Política de Uso de los Recursos TIC

Version: 2.0 Effective since: 03/06/2024

1. Introducción

Este documento contiene las normas de uso y procedimientos que deben ser aplicados en el uso de los recursos de tecnologías de la información y de comunicación (en adelante, "recursos TIC" o "las TIC") proporcionados por la Empresa, esto es, Laboratorios Farmacéuticos ROVI, S.A. y sus filiales o participadas (en adelante, ROVI), y que son de obligado cumplimiento (en adelante, la "Política").

Los trabajadores, ROVI y, por tanto, la presente Política se hallan sometidos en cualquier caso a las disposiciones que establece el Código de Buenas Prácticas de la Industria Farmacéutica en toda interrelación que mantengan con Profesionales Sanitarios y/o Organización Sanitarias, según las define el referido Código, así como a las circulares y resoluciones de Farmaindustria y Autocontrol.

Igualmente, el presente documento contiene las funciones y obligaciones en materia de protección de datos de carácter personal que, de igual modo que el resto de las normas y procedimientos recogidos en el mismo, resultan de obligado cumplimiento por toda persona que acceda y trate datos de carácter personal respecto de los cuales ROVI resulte responsable de su tratamiento.

2. Definiciones

ROVI: significa todas las sociedades, corporaciones o entidades, que estén directa o indirectamente participadas por Laboratorios Farmacéuticos ROVI, S.A., ahora o en el futuro, cualquiera que sea el porcentaje de dicha participación. En la actualidad están incluidas las siguientes compañías, cuya lista se adaptará periódicamente:

- Laboratorios Farmacéuticos ROVI S.A.
- Laboratorios Farmacéuticos ROVI S.A. (Portugal)
- Gineladius S.L.
- Pan Química Farmacéutica S.A.
- ROVI Pharma Industrial Services, S.A.
- ROVI Escuzar S.L.
- ROVI Biotech S.R.L. (Italia)
- ROVI Biotech Limited (Reino Unido)
- ROVI Biotech Sp.z.o.o (Polonia)
- ROVI GmbH (Alemania)
- ROVI S.A.S. (Francia)

ROVI o Grupo ROVI se utiliza en singular como nombre propio y se refiere individual y conjuntamente a todas las sociedades relacionadas ut supra, así como a las que en el futuro pudieran pasar a formar parte del Grupo.

Recursos TIC: significa sistemas informáticos y telemáticos proporcionados por ROVI, incluyendo entre otros: hardware, software, red corporativa, correo electrónico, sistemas de comunicación y acceso a Internet.

Información Confidencial: se refiere a toda información científica, empresarial, comercial, financiera o de cualquier otra naturaleza que obre en poder de Empresas del Grupo ROVI o sea generada por Empleados y/o Colaboradores de Empresas del Grupo ROVI en el marco de la prestación de servicios o relación laboral que estos desarrollan para Empresas del Grupo ROVI, almacenada físicamente, en papel, en servidores propios y/o ajenos, en dispositivos electrónicos o en otros sistemas de almacenamiento y gestión de documentos electrónicos de su titularidad, siempre que esa información no sea públicamente accesible, divulgada o conocida. La información confidencial comprende correos electrónicos, archivos en papel, archivos electrónicos y de cualquier soporte.

Dato de carácter personal: cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Se considera dato personal tanto la información relativa a su identidad (como nombre y apellidos, domicilio, filiación, una fotografía o video, etc.) como la relativa a su existencia y ocupaciones (estudios, trabajo, enfermedades, afiliación política o sindical, orientación sexual, etc.).

También constituyen datos personales aquellas informaciones que recopiladas pueden llevar a la identificación de una persona física.
Datos especialmente protegidos: se refiere a datos personales que revelen el origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, así como el tratamiento de datos genéticos, biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud, vida sexual u orientaciones sexuales de una persona física.
Descargar: significa el proceso de almacenar, copiar o transferir archivos de una fuente o servicio de Internet a los recursos TIC o a la red de ROVI, e incluye los archivos adjuntos a mensajes de correo electrónico.
Responsable de Seguridad IT: miembro del departamento de IT designado como responsable de seguridad IT del Grupo Rovi, o de cada de las sociedades del Grupo Rovi, según corresponda en cada caso.
Protocolo sobre el Uso y Manejo de la Información Confidencial, del Grupo Rovi: protocolo que regula el manejo del a información confidencial en el grupo Rovi y las medidas de seguridad aplicables.
Documento de Seguridad de ROVI: Documento aprobado por ROVI que regula el tratamiento de datos de carácter personal, así como las medidas de seguridad que deben ser aplicadas y respetadas en todo tratamiento.
Responsable de Seguridad de la Información Confidencial: persona responsable de la gestión de riesgos de fuga o manipulación de información confidencial.

3. Objetivo de la Política

Esta Política ha sido elaborada con el objetivo de disponer de un documento en el que se establezcan las obligaciones de los usuarios en materia de seguridad y uso de los recursos TIC, teniendo en cuenta la normativa de Protección de Datos de Carácter Personal, la ciberseguridad, el artículo 20 del Estatuto de los Trabajadores de los sistemas informáticos y las obligaciones de control establecidas en el artículo 31 bis del Código Penal español.

Es objetivo de esta Política:

a) Cumplir el marco normativo sectorial.
b) Cumplir el Código de Buenas Prácticas de la Industria Farmacéutica.
c) Cumplir el Convenio General para la Industria Química.
d) Cumplir el Reglamento (UE) 2016/679 de 27 de abril de 2016 (en adelante, RGPD).
e) Aplicar al uso de los recursos tecnológicos de ROVI las funciones de vigilancia y control establecidas en el artículo 20.3 del Estatuto de los Trabajadores.
f) Garantizar la seguridad del sistema.
g) Proteger los datos personales que en él se encuentren.
h) Proteger la intimidad y la dignidad de los trabajadores, así como el resultado de su trabajo.
i) Proteger la información confidencial de ROVI o de sus clientes.
j) Proteger los activos intangibles de ROVI.
k) Proteger los recursos tecnológicos de ROVI.
l) Garantizar la continuidad del trabajo en caso de ausencia o baja del trabajador.
m) Prevenir supuestos de responsabilidad civil o penal frente a terceros.
n) Prevenir eventuales acciones judiciales.
o) Comprobar el cumplimiento de las obligaciones del trabajador.
p) Crear pruebas de cualquier infracción producida utilizando los recursos TIC de ROVI.
q) Prevenir la saturación de la red corporativa por exceso de tráfico.
r) Prevenir la saturación de los servidores por exceso de información.

