

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN ("TIC") DEL CENTRO OPERATIVO CICLO COMERCIAL, S.A.U.

I.- PREÁMBULO.

La evolución y auge de las nuevas tecnologías de la información y la comunicación está generando en nuestra sociedad un cambio sustancial en las relaciones personales entre individuos, pero también en el mundo empresarial y de los negocios.

Los grandes cambios y la evolución de las herramientas de comunicación informática y de las nuevas tecnologías de la información permiten alcanzar cotas de eficiencia empresarial hasta ahora inimaginables; al tiempo, estas herramientas conllevan una importante responsabilidad compartida entre las propias empresas y los usuarios y beneficiarios de dichos medios en el ámbito empresarial.

Resulta por ello imprescindible elaborar, desarrollar y fomentar dentro del ámbito empresarial aquellos mecanismos de protección y seguridad oportunos que garanticen infraestructuras informáticas adecuadas y permanentemente actualizadas de las que puedan beneficiarse conjuntamente las empresas y los profesionales que las integran, desarrollando al tiempo cuantos elementos garanticen la integridad y seguridad de sus sistemas.

Por ello, el Centro Operativo Ciclo Comercial, S.A.U. (en adelante "la Sociedad") define su Política de Seguridad de la Información y Uso de las TIC, elaborando las directrices y principios que garanticen un uso adecuado y eficaz de los mecanismos tecnológicos, dentro de un entorno seguro para la información.

La política y sus directrices se rigen por los principios de concienciación social, cooperación, integridad, transparencia, legalidad y buena fe de la Sociedad y de todos los profesionales que la integran, (se consideran tales, administradores, directivos y empleados) (los "Profesionales"), sobre la base de su Código Ético.

En la Sociedad se reconoce expresamente la importancia de los Sistemas de Información, así como la necesidad de su protección, con el objeto de evitar pérdidas de datos y/o uso no autorizado o ilícito de los mismos que pudieran causar daños importantes a los clientes, Profesionales, y/o a la propia compañía y su imagen en el mercado.

A tal efecto, se define la presente Política con el propósito de adoptar cuantas medidas de índole técnica y organizativa sean necesarias para garantizar la integridad, disponibilidad y confidencialidad de los datos y los sistemas de información que los soportan. El compromiso de la Sociedad se concreta en los siguientes puntos:

- Inversión constante y responsabilidad de la seguridad de la información. Se establecerán los medios necesarios y adecuados para proteger y garantizar la seguridad de los datos, personas, programas, equipos, instalaciones, documentación y otros soportes que configuran los sistemas informáticos y tecnológicos de la Sociedad con el fin de evitar la alteración, copia, pérdida, tratamiento o acceso no autorizados de la información que contienen. Al mismo tiempo corresponderá a todos los Profesionales de la Sociedad conocer y respetar los mecanismos de seguridad adoptados por la compañía.
- Desarrollo y adaptación continua a los avances de la técnica. La presente política se especificará y desarrollará a través de normas, guías, estándares, circulares, manuales y procedimientos, que se irán actualizando cuando sea necesario en función de las nuevas exigencias impuestas por los avances de la tecnología.

- Difusión de la información y formación. Se fomentará la difusión de la información y la formación a todos los Profesionales y a consultores, agentes o terceros contratados, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible.
- Control de riesgos. Se establecerán controles adecuados y razonables, preventivos, de detección y correctivos frente a posibles conductas delictivas y a aquellos riesgos que puedan influir en que la información no sea exacta, completa o no esté disponible dentro del tiempo fijado. Estos controles serán proporcionados y adecuados a la criticidad de los activos a proteger y a su clasificación. Asimismo, dichos controles serán auditables en base a las Normas y Procedimientos aplicables y siempre de acuerdo con la legalidad vigente.

II.- ÁMBITO DE APLICACIÓN

La presente Política de Seguridad de la Información y Uso de las TIC es de obligado cumplimiento para todos los usuarios de los sistemas de información y comunicaciones de la Sociedad.

A estos efectos, se considerarán usuarios a los Profesionales de la Sociedad, integrado por todo el personal directivo, técnico, administrativo, productivo o de servicios, con independencia del tipo de contrato laboral que ostente, ya sea fijo, temporal o cualquier otro, así como demás colaboradores, consultores, agentes o terceros contratados.

