Ership
Grupo

PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

INFORMACIÓN, CONTROL DE MODIFICACIONES Y APROBACIÓN

Información importante sobre este documento	
Identificación de la Política	Política de Seguridad de la Información
Política de aplicación global o nacional	Global
Apartado de otras Políticas que desarrolla	
Normas que sustituye	N/A
Normas que deroga	Todas las anteriores en la misma materia
Normas relacionadas	Código Ético Código de Conducta
Unidad de negocio o función a la que afecta	Todas
Personal al que afecta	Todo
Responsable principal de su vigilancia	Unidad de Cumplimiento

Este Protocolo será revisado cuando se detecten situaciones que aconsejen actualizar su contenido, produciéndose entonces una nueva versión del mismo.

Nombre del Fichero	Versión	Resumen de Cambios	Autor	Fecha

El presente Protocolo ha sido aprobada por las siguientes personas en las fechas indicadas a continuación.

Nombre	Departamento	Cargo	Firma	Fecha

DESCRIPCIÓN DEL RIESGO

Los riesgos para la seguridad de la información con relevancia penal están descritos en los artículos 197 y 264. y son los siguientes:

DESCRIPCIÓN DEL RIESGO		SITUACIONES AGRAVADAS	PENAS PERSONA JURÍDICA
Art. 197 CP Descubrimiento y revelación de secretos	Conducta: Descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, apoderándose de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o interceptando sus telecomunicaciones o utilizando artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación	Organización criminal	- pena de multa de seis meses a dos años. - Posibilidad de imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.
Art. 264 CP Daños informáticos	Conducta: Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles, por cualquier medio y sin autorización, datos programas informáticos o documentos electrónicos ajenos. Obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sin estar autorizado.		a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años. b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos. - Posibilidad de imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

INTRODUCCIÓN

En una economía globalizada como la actual, la informática y los medios telemáticos han adquirido un papel esencial en el desarrollo empresarial de cualquier operador económico. Especialmente en el Grupo ERSHIP, presentes en más de 40 puertos en todo el mundo, los medios informáticos no son solo una herramienta, sino ya una necesidad.

Y con las muchas ventajas de la informatización de la actividad económica vienen también algunas debilidades que toda empresa con cierto compromiso ético debe prevenir y aminorar.

Por un lado, existen los denominados delitos informáticos *lato sensu*, entre los que se encuentran las conductas consistentes en deteriorar, alterar o suprimir, entre otras, los programas informáticos o documentos electrónicos ajenos, así como hacer inaccesibles datos informáticos sin estar autorizado para ello. Pero no solo, pues los medios informáticos pueden dar lugar a la posibilidad de descubrir ilícitamente secretos o vulnerar la intimidad de otro, sin su consentimiento, prácticas todas ellas rechazadas por la cultura empresarial comprometida que define a ERSHIP.

Pero, por otro lado, el Grupo también puede verse víctima de dichos delitos informáticos. Correos spam, *fishing* y *malware* como archivos adjuntos a un correo de apariencia inofensivo son algunas de las formas más corrientes de verse perjudicado por alguno de estos tipos penales.

Es por esto que, por medio del presente protocolo, ERSHIP pretende implementar una serie de medidas, controles y procedimientos tendentes a prevenir y evitar la comisión de delitos informáticos, así como minimizar el riesgo de ser víctima de los mismos y neutralizar las consecuencias negativas que estos pudieran tener sobre el Grupo.

CAPÍTULO I. ASPECTOS GENERALES

ARTÍCULO 1. FINALIDAD DEL PRESENTE PROTOCOLO

1. La estrategia de lucha para garantizar la seguridad de la información de la Sociedad consiste principalmente en asegurar el cumplimiento de la normativa aplicable y en procurar una adecuada coordinación de las prácticas en los negocios seguidas por las sociedades del Grupo, todo ello en el marco de la consecución del interés de la protección de la intimidad personal y seguridad informática en los negocios y del apoyo a una estrategia empresarial a largo plazo que evite riesgos derivados de la falta de seguridad en la información en la ejecución de las decisiones de negocio.

