CODIGO DE CONDUCTA TELEMATICO PARA LOS USUARIOS DE EQUIPOS INFORMATICOS DE RIESCO ABOGADOS

1. Introducción.

1.1. *Riesco Abogados* [de aquí en adelante RA] provee a sus colaboradores de medios técnicos e informáticos que garantizan la rapidez y eficacia en la prestación de sus servicios. Entre estos medios se incluyen los equipos informáticos, programas y sistemas que facilitan el uso de las herramientas informáticas, el acceso a una red interna o intranet y a una red externa o internet, así como la utilización de un buzón de correo electrónico o e-mail.

1.2. El presente código de conducta tiene por objeto garantizar el buen uso de los medios técnicos e informáticos propiedad de RA y posibilitar una mejora en la red de comunicaciones, evitando determinadas prácticas que impliquen la utilización incorrecta o inadecuada de los medios mencionados.

1.3. Con independencia de este Código RA está elaborando el Documento de Seguridad regulado en el Real Decreto 994/1.999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, siendo recomendable la refundición de ambas normas en una sola.

2. Objetivos.

2.1. El presente código de conducta pretende concienciar a los colaboradores sobre la seguridad en los equipos informáticos y de comunicaciones, tanto dentro

como fuera de las instalaciones de RA. En consecuencia, las presentes normas serán de aplicación a los distintos equipos informáticos de RA con independencia de su ubicación.

3. <u>Ámbito de aplicación.</u>

3.1. La expresión "colaboradores" comprende a todos las personas que prestan servicios en el despacho, tanto profesionales como administrativos. En el presente Código serán denominados indistintamente usuarios o colaboradores.

3.2. Las normas incluidas en el presente código serán de aplicación para todas las comunicaciones realizadas a través de la intranet y de internet.

4. <u>Utilización de los equipos informáticos:</u>

4.1. Todos los equipos informáticos de los que dispone el colaborador son propiedad de RA. Estos medios no son idóneos para un uso personal o extraprofesional. No obstante, se permite una utilización ocasional para actividades personales no reservadas de los equipos informáticos puestos a disposición de los colaboradores, si bien esta utilización debe restringirse al máximo.

4.2. No es posible alterar ni en todo ni en parte los equipos informáticos ni conectar otros (asistentes personales, impresoras, reconocedores de voz, etc.) a iniciativa del colaborador, sin contar con la autorización expresa de los socios.

4.3. Las normas establecidas en el presente capítulo son de aplicación, salvo que se disponga lo contrario, tanto a los equipos informáticos fijos (*desk tops*) como a los equipos informáticos portátiles (*laptops*) a los que el colaborador pudiera

eventualmente tener acceso, así como cualquier otro instrumento de transmisión telemática que se pueda poner a disposición de los usuarios.

5. <u>Utilización de los programas y de los archivos informáticos:</u>

<u>Principios generales:</u>

5.1. Los archivos y documentos contenidos en el disco duro y en otro tipo de herramientas informáticas (disquetes, CD-Roms, lápices de memoria, etc.) deben ser utilizados con una finalidad profesional, sin que sean idóneos, por consiguiente, para un uso personal o privado. Los documentos personales que ocasionalmente se realicen podrán guardarse en el archivo personal del disco duro del ordenador a cada colaborador.

5.2. En cualquier caso, la información de carácter confidencial (p.e.: relativa a clientes o potenciales clientes del despacho) incluida en los archivos y documentos dentro de RA, no podrá enviarse a terceras personas o compañías distintas de las receptoras de la información, salvo que se reciba autorización de un socio.

5.3. Especial consideración debe darse a todos aquellos archivos que contengan datos personales (clientes, proveedores, profesionales, colaboradores, etc.) que puedan ser susceptibles de inclusión en el ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Los usuarios que tengan acceso a dichos archivos o documentos deberán extremar las precauciones para evitar cualquier salida de información de los mismos que pueda hacer a la organización y/o usuario incurrir en algún tipo de responsabilidad. Asimismo, deberán tenerse en cuenta todas las

medidas de seguridad adoptadas en relación con los archivos que contengan datos personales,.