4. Ámbito de aplicación

La presente Política es de aplicación a toda persona que trabaje o colabore con ROVI y que sea usuaria de los recursos TIC por el mero hecho de utilizarlos, en cualquier momento y

desde cualquier lugar. Asimismo, será de aplicación a cualquier persona que trate datos de carácter personal mediante los sistemas informáticos.

Por otra parte, también se aplicará al personal que, sin mantener un vínculo laboral con ROVI, realice funciones de gestión y mantenimiento de los sistemas de información.
De este modo, la presente Política, será aplicable a:

4.1.- Personas físicas: Esta Política es aplicable a los directivos, trabajadores, y demás personas autorizadas por la empresa, que incluyen el personal de los proveedores, encargados del tratamiento, profesionales externos y subcontratistas que tengan acceso a los recursos TIC de ROVI.
4.2.- Personas jurídicas: Esta Política es aplicable a todas las sociedades a través de las cuales la empresa desarrolla su actividad, así como los proveedores, encargados de tratamiento, profesionales externos y subcontratistas que tengan acceso a los recursos TIC de ROVI.
4.3.- Excepciones: De forma temporal o continuada el Responsable de Seguridad IT podrá establecer excepciones a la aplicación de algunos puntos de esta Política en función del cargo o la función desempeñados. También podrán cursarse autorizaciones temporales para el desarrollo de actividades que exijan un nivel de seguridad distinto al previsto en esta Política.

5. Alcance material
El alcance material de esta Política se extiende, a modo orientativo y no limitativo, a las siguientes áreas:

- Servidores.
- Ordenadores fijos y portátiles.
- Teléfonos fijos, móviles y smartphones.
- PC tablets.
- Discos duros externos y memorias flash/USB (pendrives).
- Programas informáticos.
- Aplicaciones para móviles.
- Dispositivos periféricos.
- Impresoras y escáneres.
- Grabadores/lectores de soportes digitales.
- Conexiones, redes (intranets y extranets) e Internet.

Así como cualquier otro recurso informático y/o de comunicación que sea facilitado por ROVI a los trabajadores.

6. Activos protegidos
Los activos protegidos por esta Política son, principalmente, los siguientes:

- Activos intangibles, incluyendo propiedad intelectual e industrial.
- Reputación de ROVI y de sus profesionales en el mercado.
- Información confidencial propia o de clientes.
- Información sobre la estructura organizativa de la Empresa, planes estratégicos y productos, incluyendo la identidad de proveedores y clientes y las condiciones contractuales aplicadas a unos y otros.
- Máximo rendimiento y el pleno acceso a los sistemas o recursos TIC de ROVI.
- Ingresos de ROVI.
- Datos personales de trabajadores, clientes, clientes potenciales y proveedores.
- Pruebas electrónicas generadas con el uso de los recursos TIC de ROVI.
- Cualquier otro activo tangible o intangible relacionado con los recursos TIC de ROVI.

7. Vigencia y actualización de la Política

En el transcurso de su relación con la empresa, todos los directivos, trabajadores y demás personas autorizadas tienen la obligación de cumplir esta Política y deben mantenerse al corriente y acatar cualquier modificación de la misma.

El incumplimiento de esta Política puede ocasionar una acción disciplinaria e incluso el despido o la resolución contractual. En el caso de la comisión de una acción ilícita, se procederá a su comunicación a las autoridades competentes o al inicio de las acciones legales que en Derecho correspondan.

La empresa se reserva el derecho a actualizar y modificar esta Política de acuerdo con los cambios legislativos, la evolución de los sistemas, de los procesos asociados y de la seguridad relacionada con los recursos TIC. Las actualizaciones y modificaciones de esta Política serán debidamente puestas en conocimiento de los directivos, trabajadores y personas autorizadas, e informadas previamente a la Representación legal de los Trabajadores.

8. Cuentas de usuario y uso de contraseñas

El identificador y clave de usuario de cada trabajador para acceder a la red de ROVI son privados y personales. El usuario no podrá comunicar ni compartir con otra persona el identificador de usuario y/o la clave de acceso a cualquier sistema o servicio.

Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del Responsable de Seguridad IT, y crear una nueva clave.

En la gestión y uso de las contraseñas deben seguirse las siguientes pautas:

- La contraseña debe tener una extensión mínima de doce caracteres, y deben resultar de una combinación de, al menos, letras (mayúsculas y minúsculas) y números.
- Debe ser complicado intuir las contraseñas.
- No deben utilizarse palabras comunes, meses, fechas de aniversario, matrículas de coche, etc.
- Deben crearse nuevas contraseñas y evitar reutilizar las contraseñas antiguas.
- Hay que cambiar las contraseñas regularmente, y al menos cada tres meses.
- Al recibir soporte técnico, los usuarios tendrán que introducir personalmente todas las contraseñas.
- No se debe facilitar la contraseña a los empleados de servicios externos de asistencia técnica.
- No se deben conservar las contraseñas en papel ni a la vista.

El usuario autorizado para realizar teletrabajo deberá aplicar medidas adicionales de seguridad en el lugar donde se encuentre ubicado el equipo, para garantizar un nivel de confidencialidad similar al de las oficinas de la empresa.

Las mismas cautelas deberán aplicar los usuarios que accedan a los servidores de ROVI a través de la VPN o de cualquier otro sistema de conexión remota, ya que durante la conexión se incrementa el nivel de vulnerabilidad del sistema.