2. Para ello, la Sociedad toma en consideración todos los intereses legítimos que confluyen en su actividad.

ARTÍCULO 2. ÁMBITO DE APLICACIÓN Y SUJETOS OBLIGADOS

1. Este Protocolo de Seguridad de la Información es de aplicación en todas las sociedades que integran el Grupo, así como en las sociedades participadas no integradas en el Grupo sobre las que la Sociedad tiene un control efectivo, dentro de los límites legalmente establecidos.

2. Sus normas deberán ser observadas por todos los profesionales del Grupo, con independencia de su nivel jerárquico, de su ubicación geográfica o funcional y de la sociedad del Grupo para la que presten sus servicios.

3. A efectos de este protocolo, se consideran Sujetos Obligados los accionistas, los miembros del Consejo de Administración, los directivos y empleados de todas las sociedades y entidades que lo integran, así como aquellas otras personas cuya actividad se someta expresamente al presente protocolo.

4. En aquellas organizaciones y entidades en las que el Grupo, sin tener una participación mayoritaria, se responsabilice de la gestión, los profesionales que representen al Grupo promoverán la aplicación del presente Código.

5. Además, este Protocolo de Seguridad de la Información es también aplicable, en lo que proceda, a las empresas contratadas que actúen en nombre de la Sociedad, así como a las *joint ventures*, uniones temporales de empresas y otras asociaciones equivalentes, cuando la Sociedad asuma su gestión.

6. Su aplicación se adaptará a la normativa sectorial de cada uno de los ámbitos de negocio de ERSHIP.

ARTÍCULO 3. EXCEPCIONES

Salvo las expresamente previstas en su redactado, el presente Protocolo no contempla excepciones a su debida aplicación por parte de todos los Sujetos Obligados.

CAPÍTULO II. PRINCIPIOS Y CONDUCTAS PROHIBIDAS

ARTÍCULO 4. PRINCIPIOS Y OBJETIVOS

1. Mediante el presente Protocolo, ERSHIP proclama su voluntad de cumplir con la normativa reguladora del sector de las telecomunicaciones. El presente texto se configura con el objetivo de proporcionar al personal de Ership unas pautas de conductas adecuadas en relación con los distintos medios y soportes de tipo digital de obligado cumplimiento.

2. Este Protocolo desarrolla el compromiso adquirido por ERSHIP de actuar de acuerdo con la legislación aplicable para cada uno de los sectores de actividad en los que interviene, así como la responsabilidad ética de proteger los derechos a la intimidad del propio personal y de terceros que puedan relacionarse con el Grupo.

3. ERSHIP se opone al uso de los medios informáticos con fines ilegales. Ello abarca no solo las conductas delictivas, sino cualquier conducta que pueda considerarse ilícita, bien sea cometida contra el propio Grupo o en beneficio del mismo, contra su personal o contra cualquier tercero.

ARTÍCULO 5. CONDUCTAS PROHIBIDAS

1. No se destruirá, alterará, inutilizará o de cualquier otra forma dañará los datos, programas o documentos electrónicos propiedad de ERSHIP o de terceros sin expreso consentimiento de persona competente.

2. No se obstaculizará intencionadamente el acceso de otros usuarios a la red.

3. No se enviarán mensajes calificados como *spam* desde los medios telemáticos proporcionados por ERSHIP.

4. No se introducirán intencionadamente programas o aplicaciones que causen, o sean susceptibles de causar, cualquier tipo de alteración en los sistemas informáticos propiedad de ERSHIP o de terceros.

5. No se introducirán, descargarán de Internet, reproducirán, utilizarán o distribuirán programas informáticos no autorizados expresamente por ERSHIP, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezca a un tercero y no se disponga de la correspondiente licencia o autorización para ello.

6. No se instalarán copias ilegales de cualquier programa informático, incluidos los programas corporativos.

7. No se eliminará cualquiera de los programas informáticos legal y debidamente instalados por el Departamento de IT.

8. No se descargará, reproducirá, almacenará o enviará desde los efectos informáticos de ERSHIP contenidos obscenos, inmorales, ofensivos, o cualquier otro que no sea acorde a las labores desarrolladas por ERSHIP.

9. No se accederá de forma fraudulenta a las páginas web expresamente prohibidas por el Departamento de IT.

10. No se enviará información sensible o confidencial a través del correo electrónico, si no es estrictamente necesario.

11. No se utilizará el correo electrónico corporativo para el envío o recepción de datos personales ajenos a las labores de ERSHIP.