5.4. Esta prohibido instalar o visualizar salvapantallas, fotos, videos, animaciones, y/o cualquier otro medio de reproducción o visualización de contendido ofensivo o atentatorio contra la dignidad de la persona, y en especial, de contenido sexual. Se ruega en particular no instalar salvapantallas con fotografías que puedan resultar ofensivas o herir la sensibilidad del resto de colaboradores o del personal. Asimismo, se prohíbe el envío de mensajes de correo electrónico de carácter obsceno, ofensivo, difamatorio o que pueda ser susceptible de ser considerado acoso o intimidación.

Instalación de programas:

5.5. Los programas informáticos instalados en los equipos informáticos son propiedad de RA. La utilización, copia o reproducción de los mismos para fines extraprofesionales, queda excluida salvo autorización expresa.

5.6. La instalación de programas informáticos debe realizarse bajo la supervisión de los socios, siempre que RA cuente con las oportunas licencias para utilizar todo el software con el que se trabaja en la misma.

5.7. Como consecuencia de lo anterior, con el fin de evitar que los derechos de terceros se vean vulnerados o que el sistema informático pueda verse seriamente perjudicado, no cabe, salvo autorización expresa por parte de los socios, instalar ningún tipo de programa no autorizado.

5.8. Asimismo, no será posible utilizar programas para los cuales la organización no haya obtenido una licencia previa. Debe admitirse que la utilización de

programas informáticos sin la debida autorización puede ser constitutivo de responsabilidades de distinto orden, y que el colaborador puede incurrir asimismo en responsabilidad. Se ruega tener, por tanto, la máximo diligencia en este aspecto.

5.9. Las cláusulas anteriores serán de aplicación también, y especialmente, a programas enviados a través del correo electrónico o susceptibles de instalación a través de Internet. En particular, la presente cláusula se aplica a la instalación de software relativo a juegos o a la instalación de programas de música para los que no se hayan obtenido los correspondientes permisos legales.

Seguridad en los programas y archivos informáticos:

5.10. Ante el riesgo de que archivos o programas provenientes de fuentes no conocidas causen un virus que en el sistema informático RA, el programa antivirus instalado se ejecutará automáticamente para comprobar la ausencia de virus en los programas y archivos instalados en la red. No obstante, dado que estos programas antivirus no eliminan por completo el riesgo de generar y propagar un virus informático, debe actuarse con la máxima diligencia a la hora de ejecutar archivos procedentes de fuentes no conocidas.

5.11. Queda expresamente prohibida la entrada por cualquier medio en los sistemas informáticos de otros colaboradores utilizando un login y password de otro usuario, salvo autorización expresa de los socios. No obstante, para facilitar la utilización de las herramientas informáticas en determinados supuestos esta utilización resultará posible cuando se utilice el login y el password propio de cada usuario.

Finalización de la colaboración:

5.12. RA pone a disposición de los colaboradores los medios informáticos y técnicos adecuados para la realización de sus funciones mientras dure la colaboración. En el momento de la finalización de la colaboración con RA no se podrá tener acceso a los equipos informáticos ni consiguientemente a los archivos incluidos en los mismos. En el supuesto de que el ex colaborador tenga en su poder determinados medios informáticos (ordenador portátil, CD Roms, disquetes informáticos, etc.) tendrá que devolverlos inmediatamente a la finalización de su colaboración. El colaborador que finalice su relación con RA deberá dejar intactos todos los archivos y documentos que hayan tenido un fin profesional o productivo. En el supuesto de que existan archivos de carácter personal, él mismo deberá eliminarlos.

Facultad de revisión:

5.13. Cuando estime necesario para la protección del patrimonio empresarial y de los derechos de los demás colaboradores, o por motivos relacionados con el funcionamiento de la organización, RA podrá revisar periódicamente el contenido de los discos duros de los ordenadores utilizados por los distintos usuarios en el desempeño de sus funciones.