Si fuera necesario acceder a los equipos, cuentas de correo electrónico, y demás recursos TIC asignados a un trabajador por encontrarse éste en situación de baja laboral, excedencia, ausencia temporal, vacaciones o baja definitiva, por resultar necesario para garantizar el cumplimiento de las funciones laborales o para dar respuesta a necesidades del negocio; el Responsable del Departamento podrá llevar a cabo alguna de las siguientes acciones:

- Solicitar al trabajador ausente o al administrador de sistemas la configuración de un mensaje de respuesta automática en el correo electrónico comunicando los datos del trabajador que sustituya al trabajador ausente.
- Solicitar al administrador de sistemas el desvío de los mensajes entrantes hacia la cuenta de correo electrónico del trabajador que sustituya al trabajador ausente.
- Solicitar al Responsable de Seguridad IT la creación de una clave temporal que permita el acceso a los documentos de trabajo, al ordenador, directorios del servidor y al correo

electrónico del trabajador ausente. El uso de esta clave se limitará a garantizar la continuidad del trabajo iniciado por el trabajador ausente. Cuando el trabajador se reincorpore, la clave temporal deberá ser anulada.
- Solicitar al Responsable de Seguridad IT proceder con la destrucción de la documentación crítica de ROVI, cumpliendo con lo dispuesto en el apartado 15 del presente documento, para cumplir con los plazos de conservación y eliminación de documentación crítica y/o confidencial. La información a destruir debe ser indicada por el responsable del trabajador.

El Responsable de Seguridad IT, junto con el Responsable del Departamento, y en su caso con la asistencia del Responsable de Cumplimiento, valorará la medida a adoptar en cada caso de entre las alternativas arriba recogidas. En la adopción de la medida deberá seguirse lo establecido en el procedimiento SOPc106 “Protocolo de actuación en relación con el uso de los recursos TIC en caso de ausencia temporal o definitiva del trabajador” (versión en vigor).

La clave de acceso de las personas que causen baja definitiva de la empresa será eliminada el mismo día que sea efectiva la baja (deshabilitando el usuario). La empresa podrá desviar los mensajes enviados a la dirección de correo electrónico del empleado que cause baja a otros compañeros del mismo departamento, previa solicitud del Responsable de Departamento mediante el protocolo antes mencionado.
En los supuestos en los que la Dirección de ROVI lo considere necesario, la cancelación de las claves podrá producirse antes de la fecha prevista para la baja efectiva.
El uso de los recursos TIC de ROVI por parte del trabajador supone la aceptación expresa de la posibilidad de acceder a sus documentos de trabajo, ordenador, directorios del servidor y correo electrónico por parte de las personas designadas para ello por la empresa con la finalidad de garantizar la continuidad del trabajo una vez extinguida su relación laboral con ROVI.

9. Actividades permitidas y actividades expresamente prohibidas
ROVI pone a disposición de sus empleados distintos recursos TIC con el objetivo de que éstos puedan desempeñar las funciones laborales que les han sido encomendadas. La asignación de los recursos TIC necesarios para cada empleado es realizada por el Departamento de IT, quien será el encargado de determinar qué recursos deben ser asignados en cada caso, ateniendo a las necesidades del puesto de trabajo.
Los recursos TIC deben ser utilizados única y exclusivamente para el desempeño de las funciones laborales encomendadas por ROVI. Todos los trabajadores están obligados a utilizar únicamente los recursos TIC puestos a disposición por ROVI para el desempeño de sus funciones, estando prohibido el uso de recursos TIC personales para el desarrollo de la prestación de servicios laborales. Adicionalmente, y por medidas de seguridad todos los trabajadores del Grupo ROVI deberán trabajar en red, estando prohibido trabajar, grabar o almacenar cualquier documento y/o información relacionada con la actividad que el trabajador desarrolla para ROVI en el disco duro del ordenador. De igual modo, queda expresamente prohibido almacenar cualquier información personal del trabajador en red.

Como norma, ROVI prohíbe hacer un uso personal de los recursos TIC, no obstante, los empleados están autorizados para hacer un pequeño uso personal de las herramientas informáticas de la empresa fuera del horario laboral respetando el marco legal vigente y siempre y cuando se cumplan las siguientes condiciones:

- El uso realizado no puede contravenir los intereses de la Compañía y debe respetar en todos los casos la legalidad vigente y el Código Ético de Rovi; y en particular el uso personal que se haga de ellos debe respetar los derechos humanos, y la privacidad de las personas. El uso privado de los recursos TIC nunca puede alcanzar la información confidencial de ROVI ni los datos personales tratados por el Grupo Rovi.
- Debe tratarse de un uso no intensivo y ser consecuente con las limitaciones de capacidad de la red de ROVI.

- No puede contravenir ninguna de las prohibiciones expresas que se recogen más adelante en el presente epígrafe.

Los representantes de los trabajadores de empresas miembro del Grupo Rovi, en virtud de la representación otorgada por el colectivo de empleados, tienen autorización para utilizar los recursos TIC de la compañía para sus actividades sindicales y dentro de los límites que el marco legislativo en vigor establece en cuanto a tiempo de dedicación, alcance y contenido. Esta autorización incluye el envío de información del sindicato/comité de empresa/delegados de personal a todos los empleados usando los medios de comunicación electrónica a su disposición. Asimismo, los empleados tienen autorización para utilizar las herramientas informáticas de la empresa para comunicarse con los representantes de los trabajadores.
El usuario está obligado a utilizar los recursos TIC de ROVI y sus datos sin incurrir en actividades que puedan ser consideradas contrarias a la normativa vigente, a nuestras políticas, al Código Ético de Rovi, al Código de Buenas Prácticas de la Industria Farmacéutica, o bien infrinjan los derechos de ROVI, de otros trabajadores o de terceros.

