páginas web, para dotar a éstas de mayor funcionalidad (animaciones, vídeo, navegación tridimensional, etc.,). Están escritos en un lenguaje de programación y podrían estar infectados por los virus.
- Antivirus – Son programas que permiten analizar la memoria y unidades de disco del ordenador en busca de virus. Una vez se ha detectado alguno de ellos, informa al usuario procediendo inmediatamente y de forma automática a desinfectar los ficheros, directorios, o discos que hayan sido víctimas del virus.
- Applets – Son pequeñas aplicaciones (conjunto de programas) que se difunden a través de la red para ejecutarse en el navegador del usuario. Están escritos en un lenguaje de programación y podrían estar infectados por los virus.
- Chat / IRC – Comunicación simultanea escrita en tiempo real entre dos o más personas a través de Internet.
- Correo Electrónico – Aplicación mediante la cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) a través de la red.
- Datos de Carácter Personal – Cualquier información concerniente a personas físicas identificadas o identificables.
- Datos con nivel de protección alto o Datos Especialmente Protegidos – Ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud o vida sexual.
- Directivos de la Compañía – Profesionales de la Compañía desempeñando cargos de Dirección.
- Fichero – Unidad lógica significativa de información que puede ser manipulada por el sistema operativo de un ordenador designada por un nombre y considerada como una unidad para el usuario (pe.: textos, imágenes, bases de datos, hojas de cálculo, etc.,)
- Información Corporativa – Conjunto de datos de negocio y personales que son tratados por los procesos de negocio de la Compañía y sus Sistemas de Información.
- LOG – Fichero de Registros de sucesos de los sistemas.
- Macro / Virus de Macro – Secuencia de operaciones o instrucciones que definimos para que un programa (pe.: Word, Excel, Access, etc.,) realice de forma automática y secuencial. Son "microprogramas" y podrían estar infectados por los virus.
- Monitorizar/Monitorización – Hacer seguimiento, supervisar, vigilar y controlar toda actividad asociada con el uso de los Sistemas de Comunicación Electrónica de la Red Corporativa y los Recursos Informáticos.
- Navegador (Browser) – Aplicación para facilitar la navegación por los servidores de información de Internet.
- Normas de etiqueta de las redes telemáticas ("Netiquette" o "Etiqueta de la red") – Conjunto de normas, reglas de etiqueta y cortesía dictadas por la costumbre y la experiencia que definen las reglas de urbanidad y buena conducta que deberían seguir los usuarios de Internet en sus relaciones con otros usuarios.
- Protección de Datos – El artículo 18.4 de la Constitución Española establece que *"la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.
- Proveedores – Cualquier persona o entidad que proporcione software, hardware, soporte técnico u otros servicios para mantener o extender los objetivos de negocio de la Compañía.
- Real Decreto 1720/2007 de 21 de diciembre – Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
    - Art. 89.1: Las funciones y obligaciones de cada uno de los usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

  - Art. 89.2: El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- Recursos Informáticos – Cualquier dispositivo físico o lógico poseído o contratado por la Compañía que tiene la capacidad de almacenar, procesar o transmitir datos. Los Recursos Informáticos incluyen entre otros PCs, equipos portátiles, servidores, impresoras, faxes, fotocopiadoras, dispositivos de red, disquetes, CDs y dispositivos de copias de seguridad.
- Red Corporativa de la Compañía – Todas las conexiones físicas y lógicas establecidas en las instalaciones informáticas de la Compañía, y entre éstas y cualquier empresa externa.
- Responsable del Fichero – la Compañía.
- Sistemas de Comunicación Electrónica – Cualquier comunicación electrónica usada desde la Red Corporativa de la Compañía, entre ésta y otras redes, en especial Internet.
- Sistemas de cortafuego – Un sistema que protege la red de la Compañía, denegando el acceso de terceros no autorizados y controlando los accesos a Internet del personal autorizado.
- Sistemas de Información: – Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos.
- Sistema Externo – Cualquier dispositivo informático o de red que no pertenece o está subcontratado por la Compañía.
- Usuarios – Empleados de la Compañía, personal de soporte, proveedores y otros usuarios de la Red Corporativa o de los Recursos Informáticos.
- Virus – Agente nocivo que actúa en un sistema informático y perjudica el funcionamiento correcto. Son programas que se introducen en nuestros ordenadores de formas muy diversas y se coloca en lugares donde el usuario pueda ejecutarlos de manera no intencionada.