Iberplus Seguridad SL

CODIGO DE CONDUCTA TELEMATICA

Madrid a 1 de Octubre de 2019

1. Introducción

1.1 Este documento es válido para los empleados y colaboradores de la empresa Iberplus Seguridad S.L. (en adelante **"IBERPLUS", "la Organización"** o **"la Empresa").**

1.2 IBERPLUS, proporciona a sus empleados unos determinados medios técnicos e informáticos, instrumentos de trabajo propiedad de la empresa, que garantizan la rapidez y eficacia en la prestación de sus servicios. Entre estos medios se incluyen los equipos informáticos o telefónicos, los programas y sistemas informáticos que facilitan el uso de las herramientas informáticas, el acceso a cualquier tipo de red informática (Internet, Extranet o Intranet), así como la utilización de un buzón de correo electrónico o de cualquier otro medio de comunicación o gestión de datos que la empresa ponga en cada momento a disposición de sus empleados para la realización de su actividad.

2. Objetivos

2.1 El presente código de conducta telemática tiene por objeto garantizar el uso de los medios técnicos e informáticos propiedad de la Organización.

2.2 Este código pretende concienciar a los empleados sobre la seguridad en los equipos informáticos y de comunicación, tanto dentro como fuera de las instalaciones de la empresa. Así, las normas y reglas del código deben adoptarse en el supuesto que el empleado tenga acceso a la red interna desde ordenadores u otras herramientas situadas fuera de las instalaciones sociales.

3. Motivos

3.1 Se pretende concienciar a los empleados de la necesidad de utilizar correctamente las herramientas informáticas para garantizar los compromisos de calidad y confidencialidad con los clientes y con el resto de los empleados

3.2 Considerando el carácter sensible y estrictamente confidencial de las operaciones que se realizan en el seno de la empresa, ésta tiene interés en auditar y controlar la utilización de los empleados de las herramientas informáticas y de comunicación que se ponen a su disposición para la realización de su trabajo.

4. Ámbito de aplicación

4.1 Las reglas estipuladas resultan de aplicación a todos los centros de trabajo, y a la totalidad del personal de alta en los mismos.

4.2 El Código de Conducta Telemático resulta igualmente de aplicación para todas las comunicaciones realizadas a través de la empresa.

5. Pautas generales de conducta sobre el uso de los equipos informáticos y medios de telecomunicación

5.1 Las pautas que se describen a continuación, intentan precisar de una forma clara y transparente, el uso que debe hacerse de los medios de comunicación y de los equipos informáticos en el seno de la empresa

5.2 Toda utilización de los medios de comunicación a los que se refiere el presente Código de Conducta Telemático no puede repercutir en el normal desarrollo de la actividad laboral, especialmente en lo que se refiere a la utilización del correo electrónico y a la navegación por Internet.

5.3 La empresa está a disposición de los empleados para cualquier aclaración, duda, consulta o comunicación de cualquier incumplimiento que pueda surgir respecto a las pautas expuestas.

5.4 En el caso de que se desee comunicar cualquier incumplimiento del Código Telemático de Conducta, se realizará a través del Canal de Denuncia puesto a disposición de los empleados.

6. Utilización de los medios informáticos

Principios generales:

6.1 Todos los equipos informáticos facilitados a los empleados son propiedad de la empresa, que pone a disposición de los mismos, los medios y equipos (hardware) necesarios para la prestación de sus servicios laborales. Por ello, estos medios no son adecuados para un uso personal o extra profesional más allá de lo permitido por las reglas del presente Código de Conducta Telemática.

6.2 No está permitido alterar los equipos informáticos, ni conectar otros (impresoras, módems, asistentes personales...) a iniciativa del empleado, sin contar con la debida autorización expresa del responsable del departamento de informática.

6.3 Las normas de este capítulo, son de aplicación tanto a los equipos informáticos fijos y portátiles, y a los dispositivos de telefonía móvil a los que los empleados pudieran tener acceso, como a cualquier otro instrumento telemático que se pueda poner a su disposición.

6.4 Es necesario recordar al empleado que disponga de equipos informáticos portátiles o dispositivos de telefonía móvil, que debe extremar su precaución fuera de las instalaciones de la empresa para salvaguardar la confidencialidad de los datos almacenados. Si se produce la pérdida o sustracción de estos dispositivos, se debe comunicar inmediatamente mediante un correo electrónico dirigido directamente al responsable del departamento de informática.

6.5 Queda expresamente prohibido el acceso o entrada por cualquier medio en los sistemas informáticos utilizando una clave de identificación personal o contraseña de otro usuario.