Están expresamente prohibidas las siguientes actividades:

- Compartir o facilitar el identificador de usuario y la clave de acceso a los recursos TIC de ROVI a otra persona física o jurídica, incluido el personal de la propia empresa. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificador.
- Utilizar los usuarios y/o claves de otros usuarios.
- Trabajar con ficheros fuera del sistema de almacenamiento compartido en red de la compañía (queda prohibido trabajar en el disco duro local de la estación de trabajo).
- Manipular o intentar modificar los ficheros LOG que registran la actividad del usuario.
- Intentar obtener, descifrar o desactivar las claves y cualquier otro elemento de seguridad que intervenga en los procesos informáticos y telemáticos de ROVI.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de ROVI o de terceros. La prohibición se extiende a los ataques de denegación de servicio, a la difusión de virus o malware y a cualquier otra actividad de sabotaje de sistemas o potencialmente dañina.
- Introducir voluntariamente programas, virus, macros, applets, scripts, controles ActiveX o cualquier otro fichero o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de ROVI o de terceros.
- El usuario tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos, tanto de forma pasiva como activa analizando todos aquellos dispositivos externos de almacenamiento que se utilicen en cualquier estación de trabajo.
- Obstaculizar el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de ROVI, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de ROVI o de terceros.
- Intentar aumentar el nivel de privilegios propios o de otro usuario en el sistema.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la empresa, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias no autorizadas de cualquier programa, incluidos los estandarizados.
- Borrar cualquiera de los programas instalados legalmente.
- Introducir contenidos obscenos u ofensivos y, en general, carentes de utilidad para los objetivos de ROVI, en la red corporativa de ROVI.

- Instalar puntos de acceso y redes inalámbricas no autorizadas (WiFi, bluetooth o similares).
- Manipular cualquier elemento físico de la red de datos de las instalaciones de ROVI, incluida la conexión del propio puesto de trabajo.
- Desactivar el salvapantallas que protege con contraseña el acceso no autorizado al ordenador del usuario cuando éste está encendido y el usuario se ausenta temporalmente de su puesto de trabajo.
- Desactivar el firewall, el sistema antivirus y los demás elementos de seguridad que protegen individualmente los ordenadores personales, especialmente los portátiles.
- Crear ficheros de datos personales sin la autorización de ROVI, como Responsable del Fichero, o del Responsable del fichero en caso de ser este un tercero distinto a ROVI.
- Utilizar los recursos TIC de ROVI, para almacenar cualquier contenido personal, sea cual sea su procedencia y formato (fotografías, música, video, etc.).
- Salvo excepciones autorizadas por el Responsable de Seguridad IT queda prohibido el intercambio de ficheros y/o información de cualquier tipo a través de dispositivos USB o cualquier otro dispositivo de almacenamiento masivo con terceros.
- Utilizar sistemas de inteligencia artificial IA que no estén expresamente aprobados por ROVI, como puede ser ChatGTP.

El incumplimiento de cualquiera de las normas incluidas en la presente Política dará lugar a las acciones oportunas por parte de IT que pueden incluir el borrado de información, la desinstalación de programas, restricciones de uso, etc.
El uso por parte del trabajador de cualquiera de los recursos TIC de ROVI para la realización de actividades ilegales será responsabilidad personal del trabajador, sin perjuicio de las posibles acciones que ROVI pueda adoptar de acuerdo con la legislación penal, civil y laboral vigente en cada momento.

10. Seguridad de la Información Confidencial

- El usuario debe respetar las instrucciones relativas al uso de información confidencial recogidas en el procedimiento SOPc103 (versión en vigor) del Grupo Rovi de obligado conocimiento.
- El incumplimiento de la obligación de preservar la confidencialidad puede constituir un delito de conformidad con lo previsto en los artículos 197, 199, 279 y 280, entre otros, del Código Penal y dará derecho a la empresa a exigir al usuario una indemnización económica.
- Sólo las personas autorizadas directamente por la Dirección General de ROVI podrán atender a encuestadores y cumplimentar cuestionarios en los que se solicite cualquier tipo de información relativa a la empresa.
- Queda prohibida la instalación de programas descargados de Internet u obtenidos de cualquier otra fuente no fiable por el riesgo de que pueda contener spyware o troyanos, es decir programas que permitan monitorizar de forma no autorizada la actividad del usuario y enviar al exterior de ROVI información confidencial.
- Para limitar al máximo el riesgo de pérdida de información confidencial, es obligatorio guardar los documentos informáticos en el servidor y no conservar ninguno en el disco duro de los ordenadores personales. Por el mismo motivo se prohíbe el uso de soportes, pen drive, discos duros portátiles, almacenamiento en la nube distinta de la corporativa y cualquier otro dispositivo móvil que pueda almacenar información. Sólo podrán utilizarse los dispositivos móviles de almacenamiento arriba descritos en la red de ROVI con el objeto de almacenar información confidencial que estén expresamente autorizados e inventariados por el Responsable de Seguridad IT y el Responsable de Seguridad de la Información Confidencial. La grabación de información confidencial en pendrives, discos duros portátiles, nube no corporativa o cualquier otro dispositivo móvil sin la autorización del Responsable de Seguridad IT y del Responsable de Seguridad de la Información Confidencial supondrá una infracción grave de lo

establecido en la presente Política, en el Documento de Seguridad y en el procedimiento SOPc103 (versión en vigor), del Grupo Rovi.

- La compañía se reserva la facultad de requerir a los empleados la destrucción de documentación que contengan información de carácter confidencial o restringido, así como de carácter privado, personal u ofensivo.

- La compañía procede con la destrucción automática de correos electrónicos que hayan sido conservados por un periodo superior de dos años por parte de los usuarios.

11. Uso del correo electrónico

La red corporativa, los ordenadores personales y los sistemas informáticos utilizados por cada usuario son propiedad de ROVI.

El correo electrónico constituye una herramienta de trabajo y su uso debe limitarse a la transmisión y recepción de los contenidos propios de la prestación laboral. Ningún mensaje de correo electrónico será considerado como privado o personal, salvo aquellos que contengan información personal propiedad del empleado fruto de la relación laboral con el Grupo ROVI.

Se considerará correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas, y, especialmente, Internet.