Igualmente, se considerará como usuarios a los terceros clientes, proveedores, subcontratistas y demás asimilados que trabajen para la Sociedad y a todos aquéllos a quienes se les facilite el acceso a los mecanismos y recursos informáticos y tecnológicos de la Sociedad.

A través de los diferentes canales de comunicación disponibles (telefónico, presencial, correo electrónico – codigoetico.coc@agbar.es - y dirección postal del domicilio social) se atenderá y resolverá cualquier pregunta, duda o incertidumbre sobre la aplicación de esta política en cada caso concreto.

III.- DIRECTRICES EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN Y DEL USO DE LAS TIC

Junto al compromiso de la Sociedad en la creación, desarrollo, mantenimiento y control de los sistemas más eficaces y robustos de tecnologías de la comunicación y de la información, es esencial mantener un conjunto de directrices en la seguridad de la información y los usos de la tecnología.

La presente Política recoge las directrices esenciales relacionadas con la seguridad de la información y con las TIC, con la finalidad de que todos los esfuerzos de la organización confluyan en los siguientes objetivos primordiales: salvaguardar la seguridad de los sistemas tecnológicos de la Sociedad y de la información que éstos contienen, así como garantizar el correcto desarrollo de la prestación de servicios profesionales.

Puntos clave a tener en cuenta

El compromiso de la Sociedad con el cumplimiento de las leyes y los principios en que se inspiran es absoluto en todos y cada uno de sus ámbitos de actividad y forma parte esencial del desarrollo de su actividad bajo los principios de ética y excelencia.

En relación con las tecnologías de la información y la comunicación, las leyes españolas prohíben y castigan, entre otras, las siguientes conductas:

- El uso, la tenencia o la difusión de programas informáticos y archivos protegidos por derechos de propiedad intelectual o industrial, para los que se carezca de autorización o licencia de uso.
- El uso, la tenencia o la difusión de programas o medios destinados a neutralizar o suprimir las medidas de protección de los programas informáticos y archivos protegidos por derechos de propiedad intelectual o industrial.
- Borrar, deteriorar, alterar, suprimir o hacer inaccesibles programas informáticos o documentos electrónicos, o por los mismos medios impedir el normal funcionamiento de un sistema informático.
- Invadir la esfera de intimidad de otro mediante la interceptación de sus correos electrónicos o la sustracción de sus documentos o imágenes, así como su posterior difusión.
- El descubrimiento, apoderamiento o interceptación, por cualquier medio, de datos o información empresarial de carácter restringido, secreto o confidencial, así como su posterior difusión.
- La modificación, el apoderamiento o la utilización de datos reservados ajenos, así como su posterior difusión.
- La descarga, tenencia o difusión de contenido racista, sexista, xenófobo, pedófilo, pornográfico, denigrante o ilegal.
- El acoso.

Las anteriores conductas pueden ser castigadas con penas graves tanto para la persona física (hasta 5 años de prisión en algunos casos y multa) como para la empresa en nombre de la cual esa persona física eventualmente actúe (multas, suspensión de actividades, clausura de locales, etc.).

Con la finalidad de analizar incidentes de seguridad y asegurar que el uso de las tecnologías de la información y la comunicación se realiza de conformidad con esta política, la Sociedad dispone de mecanismos de monitorización y registro de los sistemas informáticos puestos a disposición de los usuarios. Esto incluye, entre otros, el uso de Internet y del correo electrónico corporativo, así como el uso de los equipos informáticos fijos y portátiles como estaciones de trabajo, dispositivos móviles, dispositivos de almacenamiento de datos, etc.

Directrices en el ámbito de Seguridad de la Información

Las siguientes directrices responden a los principios éticos y de seguridad en el desarrollo de la actividad de la Sociedad y, se dirigen a salvaguardar la integridad y la seguridad de la información puesta a disposición de los usuarios para el óptimo desempeño de sus funciones, y se complementan con las directrices específicas de uso de las TIC.