12. No se abrirán documentos adjuntos ni enlaces sin comprobar el remitente y el contenido del correo electrónico, y en todo caso, sin proceder conforme al procedimiento de control desarrollado en este Protocolo.

CAPÍTULO III. MEDIDAS PREVENTIVAS Y DE CONTROL

ARTÍCULO 6. IDENTIFICACIÓN DEL USUARIO

1. El Departamento de IT establecerá un sistema de identificación y autentificación de usuarios y gestión de credenciales de usuarios para cada uno de los efectos informáticos corporativos, a los efectos de poder identificar el usuario que hace uso del efecto en cada momento.

2. Las contraseñas para la identificación de los usuarios de ERSHIP deberán ser robustas y ser cambiadas al menos una vez al año.

ARTÍCULO 7. LICENCIAS DE USO

El Departamento de IT establecerá un inventario de licencias de uso de programas informáticos que mantendrá continuamente actualizado.

ARTÍCULO 8. ACCESOS PROHIBIDOS

El Departamento de IT a través de su proveedor de antivirus, gestiona una tipología de páginas web que, bien por considerar su contenido obsceno, inmoral u ofensivo, bien por entender que su acceso es contrario a los valores éticos de ERSHIP, se entenderán como prohibidas. El Departamento de IT a través de un firewall impide el acceso a dichas páginas web desde los efectos informáticos corporativos, pudiendo de manera extraordinaria y con autorización, desbloquear temporalmente una de estos sitios web.

ARTÍCULO 9. MEDIDAS DE CONTROL CONTRA EL *SPAM*, EL *FISHING* Y LOS CORREOS ELECTRÓNICOS CON ARCHIVOS ADJUNTOS SOSPECHOSOS

A fin de evitar que ERSHIP sufra un ataque informático, el personal de ERSHIP deberá actuar planteándose tres preguntas ante cualquier e-mail recibido a la dirección de correo corporativo:

a) ¿Conozco al remitente? Si no se conoce al remitente, lo más probable es que deba descartar el correo electrónico recibido.
b) ¿Esperaba el correo? Si es de un remitente conocido, pero no se esperaba dicho correo, debe tenerse cierta precaución en cuanto a lo que le pida dicho correo y aún más respecto a los archivos que dicho correo adjunte.
c) ¿Reconozco el archivo adjunto? En el caso de descargar el archivo adjunto de un correo electrónico, debe analizarlo con el software anti-*malware* autorizado por el Departamento de IT antes de abrirlo. En caso de duda, elimine el archivo.

Adicionalmente habrá que poner siempre bajo el conocimiento de Departamento de IT, estas situaciones para que actúen en consecuencia y le den el debido seguimiento.

CAPÍTULO IV. SEGUIMIENTO, CONTROL Y PROCEDIMIENTO

ARTÍCULO 10. DEBER DE COMUNICAR UN POSIBLE DAÑO INFORMÁTICO

1. Cuando algún miembro del personal de ERSHIP tenga la sospecha de haber sido víctima de *fishing* o ha descargado un archivo adjunto que ha resultado ser, o sospecha que pueda ser un *malware*, lo pondrá en conocimiento del Departamento de IT de forma inmediata, incluso antes de detectar un comportamiento anormal por parte del efecto informático.

2. También podrá dirigirse directamente a los miembros de la Unidad de Cumplimiento o bien, podrá hacerlo por medio del Canal de Denuncias.

3. En cualquier caso ERSHIP garantizará el carácter confidencial de la denuncia y de los datos del denunciante, así como la indemnidad del denunciante de buena fe.

4. En caso de tener alguna pregunta o duda sobre el contenido del presente protocolo o si no se está seguro/a de cómo aplicarla en determinados casos, los Sujetos Obligados pueden ponerse en contacto con la Unidad de Cumplimiento de ERSHIP a través de los medios mencionados.

ARTÍCULO 11. INCIDENCIA DE LAS INVESTIGACIONES INTERNAS EN LA GESTIÓN DE LA INFORMACIÓN

1. Los efectos corporativos de ERSHIP son siempre propiedad del mismo, con independencia del usuario al que se presten, y se les deberá dar un uso acorde con la actividad económica y los valores éticos suscritos por el Grupo.