Finalización de la relación laboral con la empresa:

6.6 A partir de la finalización de la relación laboral con la empresa, no se podrá tener acceso a los equipos informáticos y a los archivos incluidos en los mismos.

6.7 Si el ex empleado tiene en su poder determinados medios o equipos informáticos o (ordenador portátil, CD Rom, disquetttes, etc) o dispositivos de telefonía móvil, tendrá que devolverlos inmediatamente a la finalización de su colaboración.

7. Protección de datos:

7.1 Todos los empleados de la empresa, en la medida en que, por su actividad profesional pueden tener acceso a ficheros de datos de carácter personal, están obligados a guardar absoluta confidencialidad sobre los mismos así como a observar las prescripciones de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (en adelante LOPD) y el Reglamento de Seguridad que lo desarrolla.

7.2 Por lo que respecta al objeto de este Código de Conducta Telemático, se recuerda, que entre las funciones y obligaciones del personal que tiene acceso a datos personales se establece la responsabilidad del usuario final en cuanto a:

- Utilizar su identificador personal/contraseña para la realización de sus acciones. Las contraseñas individuales no deben ser compartidas o reveladas a otro usuario distinto del autorizado.
- Renovar periódicamente sus contraseñas con el fin de protegerlas del conocimiento de usuarios no autorizados.
- Proteger los Sistemas de Información que les han sido asignados físicamente, como por ejemplo, equipos personales, servidores, etc.
- No ceder directa ni indirectamente información confidencial a ninguna persona, salvo personal de la sociedad o de sus proveedores que necesiten conocerla para desarrollar las funciones que tiene encomendadas, siempre que hayan firmado compromisos de confidencialidad semejantes al contenido en el Documento de Seguridad.
- No sacar información confidencial de las instalaciones de la empresa o de sus sistemas de información sin consentimiento de la Dirección.
- No utilizar información confidencial en su propio beneficio o en el de otra persona o entidad.
- Cumplir con los procedimientos de seguridad establecidos para proteger la información y contribuir a asegurar su confidencialidad.
- Devolver los permisos de acceso inmediatamente después de finalizar la necesidad del mismo, al cambiar de responsabilidad o al finalizar la relación laboral.

8. Utilización de los programas y de los archivos informáticos

Principios generales:

8.1 El software, los archivos, programas y documentos informáticos instalados o contenidos en la red de la empresa, así como en otro tipo de herramientas informáticas deben ser utilizados con una finalidad profesional, sin que sean adecuados para un uso personal o privado.

8.2 La información de carácter confidencial incluida en los archivos y documentos dentro de la entidad, no podrá enviarse a través de ninguna herramienta a terceras personas o compañías distintas de las que deben recibir la información.

8.3 Es política de la empresa evitar cualquier tipo de actuación a través de los equipos informáticos y de telecomunicaciones que pueda considerarse como acoso o intimidación en el trabajo. Por consiguiente, no se deben instalar o visualizar, salvapantallas, fotos, videos o cualquier otro tipo de reproducción o visualización de contenido ofensivo o atentatorio contra la dignidad de la persona humana y, en especial, de contenido sexual.

Instalación de programas:

8.4 Los programas informáticos instalados en los equipos informáticos son propiedad de la empresa. Está prohibida la reproducción de los mismos para fines no profesionales.

8.5 La instalación de programas informáticos debe realizarse siempre con autorización previa y bajo supervisión del departamento informático de la empresa. Esta cláusula también es de aplicación a la instalación de software relativo a juegos o la instalación de programas de música u otros similares, para los que no se hayan obtenido los correspondientes permisos legales.

Facultad de revisión:

8.6 Cuando se estime necesario por motivos relacionados con el buen funcionamiento de la empresa, ésta se reserva la facultad de revisar periódicamente, a través de los servicios técnicos, los archivos y contenidos elaborados por cada empleado y almacenados en la red telemática local, así como el contenido del disco duro del equipo informático que sea utilizado por los empleados en el desempeño de sus funciones.

9. Navegación en la red de Internet

Principios generales:

9.1 Las conexiones que se produzcan a través de la red Internet deben obedecer a fines profesionales, con el fin de obtener el mayor aprovechamiento de los recursos informáticos.

9.2 Se prohíbe expresamente el acceso a direcciones de contenido sexual, racista, etc.; y en general, atentatorios contra la dignidad humana o a los derechos fundamentales.