PRIMERA.- Seguridad del Personal

Todo usuario de los recursos tecnológicos que tenga acceso a los Activos de Información de la empresa, deberá observar el principio de confidencialidad que prohíbe la revelación de información sensible a terceros de dentro o fuera de la Organización sin autorización expresa.

SEGUNDA.- Privacidad

Se observará el cumplimiento de la regulación relacionada con la protección de datos de carácter personal.

TERCERA.- Control de Accesos a los Activos de Información

Las contraseñas son estrictamente confidenciales y personales, y, por tanto, se deberá hacer un uso responsable y diligente de las mismas.

CUARTA.- Responsabilidad del Usuario

Todos los usuarios de recursos tecnológicos que tengan acceso a los Activos de Información de la Sociedad deberán adherirse a las Normas y Procedimientos que se desprendan de esta Política para la protección de los Activos de Información.

QUINTA.- Relaciones comerciales por vía telemática

El establecimiento de una relación con un cliente, socio y/o proveedor a través del comercio electrónico, deberá ir precedido de una estimación de riesgos que determine el valor de la información que se intercambia, el sistema de acceso compartido y el nivel de riesgo aceptable.

SEXTA.- Seguridad de Acceso de Colaboradores Externos

El acceso de colaboradores externos (consultores, agentes o terceros contratados) a las comunicaciones o a los recursos informáticos de la Sociedad se hará de forma restringida y debidamente autorizada.

SÉPTIMA.- Alianzas empresariales

Las interacciones y relaciones que la Sociedad mantiene con sus socios, colaboradores, etc. deberán ser debidamente protegidas para asegurar la confidencialidad, integridad, disponibilidad y trazabilidad de la información de ambas partes. Por tanto, se deberá analizar la información cedida y recibida y los procedimientos de seguridad propios y ajenos, al respecto.

OCTAVA.- Evaluación de Activos de Información y protección de los mismos

Toda la información empresarial de la Sociedad será clasificada y su valor establecido para asegurar que se le otorga la protección adecuada a la información durante su ciclo vital.

NOVENA.- Seguridad de Control de Acceso de Entrada

Se protegerá el acceso a todas aquellas instalaciones que contengan Activos de Información que precisen ser protegidos.

Directrices de uso de las Tecnologías de la Información y la Comunicación (TIC)

Las siguientes directrices responden a los principios éticos y de seguridad en el desarrollo de la actividad de la Sociedad y, particularmente, en el uso de las tecnologías de la información y la comunicación puestos a disposición de los usuarios para el óptimo desempeño de sus funciones. Asimismo, estas directrices se desarrollan y concretan en las Normas y Procedimientos vigentes sobre Seguridad de la Información y TIC, disponibles en la Intranet.

PRIMERA.- La información, los recursos y las herramientas TIC profesionales son propiedad de la Sociedad

Todos los recursos y herramientas informáticas y de comunicaciones puestas a disposición por la Sociedad a sus Profesionales son de su propiedad y se suministran para aumentar la productividad y mejorar el entorno laboral. El usuario de estos recursos informáticos deberá hacer un uso responsable y diligente.

Toda la información contenida en soportes físicos (archivos, papel, etc.) o en soporte electrónico (intranet, equipos informáticos y dispositivos electrónicos de la Sociedad) es parte del conocimiento y valor de la empresa y, por lo tanto, propiedad de la Sociedad.

SEGUNDA.- Uso profesional de los dispositivos y sistemas

Los dispositivos y sistemas puestos a disposición de sus Profesionales por la Sociedad se emplearán exclusivamente para las funciones fines que se desprendan del cargo ocupado.

Cada usuario respetará los privilegios que le han sido atribuidos y actuará en concordancia con los principios éticos y de conducta recogidos en el Código Ético.

TERCERA.- Usos no permitidos de los dispositivos y sistemas

Se considera no permitido cualquier uso de los dispositivos y sistemas contrario a la ley, a la presente Política y a los principios de actuación establecidos en el Código Ético. En particular los que puedan afectar a los principios de integridad, disponibilidad y confidencialidad de los datos, la protección de la propiedad intelectual, el respeto a las personas y su intimidad, y la prevención del descubrimiento o revelación de secretos empresariales.