5.14. Las mencionadas revisiones se efectuarán siempre respetándose las garantías legales.

6. Acceso a la red interna de la organización:

RA está organizada globalmente en torno a la red interna (local área network o LAN). El acceso a la misma a través de los medios técnicos permite al colaborador de RA

acceder a información confidencial de los clientes del despacho, por lo que para evitar que determinadas personas ajenas al entorno del despacho puedan tener acceso a la información contenida en la red interna de la organización , se deben tener en cuenta una serie de requisitos mínimos de seguridad.

Uso de clave de identificación y de contraseña:

6.1. Cada colaborador de RA recibirá una clave de identificación y elegirá una contraseña de acceso a la red interna de la organización, de conformidad con lo previsto en las cláusulas 6.5 y siguientes del presente código de conducta. La mencionada contraseña no deberá ser comunicada a terceras personas, salvo que concurran circunstancias excepcionales, y siempre que se reciba autorización expresa de los socios.

Contraseña para equipos fijos:

6.2. Las medidas de seguridad aplicables a los equipos (desk tops) son las siguientes:

6.2.1. Cada usuario dispondrá de una única clave de identificación personal, que le será remitida inmediatamente después de su incorporación.

6.2.2. Cada usuario elegirá una contraseña o password para tener acceso a la red interna de la organización. La contraseña se elegirá y cambiará de conformidad con las reglas establecidas en el apartado 6.5 y siguientes.

6.2.3. El sistema requerirá al usuario que introduzca su clave de identificación personal y su contraseña o password cada vez que proceda al encendido o desbloqueo de su ordenador.

6.2.4. Para garantizar la seguridad de los archivos y documentos integrados en la red interna, queda prohibido que el usuario modifique la configuración del ordenador para evitar tener que introducir su clave de identificación personal y su contraseña cada vez que se proceda al encendido del ordenador.

6.2.5. La contraseña de acceso a la red interna de la organización caducará cada 90 días. En ese momento, el propio sistema recordará al colaborador la elección de una nueva contraseña que estará vigente a partir de ese momento, y que tendrá un plazo de duración de 90 días. La contraseña que ha expirado no podrá ser utilizada nuevamente. El usuario puede proceder al cambio de contraseña tantas veces como crea oportuno, no siendo necesario esperar al plazo de 90 días para proceder a su cambio, si desea realizarlo con una mayor celeridad.

6.2.6. Para evitar que terceras personas puedan acceder a su terminal, se recomienda proceder al cierre del sistema en caso de ausencia interrumpida por un período superior a dos horas. Asimismo, se recomienda proceder al bloqueo de la estación en aquellos supuesto de ausencia por tiempo inferior a las dos horas.

<u>Contraseña para equipos portátiles:</u>

6.3. En el caso de que RA ponga a su disposición un ordenador portátil, se configurará de forma que tenga que introducir su clave de identificación personal y su contraseña cada vez que proceda al encendido de la terminal de ordenador portátil (conectado o desconectado de la red).

6.4. Asimismo es preciso recordar nuevamente que el colaborador que tenga a su disposición equipos informáticos portátiles debe extremar su precaución cuando haga uso de los mismos o cuando los transporte fuera de las instalaciones de RA. El contenido del ordenador portátil puede ser altamente confidencial por lo que las más altas precauciones deben tomarse para evitar la pérdida o sustracción del mismo. El colaborador deberá dar cuenta inmediatamente a RA del extravió o pérdida que pueda haberse producido.

Elección y cambio de contraseña:

6.5. La contraseña o password será escogida de forma individual y personal.

6.6. No podrá elegirse una contraseña que haya sido utilizada con anterioridad por el colaborador o usuario de una clave de identificación personal.

6.7. En el caso de que olvide su contraseña o password, contactar inmediatamente con los socios.

6.8. La contraseña finalmente elegida no podrá ser comunicada a terceros, salvo determinadas excepciones, y siempre bajo autorización del supervisor o profesional responsable.

6.9. El usuario procederá a cambiar la contraseña o password con carácter periódico según se establece en el apartado 6.2.5.