9.3 Es propósito de la empresa velar por el cumplimiento de las leyes de la propiedad intelectual o industrial, por lo que los empleados deberán comprobar, antes de utilizar información proveniente de Internet, si la misma se encuentra protegida por las leyes de la propiedad intelectual o industrial.

Facultad de Revisión:

9.4 Cuando se estime necesario para la protección del patrimonio empresarial o por motivos de funcionamiento de la empresa, ésta se reserva la facultad de revisar periódicamente, a través de los servicios técnicos, los datos de las conexiones a la red de internet desde los ordenadores utilizados por los empleados, así como el contenido concreto de dichas conexiones.

10. Uso del correo electrónico

Principios generales:

10.1 La dirección interna de correo electrónico que se adjudica por el departamento de informática a cada empleado no se considera privativa de éste, sino en la medida en que se facilita para que se use como la identificación del empleado en el correo electrónico interno de la empresa, es propiedad de ella. En consecuencia, y dado que el correo electrónico – así como Internet – es una herramienta de trabajo, la sociedad se reserva la posibilidad de controlar e inspeccionar y acceder a las direcciones de correo para comprobar el correcto uso de las comunicaciones electrónicas y la información transmitida en la red y los expedientes electrónicos localizados en los pc's y ordenadores propiedad de la empresa.

10.2 No está permitido el uso del correo electrónico para el envío al exterior a direcciones de Internet de datos, informaciones o ficheros particulares, o de datos internos de la empresa o datos de clientes, a personas ajenas a la sociedad o que por su actividad no esté justificado su conocimiento y envío.

10.3 Por razones de seguridad ante la posibilidad de incorporar virus así como por ser extraños al correcto uso de los medios informáticos, los ficheros, datos imágenes, etc... que se reciban del exterior a través de internet no podrán ser transmitidos internamente por empleados a otros mediante el correo electrónico sin haber realizado los correspondientes chequeos con el apoyo del área de soporte microinformático. El empleado deberá ocuparse de no recibir del exterior correos particulares y ajenos a su trabajo y, en caso de recibirlos, de proceder a su inmediata destrucción, comunicando al emisor la improcedencia de tales envíos.

Facultad de Revisión:

10.4 Cuando se estime necesario para la salvaguarda de la sociedad y de los demás empleados o por motivos relacionados con el funcionamiento de la empresa, ésta se reserva la facultad de revisar periódicamente, a través de los servicios técnicos, el contenido del correo electrónico empresarial asignado a cada empleado para el desempeño de sus funciones laborales.

11. Uso del teléfono fijo y de dispositivos de telefonía móvil.

Principios generales:

11.1 En ningún caso se podrán utilizar las líneas de voz fijas o móviles de la empresa puestas a disposición de los empleados para enviar comunicaciones de

voz o mensajes que sean ilegales, ilícitos, ofensivos, que atenten contra la dignidad humana, contra los derechos fundamentales o que sean susceptibles de ser considerados delictivos.

11.2 Se prohíbe la interceptación o el uso no autorizado de las líneas y terminales de voz fija y móvil de otros empleados.

11.3 Las tarjetas ubicadas dentro de los terminales móviles de empresa (tarjetas SIM) que proporcionan línea de voz móvil, no se podrán retirar del terminal suministrado por la empresa para su utilización en terminales privados del empleado.

Finalización de la relación laboral:

11.4 El empleado tiene acceso a los teléfonos fijo o móvil de empresa mientras su relación laboral esté vigente. Cuando ésta se extinga, la empresa retirará el citado acceso y podrá solicitar la baja de las líneas al proveedor.

12. Incumplimiento del Código de Conducta Telemática y quebranto del deber de confidencialidad

12.1 El incumplimiento de las normas incluidas en el presente Código de Conducta Telemática será considerado una transgresión de la buena fe contractual y abuso de confianza respecto a las tareas encomendadas, por lo que podrán adoptarse por la empresa las medidas correctoras necesarias en proporcionalidad a la gravedad de las infracciones.

12.2 Igualmente, el quebranto del deber de confidencialidad en el uso y tratamiento de datos tanto de carácter personal como empresarial, será considerado un grave incumplimiento de las obligaciones laborales que podrá motivar la adopción por la empresa de medidas sancionadoras y correctoras.

13. Entrada en vigor y vigencia

13.1 El contenido del presente Código de Conducta es de obligatorio cumplimiento para todos los empleados. Su contenido entrará en vigor a partir de la comunicación a la plantilla de la empresa y se mantendrá vigente en tanto no sea modificado o reemplazado por otro.

D. Pedro Manuel Moreno Borreguero
Director General.