2. El principio de transparencia impone la necesidad de que la Unidad de Cumplimiento pueda llevar a cabo las correspondientes inspecciones en los efectos informáticos corporativos.

3. El uso de los efectos informáticos corporativos supone la aceptación, por parte del usuario, de la posibilidad de que la Unidad de Cumplimiento, en el marco de una investigación interna, pueda acceder a dicho efecto y volcar la información que contenga y se crea

necesaria para el buen fin de la investigación.

4. En el marco de una investigación interna, la Unidad de Cumplimiento podrá autorizar el acceso al ordenador, tabletas, teléfonos móviles y cualesquiera otros efectos informáticos corporativos de cualquier usuario para recabar la información necesaria para el buen fin de la investigación. Dicho acceso deberá ser proporcional con el fin de la investigación y deberá limitarse únicamente al contenido que pueda comprender la información que se busca, no siendo posible un acceso inquisitivo. La información obtenida a raíz de dicho acceso tendrá carácter confidencial.

5. En el marco de una investigación interna, la Unidad de Cumplimiento podrá autorizar el acceso al correo electrónico corporativo de cualquier usuario para recabar la información necesaria para el buen fin de la investigación. Dicho acceso deberá ser proporcional con el fin de la investigación y deberá limitarse únicamente al contenido que pueda comprender la información que se busca, no siendo posible un acceso inquisitivo. La información obtenida a raíz de dicho acceso tendrá carácter confidencial.

ARTÍCULO 12. RÉGIMEN SANCIONADOR

1. En caso de que se produzca un incumplimiento por parte de algún Sujeto Obligado, ERSHIP aplicará el régimen sancionador previsto en Código de Conducta, de acuerdo con la gravedad del incumplimiento y dentro del marco legal aplicable en la jurisdicción donde se haya cometido. Asimismo, ERSHIP pondrá en conocimiento de las Autoridades pertinentes el incumplimiento normativo si pudiese haber indicios de delito.

2. La Unidad de Cumplimiento coordinará:

a) Con el Departamento de Recursos Humanos aquellas acciones que sean necesarias adoptar en relación con el personal de ERSHIP.
b) Con el Departamento de Asesoría Jurídica de ERSHIP las que resulten de aplicación a las personas asociadas con ERSHIP por relación mercantil.

3. En ambos casos, la Unidad de Cumplimiento informará inmediatamente al Consejo de Administración, cuando la gravedad de los casos así lo aconseje.

4. En cualquier caso, las medidas que se adopten se ceñirán al principio de proporcionalidad, dándose audiencia al afectado a fin de que pueda dar razón de lo ocurrido.

ARTÍCULO 13. REVISIÓN DE RESULTADOS

1. ERSHIP revisará periódicamente su política de seguridad de la información, especialmente el grado de cumplimiento de las actuaciones iniciadas conforme al programa establecido, los resultados de las mismas y de la legislación aplicable.

2. Para la revisión del grado de cumplimiento en la seguridad de la información se tendrán en cuenta por lo menos los siguientes factores:

a) Quejas externas.
b) Sugerencias internas.
c) Actuaciones de empresas de la competencia.
d) Opinión de clientes.
e) Legislación futura.
f) Planes sectoriales.
g) Nuevas tecnologías aplicables al sector de actividad de la compañía de acuerdo con su objeto social.

ARTÍCULO 14. SEGUIMIENTO Y CONTROL

1. Las sociedades del Grupo adoptarán los mecanismos de control necesarios para asegurar, dentro de una adecuada seguridad de la información, el cumplimiento de la normativa. Igualmente, dedicarán a tales fines los recursos humanos y materiales adecuados y suficientemente cualificados.

2. Anualmente, la Unidad de Cumplimiento, en coordinación con el Departamento de IT, realizará informes del grado de cumplimiento del Protocolo de Seguridad de la Información.

ARTÍCULO 15. MONITORIZACIÓN

1. Para garantizar el cumplimiento continuado de los procedimientos desarrollados en este Protocolo, ERSHIP realizará revisiones internas y periódicas, emitiendo los correspondientes informes de conclusiones, que serán valorados por la Unidad de Cumplimiento, para en su caso informar al Consejo de Adminsitración.