Todos estos mensajes y sus ficheros adjuntos irán abiertos, con excepción de aquéllos que contengan datos personales especialmente protegidos, constituyan información confidencial de acuerdo con el procedimiento SOPc103 (versión en vigor) del Grupo Rovi o que, por cuestiones de seguridad, deban ir cifrados. Para cifrar dichos correos electrónicos será necesario incluir la información a intercambiar en un fichero comprimido con contraseña. Esta contraseña debe ser intercambiada por un medio distinto al utilizado para enviar el fichero comprimido (al menos debe ser enviada en todo caso a través de un correo electrónico independiente sin asunto y solicitando su inmediata destrucción por parte del destinatario).

La empresa se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de esta Política y prevenir actividades que puedan afectar a la empresa como responsable civil subsidiario.

Esta revisión dirigida sólo podrá llevarse a cabo cuando exista una sospecha razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de esta Política que comprometa la seguridad del sistema, o un uso indebido con fines distintos a los propios del contenido de la relación laboral.

El trabajador tampoco podrá acceder, leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin previa autorización. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).

Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en esta Política y, en especial, las referidas a propiedad intelectual e industrial, control de virus, phishing y pharming.

La transmisión de datos de carácter personal especialmente protegidos (como los datos de salud), a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

ROVI prohíbe expresamente el reenvío de mensajes y documentos corporativos a cuentas privadas del trabajador o de sus familiares o amigos (salvo aquellos que contengan información personal propiedad del empleado fruto de la relación laboral con el Grupo ROVI). De igual modo, queda expresamente prohibido configurar la cuenta de correo corporativo para reenviar los mensajes recibidos a una cuenta de correo electrónico privada.

Así mismo, queda prohibida la creación de copias, totales o parciales, del buzón de correo en local en unidades de red o cualquier otra ubicación distinta al servidor de correo en formato PST o cualquier otro formato que permita la descarga masiva de correos localmente.

Para garantizar el uso eficiente de los recursos TIC no deberá utilizarse el correo electrónico para transmitir o enviar:

- Contenidos que infrinjan las normas de Copyright o de Propiedad Intelectual.
- Ficheros adjuntos (attachments) con juegos, música, imágenes, vídeo o cualquier material que no esté relacionado con el trabajo.
- Que atenten contra los derechos de terceras personas, o de la propia organización.
- Mensajes difamatorios, obscenos, inapropiados, fraudulentos, amenazantes o de cualquier otra naturaleza que pudieran incurrir en conductas ilegales o contrarias a nuestro Código Ético.
- Mensajes de correo en cadena o de tipo piramidal (chain letters).
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento expreso del destinatario (Spam).

En caso de que una persona cause baja de la empresa, se mantendrá durante un periodo máximo de dos meses su buzón de correo, en previsión de las necesidades del servicio o departamento al que estaba adscrito o por motivos legales. Transcurridos los dos meses se eliminará el buzón junto con todo su contenido. Para el acceso al buzón de correo del usuario que causa baja se debe seguir lo pautado en el procedimiento SOPc106 (versión en vigor).

El correo electrónico puede utilizarse ocasionalmente y fuera del horario laboral con propósitos personales siempre y cuando:

- No implique una inversión de tiempo importante.
- No pueda dañar los equipos.
- No tenga como objetivo el lucro personal.
- No se trate de envíos masivos.
- No se trate de mensajes en cadena o de tipo piramidal.
- No se envíen contenidos expresamente prohibidos en este documento o contrarios al Código Ético de Rovi.

12. Acceso a Internet

El uso del sistema informático de ROVI para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de ROVI y los cometidos del puesto de trabajo del usuario, salvo en el caso de que se cuente con autorización expresa para ello.

El acceso a debates en tiempo real (Chat-IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido. Igualmente está prohibido el uso de sistemas de mensajería instantánea como el Messenger, Skype personal o WhatsApp para PC, el uso de plataformas de inteligencia artificial en internet (cualquiera que sea su propósito) y la instalación de programas que permitan el acceso a redes P2P (Peer to Peer), así como cualquier otro tipo de acceso a entornos o plataformas que permitan el intercambio de ficheros sin la previa autorización del Responsable de Seguridad IT. Este tipo de programas pueden ayudar a superar los sistemas de defensa ante accesos no autorizados y son un canal de entrada de virus y troyanos.

El acceso a páginas web (www), grupos de noticias (Newsgroups) y otras fuentes de información y utilidades como FTP, etc. se limita a aquéllos que contengan información relacionada con la actividad de ROVI o con los cometidos del puesto de trabajo del usuario, salvo en el caso de que se cuente con autorización expresa para ello. La empresa podrá establecer filtros para garantizar el cumplimiento de esta obligación.

Si un usuario precisa estas herramientas para un uso profesional justificado, deberá solicitar que se habilite técnicamente un acceso temporal a Internet para poder utilizarlas, con excepción de los programas P2P, que no podrán ser utilizados en ningún caso, debido a su especial riesgo.

La empresa se reserva el derecho de monitorizar y comprobar, sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa. Esta revisión dirigida sólo podrá llevarse a cabo cuando exista una sospecha razonable de la comisión de un delito, una infracción administrativa o un incumplimiento grave de esta Política que comprometa la seguridad del sistema, de cualquier otra política de ROVI o del Código Ético de Rovi.
Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en esta Política y, en especial, las referidas a propiedad intelectual e industrial, control de virus, phishing y pharming.

13. ROVI en el entorno digital

Ningún trabajador no autorizado puede promocionar en modo alguno medicamentos, compartir información o consejos profesionales en nombre propio como miembro o en nombre de ROVI en plataformas, e-commerce, redes sociales u otros “entornos digitales”, de conformidad con lo previsto en el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, en el Real Decreto 1416/1994, de 25 de junio, por el que se regula la Publicidad de los Medicamentos de Uso Humano o en el Código de Buenas Prácticas de la Industria Farmacéutica, entre otros. A título enunciativo, que no limitativo, se entiende por “entorno digital”: SMS, MMS, páginas web, correo electrónico, foros, blogs, redes sociales, chats, plataformas, aplicaciones o cualquier otro tipo de canal, soporte o medio digital.
Cualquier comunicación realizada en nombre del Grupo Rovi debe respetar lo establecido en el Código Ético de Rovi y deberá ser canalizada a través del Departamento de Comunicación o el Departamento de Relación con Inversores según corresponda.