Acceso a la red interna desde ordenadores situados fuera de las instalaciones:

6.10. Las mismas precauciones establecidas en el presente capítulo deberán tenerse en cuenta en el supuesto de que el usuario tenga acceso a la red interna de la

Organización desde ordenadores situados fuera de las instalaciones de RA. En tal caso, la clave de identificación personal y la contraseña o password deberán introducirse en el momento de acceder a la red interna.

7. <u>Navegación en la red de Internet:</u>

<u>Principios generales:</u>

7.1. Por lo que respecta a la navegación en la red de Internet, es política de RA que las conexiones que se produzcan a través de la mencionada red, obedezcan a fines profesionales, todo ello con el propósito de obtener el mayor aprovechamiento de los recursos informáticos. Si bien la organización permite a sus colaboradores realizar un uso del acceso a internet para actividades personales ocasionales, en este uso personal ocasional debe restringirse al máximo.

7.2. En ningún caso debe accederse a ciertas direcciones de internet, entre las que se encuentran las de contenido ofensivo o atentatorio contra la dignidad humana, y en especial, de naturaleza sexual.

7.3. Es propósito de RA dar cumplimiento al contenido de las leyes de la propiedad intelectual o industrial, por lo que los colaboradores deberán comprobar cuidadosamente, antes de utilizar información proveniente de la red, si la misma se encuentra protegida por las leyes de la propiedad intelectual o por las leyes de marcas.

7.4. Para que la utilización de la red de internet con fines profesionales o productivos sea lo más provechosa posible, se recomienda hacer uso de los

bookmarks (o favoritos), en el que se incluirán aquellas direcciones que por motivo de su presentación de servicios, deban ser consultadas periódicamente.

Facultad de revisión:

7.5. La tecnología de internet permite el almacenamiento de información en el servidor de la organización, quien podrá acceder por motivos justificados a esta información de conformidad con tal sistema de almacenamiento.

7.6. Sobre estas bases, cuando se estime necesario para la protección del patrimonio empresarial y de los derechos de los demás usuarios , o por motivos relacionados con el funcionamiento de RA, se podrá revisar periódicamente, a través de los servicios técnicos , los datos de las conexiones a red de Internet desde los ordenadores utilizados por los colaboradores en el desempeño de sus funciones.

7.7. Las mencionadas revisiones se efectuarán siempre respetándose al máximo las garantías legales.

8. Uso del correo electrónico o e-mail:

Principios generales:

8.1. RA suministra a cada colaborador una dirección individual de correo electrónico. Es política de RA hacer un buen uso del correo electrónico o e-mail. Recordamos que el mismo es un instrumento básico de colaboración, propiedad de la organización, y que debe ser utilizado con fines profesionales.

8.2. Debemos recordar asimismo que es política de la organización no utilizar el correo electrónico para "actividades personales restringidas", en las que pueda haber alguna expectativa de privacidad o secreto en las comunicaciones.

8.3. Si bien la organización permite utilizar el correo electrónico puesto a disposición de cada colaborador para "actividades personales no reservadas" en las que no exista expectativa alguna de privacidad , tales como usos sociales individualizados, esta utilización debe restringirse al máximo. Ahora bien, y sin perjuicio de lo anterior, no debe utilizarse el correo electrónico para ocasiones sociales colectivizadas (por ejemplo, felicitaciones colectivas de Navidad), que puedan poner en peligro el sistema informático.

8.4. El colaborador procederá a almacenar los mensajes profesionales de conformidad con las normas que se aprueben al respecto.

8.5. El trato confidencial que requiere la relación entre RA y sus clientes o potenciales clientes implica necesariamente la utilización de los medios de comunicación más apropiados en relación con la naturaleza de la comunicación a realizar. Por ello, en determinadas circunstancias, el colaborador deberá acompañar y/o sustituir la utilización de estos medios telemáticos por otros medios tradicionales, todo ello en función de la naturaleza de la comunicación a realizar.

<u>Seguridad en el uso del correo electrónico o e-mail:</u>

8.6. Las presentes normas de seguridad en el correo electrónico o e-mail tienen por objeto evitar, en la medida de lo posible, la posibilidad de cambio de identidades a través del sistema de correo de la organización.