2. En dichos informes se hará mención expresa a las deficiencias detectadas durante la revisión y se establecerán los planes de actuación para su subsanación.

3. La periodicidad de esta revisión interna se establecerá siguiendo criterios objetivos que garanticen el cumplimiento normativo.

4. La Unidad de Cumplimiento mantendrá un registro actualizado de los incumplimientos que lleguen a su conocimiento, así como de las acciones efectuadas frente a ellos.

5. En caso de que, tras la correspondiente denuncia e investigación, se detecte que el incumplimiento de las disposiciones aquí contenidas ha sido fruto de un defecto en los procedimientos o controles implementados por ERSHIP, se procederá a su revisión y actualización con la finalidad de evitar que se reproduzcan en el futuro.

CAPÍTULO V. CONSIDERACIONES ADICIONALES

ARTÍCULO 16. CONOCIMIENTO DE LA LEGISLACIÓN

1. La empresa tiene la obligación de conocer toda la legislación que le aplica y las consecuencias potenciales de su no cumplimiento.

2. Los requisitos legales aplicables se mantendrán permanentemente actualizados para evitar el riesgo de incumplir nueva normativa en materia de seguridad de la información que pudiera surgir con posterioridad a la aprobación e implementación del presente Protocolo.

ARTÍCULO 17. DIFUSIÓN

1. ERSHIP establecerá las medidas oportunas para que los empleados, directivos y miembros del Consejo de Administración tengan conocimiento de las exigencias derivadas de la normativa sobre seguridad de la información. Dichas medidas incluyen la organización de planes de formación y cursos especiales de formación que, dirigidos al personal en general y específicamente a las personas que desempeñen aquellos puestos de trabajo, que, por sus características, sean idóneos para detectar los hechos y operaciones que puedan estar relacionados con conductas de riesgo para la seguridad de la información, capaciten a todo el personal para efectuar dicha detección y para conocer la manera de proceder en tales casos.

2. Este protocolo se entregará al personal de ERSHIP que, por su actividad, pueda

incurrir en algunos de los riesgos descritos.

3. En el caso de las personas asociadas a la Sociedad, será función de quien contrate con ellas cerciorarse y documentar que dichas personas asociadas conocen tanto el Código de Conducta de ERSHIP como este Protocolo, estando alineadas y respetando el contenido de ambos textos.

4. La Unidad de Cumplimiento se ocupará de que los Sujetos Obligados dispongan de acceso a este Protocolo, promoviendo aquellas medidas necesarias para que su contenido sea fácilmente accesible y solventando cualquier duda que personal, empleados, responsables, directivos o personas asociadas a ERSHIP puedan plantearle respecto de su contenido y alcance.

ARTÍCULO 18. FORMACIÓN

Corresponderá al Departamento de Recursos Humanos la promoción de formación recurrente entre el personal de ERSHIP, cerciorándose de que todos los Sujetos Obligados por este Protocolo realizan y aprovechan la formación a su alcance.

ARTÍCULO 19. REVISIÓN DEL PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN

1. El presente Protocolo deberá mantenerse permanentemente actualizado.

2. Serán causas de actualización del Protocolo:

a) Cambios en el entorno legislativo.

b) Adaptación a políticas, recomendaciones o estándares establecidas por ERSHIP.

c) Introducción de todas aquellas modificaciones que sean necesarias para mejorar la operativa de prevención derivada de los desarrollos y mejores prácticas observados en el sector o del análisis de aquellos puntos de mejora identificados por la Unidad de Cumplimiento o por el Departamento de IT.

3. Bajo la responsabilidad la Unidad de Cumplimiento se llevará un registro de los cambios al Protocolo. Dicho registro incluirá la indicación resumida de las modificaciones efectuadas, causas que han motivado dichos cambios, así como las fechas en las que éstos se han llevado a cabo.

4. Las modificaciones del Protocolo que pudieran resultar necesarias como resultado del procedimiento de actualización, serán realizadas por la Unidad de Cumplimiento de Ership.

5. Una vez realizadas las modificaciones, se pondrá el Protocolo a disposición de todos los Sujetos Obligados.