14. Control y monitorización de los recursos TIC y de las comunicaciones electrónicas

La empresa vigilará el cumplimiento de esta Política de forma constante, registrando la actividad de la red corporativa, diseñando y revisando estadísticas y patrones de uso y efectuando rastreos ocasionales del uso de Internet y del tráfico de correos electrónicos con el fin de evitar cualquier perjuicio derivado del incumplimiento de la presente Política. También podrá proceder a la revisión y monitorización de los recursos TIC de ROVI, con la misma finalidad.
La empresa puede comprobar en cualquier momento el uso que los empleados hacen de los recursos TIC puestos a su disposición y las comunicaciones electrónicas generadas a través de dichos recursos. Esto incluirá, aunque sin restringirse sólo a ello, el acceso y revisión de los contenidos de los servidores, cuentas de correo electrónico, discos duros, mensajes de texto, el sistema de telefonía, buzón de voz y registros de telefonía móvil.
Con los fines citados, el control puede incluir, de forma no limitativa, la monitorización y registro de:

- Navegación web: Navegación por la web utilizando los servicios y sistemas de ROVI, incluida la URL (dirección web) a la que se accede, fecha, hora, duración del acceso, páginas visitadas y/o descargadas.
- E-mail: Cualquier mensaje (incluidos ficheros adjuntos) enviados o recibidos por o en los equipos de ROVI. Los mensajes (incluidos ficheros adjuntos) enviados o recibidos pueden ser bloqueados a discreción del administrador del sistema cuando se considere que son demasiado grandes, o que pueden ser un mensaje de tipo spam u otro tipo de correo dañino que puedan interferir el funcionamiento de la red informática o que puedan ser considerados como amenazantes, molestos u ofensivos.
- Almacenamiento: Cualquier almacenamiento digital propiedad de ROVI que contenga ficheros, independientemente de su tipo o naturaleza, que puedan ser creados o modificados por los usuarios de estos recursos. No se excluye el área reservada a los Administradores de la Red. Se revisará su contenido en busca de ficheros que incumplan las normas descritas en esta Política, así como la cantidad de recursos del que hace uso cada uno de los usuarios.
- Uso de la información confidencial y cumplimiento de lo establecido en el procedimiento SOPc103 (versión en vigor).

A continuación, se relacionan algunos de los controles que de forma continuada, puntual o excepcional pueden ser aplicados a los recursos TIC de ROVI, sin perjuicio de cualesquiera otros que pudieran reputarse necesarios según los casos:

- Control del contenido de los mensajes de correo electrónico.
- Control de remitentes y destinatarios de los mensajes de correo electrónico.
- Control del contenido del ordenador del trabajador.
- Control de las áreas privadas del servidor.
- Control de los logs y estadísticas de uso.
- Conservación de los logs durante un plazo determinado.
- Control del historial de navegación.
- Control de los patrones estadísticos de uso de los recursos informáticos.
- Cámaras de videovigilancia.
- Registro de llamadas.
- Acceso a documentos de trabajo en caso de ausencia o baja del trabajador.
- Acceso al buzón de e-mail en caso de ausencia o baja del trabajador.
- Control especial previo y posterior al despido.
- Control especial previo y posterior a la baja voluntaria.
- Medidas de seguridad y controles relativos a la protección de datos personales.
- Bloqueo de acceso a páginas web no autorizadas.
- Control del firewall.
- Control del Proxy.
- Herramientas de monitorización del sistema.
- Herramientas de creación de pistas de auditoría y evidencias.
- Servicio externo de forensic readyness.
- Perfiles estadísticos y patrones de conducta individualizados.
- Mensaje mensual con estadísticas individuales de consumo de recursos.
- Configuración de alertas ante patrones de uso o cambios sospechosos.
- Comprobación periódica del funcionamiento de las medidas de control.
- Análisis de riesgo en caso de salida de empleados conforme al procedimiento SOPc106 (versión en vigor).
- Otros controles.

Todas estas actuaciones se realizarán cumpliendo con la normativa aplicable en cada momento, y con el máximo respeto a la dignidad del trabajador, de acuerdo con las facultades de vigilancia y control establecidas en el artículo 20.3 del Estatuto de los Trabajadores. Los controles automatizados se realizarán de forma continuada y sin restricciones. Los registros efectuados de forma manual sólo podrán llevarse a cabo cuando exista una sospecha razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento de las políticas y procedimientos de ROVI o de su Código Ético que pueda comprometer la seguridad del sistema, o que pueda comportar riesgos o perjuicios para los activos protegidos descritos en esta Política.

El trabajador da su consentimiento expreso para que la empresa pueda acceder al contenido de su cuenta de correo electrónico, documentos de trabajo, historial de navegación por Internet, logs, contenido del disco duro y del servidor y a cualquier otra área pública o privada de los recursos TIC de la compañía, en los supuestos, con el alcance y con las finalidades descritos en esta Política.

A estos efectos, la empresa dispone de los protocolos y procedimientos de actuación necesarios para asegurar que el acceso a la información no vulnerará, en ningún momento, la dignidad del usuario afectado por el control.

Del mismo modo, si los administradores de la red detectan un incumplimiento de esta Política deberán comunicarlo al Responsable de Seguridad IT y al Responsable de Cumplimiento para que le den el curso apropiado.

La empresa colaborará con las fuerzas y cuerpos de seguridad del Estado, informando o contestando a sus requerimientos de información sobre cualquier circunstancia que pueda ayudar a la investigación de un delito, una falta o una infracción administrativa.