8.7. Se prohíbe expresamente la interceptación y/o uso no autorizado del correo electrónico o e-mail de otros usuarios.

8.8. RA realizará cuantos controles, intervenciones o medidas cautelares puedan ser exigidas para evitar que los colaboradores o usuarios puedan cometer delitos informáticos mediante la utilización del correo electrónico o e-mail. En ningún caso asumirá RA responsabilidad por los hechos dolosos o culposos imputables a los colaboradores, contra los que, en su caso, se reserva las acciones que correspondan para conseguir la indemnidad de tales hechos.

8.9. Las reglas de seguridad establecidas en el apartado 6 del presente código de conducta en relación con el acceso a la red interna serán de aplicación al uso del correo electrónico o e-mail por parte de los colaboradores.

8.10. Se debe de tener especial cuidado con los mensajes de correo de cuya procedencia no se esté totalmente seguro o que no haya sido solicitado.

8.11. No se deberán de abrir ficheros anexados en los mensajes de correo y evitar la descarga de ficheros e instalación dejecutables (exe) procedentes de internet.

Finalización de la colaboración:

8.12. El colaborador tiene acceso al correo electrónico de RA durante el periodo que dura su colaboración con la misma. En el momento de la extinción de la colaboración, se interrumpirá el acceso a su buzón de correo. Los servicios técnicos podrán acceder al buzón para reenviar los mensajes profesionales a los colaboradores que se determinen.

Facultad de revisión:

8.13. Cuando se estime necesario para la protección del patrimonio empresarial y de los derechos de los demás usuarios, o por motivos relacionados con el funcionamiento de RA, se podrá revisar periódicamente, a través de los servicios técnicos, el contenido de la bandeja de salida del correo electrónico que ha sido asignado a cada colaborador para el desempeño de sus funciones.

8.14. Las mencionadas revisiones se efectuarán siempre respetándose al máximo las garantías legales.

9. Pautas generales de conducta sobre el uso de los sistemas de comunicación:

Las pautas hasta aquí descritas intentan precisar de forma clara y transparente el uso que debe hacerse de los medios de comunicación y equipos informáticos en el seno del Despacho. Los socios quedan a la entera disposición de los colaboradores para cualquier aclaración o duda que pueda surgir respecto del cumplimiento de las mismas, admitiendo de antemano todas las sugerencias que los colaboradores puedan realizar al respecto con el fin de mejorar el funcionamiento de dichas pautas.

10. Preguntas:

Para la resolución de cualquier duda o consulta de carácter técnico que se le pueda plantear con relación al contenido del presente código de conducta, se debe consultar a los socios.

11. Necesidad de cumplimiento de las normas de conducta:

Finalmente, la organización considera conveniente recordar a los colaboradores la necesidad de que las mencionadas pautas sean seguidas fielmente por parte de los mismos, con el fin de salvaguardar el derecho a su intimidad y de mejorar la calidad de la red de comunicaciones.

12. Entrada en vigor, vigencia y aprobación:

El contenido del presente código de conducta es de obligatorio cumplimiento para todos los colaboradores de RA. Su contenido entrará en vigor a partir de la recepción de la presente, y se mantendrá en vigencia hasta tanto no se a modificado o reemplazado por otro.

DECALOGO DEL CODIGO DE CONDUCTA

1. Salvaguardar la eficiencia en los recursos compartidos
2. Los sistemas informáticos no son idóneos para un uso personal
3. No utilice los equipos y sistemas para actividades personales restringida
4. Pueden utilizarse ocasionalmente para actividades personales no reservadas
5. Los socios deben supervisar la instalación de cualquier programa o aplicación
6. Mantener estricta confidencialidad sobre la clave de usuario y contraseña
7. Los servicios técnicos podrán acceder al buzón al extinguirse la colaboración
8. Evitar cualquier tipo de actuación que pueda considerarse como acoso
9. RA podrá revisar los equipos, programas y sistemas
10. Se debe consultar a los socios para la resolución de cualquier duda