Los parámetros y límites de actuación de uso de las TIC se desarrollan para cada ámbito dentro del cuerpo normativo, siendo de aplicación directa la norma adjunta "***Uso de los sistemas de información del Centro Operativo Ciclo Comercial, S.A.U.***".

Control y supervisión

La Sociedad vela por la seguridad de la información y por el uso de las TIC conforme a los principios establecidos en la presente Política a través de los mecanismos de supervisión adecuados.

En todo caso, la Sociedad establecerá los mecanismos necesarios para monitorizar la utilización de sus sistemas informáticos, incluyendo entre otros, los servicios de Internet y correo electrónico corporativos, con independencia de la ubicación y dispositivo utilizado.

Los sistemas de control y de seguridad se auditarán periódicamente para garantizar su fiabilidad y eficacia aplicando las normas y procedimientos adecuados que se establecerán a tal fin. De igual modo se auditará periódicamente el seguimiento por parte de los usuarios de las Normas y Procedimientos de seguridad.

Los mecanismos de control referidos en los párrafos precedentes se utilizarán en controles automáticos, periódicos o cuando concurra alguno de los supuestos siguientes:

- existencia de indicios de que un usuario está realizando alguna de las conductas prohibidas por esta Política;
- existencia de indicios razonables de que se puedan estar cometiendo ilícitos penales o de cualquier naturaleza (administrativos, laborales, etc.) a través de los medios TIC de la Sociedad;

- existencia de indicios razonables de una situación de acoso o de cualquier otra conducta en el uso de los medios TIC de la Sociedad que pueda causar perjuicios.

En estos supuestos, la Sociedad podrá investigar el correspondiente incumplimiento, dentro de los límites y garantías legalmente procedentes.

IV.- RESPONSABILIDAD

El incumplimiento de lo dispuesto en esta Política, las directrices de actuación que contiene o las Normas y Procedimientos de desarrollo acarrearán sanciones disciplinarias que, en su caso, pueden conllevar la terminación de la relación laboral o mercantil que el infractor mantenga con la Sociedad, según la legislación y la normativa convencional que resulte de aplicación, así como la iniciación de las acciones legales oportunas por parte de la compañía.

En caso de extinción del contrato de trabajo, se seguirán los procedimientos descritos en las Normas y Procedimientos vigentes.

V.- REPORTE DE INCUMPLIMIENTOS

Cualquier persona de la Sociedad que tenga conocimiento de una actuación que infrinja esta Política o constituya un incumplimiento de alguna de sus directrices deberá ponerlo en conocimiento del *Compliance Officer* a través del *Canal de Comunicación Interno* establecido a estos efectos, remitiéndolo a la dirección postal del domicilio social o al correo electrónico codigoetico.coc@agbar.es

Se tendrán en cuenta, y se investigarán adecuadamente, todas las notificaciones sobre incumplimientos de esta política y sus directrices.

Esta notificación, siempre y cuando se produzca de buena fe, estará amparada por la confidencialidad (de modo que la identidad de la persona que la realiza no será revelada sin su consentimiento).

Asimismo, la Sociedad garantiza que, bajo ninguna circunstancia, podrá derivarse represalia o consecuencia perjudicial alguna para la persona que realice esta notificación de buena fe o para aquellas personas de la Sociedad que presten su colaboración en la investigación de un incumplimiento de esta política.

VI.- COMUNICACIÓN DE ESTA POLÍTICA

La presente Política de Seguridad de la Información y Uso de las TIC será objeto de comunicación a la totalidad de los Profesionales de la Sociedad, así como de acciones periódicas de concienciación y recordatorio de su existencia.

Aquellos consultores, agentes o terceros contratados a quienes se les facilite temporalmente acceso a los recursos informáticos y tecnológicos de la Sociedad deberán adherirse con carácter previo a la presente Política de Seguridad de la Información y Uso de las TIC, de forma que queden vinculados por sus directrices de actuación.

* * *

NOTA: Esta política ha sido aprobada por acuerdo del órgano de administración e incluida en el modelo de prevención, detección y gestión de riesgos penales de Centro Operativo Ciclo Comercial, S.A.U., en fecha 4 de Noviembre de 2019.