La utilización de los recursos TIC de ROVI presupone el conocimiento y la aceptación de la presente Política. A tal fin, los trabajadores que utilicen los recursos TIC deberán realizar la formación vigente en cada momento relativa a la presente Política y firmar el documento (en papel o digital, a través de la forma que determine ROVI en cada momento) que figura como **Anexo A** para acusar aceptación y compromiso de cumplimiento de la presente Política (este tipo de reconocimiento se aplicará para las nuevas incorporaciones de ROVI).
Esta Política deberá ser leída y comprendida por todos los trabajadores de ROVI que utilizan los recursos TIC. El departamento responsable deberá adoptar las medidas oportunas para asegurar que esta Política se entregue a todos los nuevos trabajadores y los mecanismos adecuados para recordar periódicamente sus contenidos a todos los trabajadores que utilicen los recursos TIC.

15. Plazos de conservación y eliminación de documentación crítica y/o confidencial

Todo el personal debe utilizar mecanismos seguros a la hora de destruir documentación crítica para ROVI. Se considera documentación crítica aquella que contiene información confidencial o datos de carácter personal, o documentación calificada como restringida.
Los trabajadores que hayan tenido acceso a documentación crítica deberán destruir cualquier soporte que contenga esta información en el momento en el que haya dejado de ser útil, salvo que exista algún requisito legal o de negocio, que justifique su conservación. En este sentido, se deberá tener en cuenta no solo que han de destruirse versiones definitivas de los documentos críticos, sino también todos los borradores, copias, extractos y demás documentos de trabajo que contengan información crítica.
Los trabajadores tienen que hacer uso de destructoras de papel para eliminar documentación crítica en papel y que sea obsoleta. Las destructoras deben estar situadas en zonas accesibles para los empleados. Queda prohibido arrojar documentos con información sensible de la empresa a papeleras.
Asimismo, los trabajadores tienen el deber de eliminar cualquier correo electrónico y documentos en formato digital tan pronto como su conservación no sea exigible legalmente o estrictamente necesaria para ROVI desde un punto de vista de negocio.
En caso de recibir una notificación para la destrucción de documentación corporativa por parte de ROVI, deberá proceder de acuerdo con las instrucciones recibidas en el plazo previsto y conforme lo dispuesto en la presente Política.
Asimismo, en caso de ausencia del trabajador, deberá ser el administrador de sistemas, esto es, el Departamento de IT, quien proceda, en nombre del trabajador, con el cumplimiento de las instrucciones previstas en el presente apartado, con tal de cumplir con los plazos de conservación y eliminación de documentación general, crítica y/o confidencial de ROVI.
Mención especial merece la información contenida en el Sistema de Correo electrónico: Este sistema no está concebido para el almacenamiento de información, sino como una herramienta de comunicación, por este motivo se define que el plazo máximo de almacenamiento para el correo electrónico será de 2 años, por lo que transcurrido dicho plazo máximo el sistema eliminará los correos que superen este límite temporal, así como sus adjuntos, de forma automática. No obstante, la dirección de la compañía, junto con el Responsable de Seguridad IT, Responsable de Seguridad de la Información Confidencial y el Responsable de Cumplimiento, podrán definir plazos de almacenamiento diferentes para aquellos departamentos o buzones de correo que así lo justifiquen.

16. Propiedad intelectual e industrial

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.
La empresa tiene una lista de aplicaciones informáticas y sistemas operativos, autorizados y licenciados para su instalación, ejecución y uso en los ordenadores y demás recursos TIC por parte de los trabajadores y personas autorizadas. Únicamente se deben utilizar estas aplicaciones y sistemas operativos.
El software licenciado a favor de ROVI no puede ser instalado ni utilizado en ordenadores o dispositivos que no sean propiedad de ROVI. Es decir, no se permite copiar software licenciado

a favor de ROVI en dispositivos informáticos personales, aunque el software vaya a emplearse para la actividad de ROVI.
No deben emplearse los recursos TIC de ROVI para descargar, copiar, alterar, modificar, mezclar o manipular ningún medio electrónico, datos o software que pudiera contravenir la legislación sobre derechos de la propiedad intelectual. La carga, descarga e intercambios no autorizados de software, música, cine y cualquier otro contenido digital a través de plataformas P2P (Peer to Peer) o cualquier otro medio de transmisión de datos a través de Internet constituye un delito contra la propiedad intelectual, por lo que el usuario no podrá realizar ninguno de dichos actos.
Deben respetarse los acuerdos y licencias de propiedad intelectual e industrial que la empresa tenga con terceros.

17. Protección de datos

Es obligación de todo el personal que acceda a datos personales en soporte informático, en papel o en cualquier otro soporte, respetar la normativa aplicable en esta materia, manteniendo la máxima confidencialidad sobre dichos datos y aplicando las medidas de seguridad establecidas en esta Política, en el Documento de Seguridad de ROVI y en las restantes políticas aprobadas por ROVI para proteger la seguridad de los datos personales que tratamos.
No podrán crearse ficheros o nuevos tratamientos de datos personales sin la autorización del Responsable de Cumplimiento, que es quien ostenta la responsabilidad en materia de protección de datos en el Grupo Rovi.
Los datos personales titularidad de ROVI tan solo podrán ser tratados de conformidad con las finalidades previstas y respetando siempre y en todo caso lo establecido en el Documento de Seguridad.
No se podrá cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del Responsable de Cumplimiento y el Delegado de Protección de Datos (DPO).
No podrá realizarse cualquier otra actividad expresamente prohibida en esta Política o en las normas sobre protección de datos e Instrucciones de la Agencia de protección de Datos.
Deberán cumplirse las medidas de seguridad establecidas para el tratamiento y la conservación de datos personales de forma automatizada o no automatizada, en soporte informático o en papel, de acuerdo con el análisis de riesgo e impacto en la privacidad que haya efectuado la compañía, y bajo la supervisión y conocimiento del DPO.

