USO DE LOS SISTEMAS DE INFORMACIÓN DE AQUALOGY BUSINESS SOFTWARE, S.A.

OBJETO

Esta norma específica las directrices de seguridad necesarias para evitar el uso de los recursos y dispositivos de tratamiento de información para fines no autorizados o ajenos a la actividad de Aqualogy Business Software, S.A. (en adelante "la Sociedad").

DESARROLLO

Los sistemas de información, entendidos como el conjunto de elementos de software (programas, aplicativos y ficheros) y recursos y dispositivos tecnológicos (hardware), constituyen un factor de creciente importancia en la operativa empresarial. Es un compromiso de la Sociedad la puesta a disposición de sus profesionales de los más robustos sistemas tecnológicos que contribuyan a una mayor operatividad y eficiencia.

Para preservar la integridad de estos sistemas y dispositivos, evitar pérdidas de datos y/o un uso ilícito o no autorizado es esencial establecer un marco de actuación en el uso y acceso a los mismos.

Adicionalmente, los equipos portátiles y dispositivos móviles deberán contar con un conjunto de medidas de seguridad específicas. Por parte de los usuarios, para efectuar un uso diligente de estos sistemas y dispositivos, se observarán las siguientes directrices comunes en relación a los equipos informáticos y teléfonos, así como en el uso del correo electrónico y del acceso a internet:

Uso de los sistemas de información

Usos permitidos

- Uso para los fines que se desprenden del cargo ocupado y funciones, y acorde con los principios éticos y de conducta recogidos en el Código Ético.
- Instalar, utilizar y actualizar el software autorizado por el departamento de sistemas de la Sociedad.
- Almacenar informaciones, archivos y datos propios de la actividad empresarial de la Sociedad.

Usos no permitidos

- Descargar y/o instalar cualquier tipo de programa que no haya sido específicamente autorizado o proporcionado por el departamento de Sistemas.
- Conectar a los equipos informáticos facilitados por la Sociedad dispositivos de almacenamiento de datos no homologados o no proporcionados por el departamento de Sistemas.

- Utilizar un nombre de usuario y contraseña ajenos para acceder a los sistemas de información.
- Compartir con otros usuarios o terceros la contraseña personal de acceso a los equipos informáticos.
- Acceder o tratar de acceder a documentos e información para cuyo acceso no se dispone de los privilegios o permisos suficientes.
- Apoderarse, compartir o difundir, por cualquier medio, datos, documentos o información restringida o confidencial de la Sociedad para los cuales no se dispone de los correspondientes permisos o autorización.
- Almacenar información o documentación empresarial de la Sociedad exclusivamente en carpetas personales o locales.
- Descargar, almacenar o compartir material de carácter pornográfico, racista, xenófobo, sexista o ilegal, en cualquier formato.
- Descargar, almacenar, utilizar o compartir programas informáticos destinados a facilitar la supresión no autorizada o la neutralización de cualquier sistema técnico utilizado para la protección de los equipos tecnológicos puestos a disposición por la Sociedad.
- Descargar, almacenar, utilizar o compartir programas destinados a averiguar o descifrar contraseñas, salvo en los supuestos expresamente autorizados a los efectos de realización de auditorías de seguridad del sistema.
- Descargar, almacenar, instalar o compartir software en los sistemas de información de la Sociedad que no hayan sido adquiridos por la empresa o para los que no disponga de la correspondiente licencia.
- Acceder, borrar, eliminar o hacer inaccesibles por cualquier medio los documentos y archivos almacenados en los sistemas de información de la Sociedad al margen de aquellas acciones autorizadas.
- Acceder, por cualquier medio, presencial o remotamente, al equipo informático de otro empleado o de un tercero sin su consentimiento.
- Acceder, alterar o dañar por cualquier medio un archivo o documento ajeno, sin autorización.
- Acceder o tratar de acceder a redes internas corporativas desde un dispositivo informático no gestionado por la Sociedad.
- Descargar o compartir programas, documentos o archivos protegidos por derechos de propiedad intelectual o industrial sin el previo consentimiento de su titular.
- Cualquier otro uso contrario a los principios éticos y de conducta recogidos en el Código Ético y en la Política de Seguridad de la Información y Uso de las TIC

Sobre los usos indicados anteriormente para cualquiera de los sistemas de información de la Sociedad en general, se contemplan además los siguientes usos para las tecnologías específicas.