18. Soportes de información

El Departamento de IT de ROVI pone a disposición de los usuarios una serie de carpetas compartidas, con los permisos de seguridad adecuados, otorgados por el responsable de los datos contenidos en cada una de ellas, y configurados por los Administradores de la red. Como norma general ROVI prohíbe el almacenamiento de su información y/o documentación, ya sea confidencial o no, en dispositivos de almacenamiento de información distintos a éstos. Excepcionalmente y por motivos laborales se podrá solicitar al Responsable de Seguridad IT autorización para almacenar información y/o documentación en dispositivos de almacenamiento distintos a los previamente homologados por la empresa.
Dicha autorización deberá ser solicitada adicionalmente al Responsable de Seguridad de la Información Confidencial, si el carácter de la información es confidencial.
Cualquier soporte de información, informática, digital, en papel o de cualquier otro tipo, que un trabajador localice en las instalaciones de ROVI o en sus inmediaciones que tenga la apariencia de haber sido extraviado, será entregado de forma inmediata al Responsable de Seguridad IT según lo indicado en el apartado 19. Incidencias, de la presente Política.
Los portátiles y todos los dispositivos móviles en general no deben guardarse ni siquiera de forma temporal en un coche o en un lugar de acceso público.
Debe informarse de inmediato sobre cualquier robo, pérdida de hardware o documentación en cualquier formato. En caso de robo o pérdida de un ordenador o cualquier otro dispositivo móvil, debe notificarse inmediatamente al Responsable de Seguridad IT, según lo indicado en el apartado 19. Incidencias, de la presente Política.

Al finalizar la relación laboral o de cualquier otra índole con la empresa, se deberán devolver todos los recursos TIC que hayan sido asignados en el transcurso de la relación con la empresa. Estos dispositivos deben ser devueltos en buen estado, con todos los periféricos y sin borrar o formatear.

19. Incidencias

Se entiende por incidencia cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, por ejemplo, la pérdida de datos de forma accidental, la sospecha de intrusión en la red corporativa, el deterioro de cintas de soporte, etc.

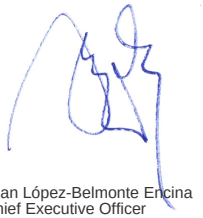
Es obligación de todo el personal de ROVI comunicar al Responsable de Seguridad IT y al Responsable de Cumplimiento cualquier incidencia que se produzca en los sistemas de información a los que tengan acceso, o que, sin tenerlo, puedan observar externamente.

Dicha comunicación deberá realizarse inmediatamente y, en cualquier caso, en un plazo de tiempo no superior a una hora desde el momento en que se conozca la misma, mediante correo electrónico a la dirección de correo de seguridad de TIC habilitada a tal efecto: seguridadit@rovi.es.

20. Sanciones

El incumplimiento de la presente Política podrá comportar responsabilidades personales de tipo penal, civil y/o laboral para el trabajador y además constituir una infracción grave a los efectos previstos en el Estatuto de los Trabajadores y el Convenio General para la Industria Química y Farmacéutica en vigor.

En cualquier caso, la presente Política no establece las medidas sancionadoras de forma expresa, dejando al criterio de ROVI y de los órganos legales competentes la aplicación de cualquier tipo de medida sancionadora derivada de su incumplimiento.



Juan López-Belmonte Encina
Chief Executive Officer
2024-05-21T15:29:46

Juan López-Belmonte Encina
Presidente

ANEXO A
Aceptación del Trabajador

Reconozco que he recibido la información relativa a la Política de uso de los recursos TIC facilitada por ROVI a los trabajadores (en adelante, la "Política").

Entiendo los términos y condiciones de la misma correctamente, no tengo dudas sobre los usos permitidos y prohibidos de los recursos TIC y me comprometo a respetarlos.

He sido informado de que ROVI vigilará el cumplimiento de esta Política de forma constante, registrando la actividad de la red corporativa, diseñando y revisando estadísticas y patrones de uso y efectuando rastreos ocasionales del uso de Internet y del tráfico de correos electrónicos con el fin de evitar cualquier perjuicio derivado del incumplimiento de esta Política.

Asimismo, cuando exista una sospecha razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de las políticas y procedimientos de ROVI, incluido el Código Ético, que pueda perjudicar a la actividad de ROVI, a sus activos, o pueda comprometer la seguridad del sistema, ROVI podrá;

- Registrar:

  (i) la dirección de correo electrónico por la que envío y recibo mensajes,
  (ii) la navegación en internet del usuario,
  (iii) cualquier actividad en la red en la cual transmita o reciba cualquier documento,
  (iv) cualquier fichero creado, modificado, copiado, transmitido o eliminado de cualquier sistema de almacenamiento de Rovi.

- Acceder y/o registrar el contenido de cualquier documento, incluido ficheros adjuntos y mensajes de correo electrónico, creado, modificado, copiado, borrado, enviado y/o transmitido con o a través de los recursos TIC de ROVI.

Quedo igualmente informado de que la revisión y utilización de dicha información se realizará por la dirección de ROVI a los efectos legales correspondientes.

Entiendo que cualquier violación de esta Política puede constituir una infracción grave que dará lugar a las acciones que se reputen oportunas en cada caso desde el punto técnico y legal, y que podría comportar sanciones disciplinarias de acuerdo con el Estatuto de Trabajadores y el Convenio General para la Industria Química en vigor.

En [ ], a [ ] de [ ] de [ ].

_____
[Nombre del Trabajador]

ANEXO B

Requerimiento excepcional para la destrucción de documentación

Por la presente, le informamos que en el plazo de (indicar plazo) días, deberá proceder a la destrucción de la documentación que a continuación se detallan, todo ello sin perjuicio de su obligación de cumplir con los plazos de destrucción de información contenidos en el apartado 15 de la Política de Uso de los Recursos TIC, y demás requisitos allí detallados.

- XXXXX
- XXXXX

La documentación arriba referenciada, deberá ser destruida conforme las instrucciones establecidas en la Política de Uso de los Recursos TIC de ROVI, y más concretamente, siguiendo lo dispuesto en el apartado 15 de las mismas.

En caso de no atender a la presente notificación, entenderemos que incurre en una violación de la Política de Uso de los Recursos TIC y, por tanto, cometer una infracción grave que podría comportar sanciones disciplinarias de acuerdo con el Estatuto de Trabajadores y el Convenio General para la Industria Química en vigor.

En [ ], a [ ] de [ ] de [ ].

_____

Grupo Rovi