Uso de Internet

Usos permitidos

- Navegar por Internet para los fines empresariales o laborales propios del cargo ocupado y funciones desempeñadas.

Usos no permitidos

- Enviar documentación o información propiedad de la Sociedad a través de páginas de correo electrónico no corporativo o subir dicha información a páginas web de almacenamiento de datos ajenas a la Sociedad.
- Compartir la contraseña de acceso a los servicios de Internet proporcionados por la Sociedad con otros usuarios o terceros.
- Acceder a Internet con nombre de usuario y contraseña ajenos.
- Acceder a páginas de Internet cuyo contenido tenga carácter pornográfico, racista, xenófobo, sexista o ilegal.
- Acosar a cualquier otro empleado o tercero a través de páginas web, foros de discusión, chats online o redes sociales corporativas o públicas.
- Uso de enlaces *Wi-Fi* con acceso sin contraseña y puertos *Ethernet* de lugares públicos para realizar operativa en la que se gestione información corporativa.

Uso del correo electrónico corporativo

Usos permitidos

- Enviar, recibir y/o almacenar correos electrónicos relacionados con el cargo ocupado y funciones desempeñadas.

Usos no permitidos

- Utilizar el correo electrónico corporativo para fines diferentes de los que se desprendan del cargo ocupado y funciones.
- Enviar o reenviar correos electrónicos de distribución masiva no relacionados con el desempeño del cargo y funciones.
- Enviar documentación de la Sociedad a direcciones de correo electrónico personal, o a direcciones de correo electrónico no corporativas, siempre que dicho envío no esté relacionado con el normal desempeño del cargo y funciones.
- Utilizar cuentas de correo electrónico personal para el desempeño de su actividad laboral en la Sociedad.
- Enviar correos electrónicos que contengan datos de carácter pornográfico, racista, xenófobo, sexista o ilegal.

- Enviar o distribuir correos electrónicos que contengan documentos o informaciones para cuyo acceso no se disponga de los privilegios suficientes.
- Acosar a cualquier empleado o tercero mediante el envío de reiterados correos electrónicos de contenido inapropiado.
- Configurar teléfonos móviles u otros dispositivos no proporcionados por la Sociedad para recibir y gestionar los correos electrónicos corporativos, salvo autorización expresa y por escrito de la Sociedad.
- Leer, borrar, copiar o modificar mensajes de correo electrónico de otros usuarios o de terceros sin su previa autorización.
- Enviar correos electrónicos usando el nombre o la dirección de otros usuarios o terceros con el fin de engañar al destinatario sobre su remitente.

Uso de teléfonos, fijos o móviles

Usos permitidos

- Emplear el teléfono fijo y/o móvil corporativo acorde con los principios éticos y de conducta recogidos en el Código Ético.

Usos no permitidos

- Utilizar los terminales de telefonía fijos o móviles para comunicaciones personales de forma reiterada e inapropiada.
- Llevar a cabo conversaciones propias del desempeño del cargo y funciones en lugares públicos, siempre que éstas versen sobre información restringida o confidencial de la Sociedad.
- Realizar llamadas a servicios de tarificación adicional.
- Desconectar los ajustes de seguridad del terminal de telefonía corporativo configurados por el departamento de sistemas.
- Desbloquear o manipular el software interno del terminal de telefonía corporativo.
- Acosar a cualquier otro empleado o tercero a través de reiteradas llamadas de contenido inapropiado, o de cualquier aplicación descargada o instalada en el terminal de telefonía corporativo.

En relación a los dispositivos externos de tratamiento o almacenamiento de la información, será responsabilidad de los departamentos de informática, en colaboración con los de Seguridad TI, la definición y homologación de estos dispositivos.

Los usuarios deberán realizar un uso diligente y responsable de los dispositivos, y de acuerdo con lo establecido en la norma de aplicación.