POLÍTICA DE SISTEMAS DE INFORMACION DE TECUNI S.A.

5 de septiembre de 2018

Tamara Yagüe Martínez
DIRECTORA GENERAL

CONTENIDO

1 OBJETO, ALCANCE Y VIGENCIA

Se pretende establecer una serie de principios básicos que regulen el marco de las comunicaciones y sistemas de información dentro del seno de la empresa y su actividad profesional, por lo que el uso de los mencionados recursos y sistemas deberá realizarse conforme a la presente Política y las prescripciones y recomendaciones del responsable de la licencia.

La presente Política complementa las directrices establecidas por el Grupo VINCI recogidas en su intranet en los siguientes documentos:

- Guidelines for the proper use of IT resources
- Guide for users
- Charter for administrators
- SPMIS Security practices and measures for information systems

Es por ello que se implementa en su seno la presente Política de Sistemas de Información de Tecuni S.A., con alcance que afecta a todos los trabajadores que conforman su plantilla, independientemente de la categoría laboral y funciones de cada uno, directivos incluidos.

La vigencia es ilimitada en el tiempo a partir de la aprobación y firma del presente documento.

2 NORMAS DE USO DE LAS HERRAMIENTAS DE TRABAJO DE TECUNI S.A.

Tecuni S.A. pondrá a disposición de sus empleados las herramientas de trabajo que sean necesarias para la prestación de los servicios contratados en cada caso (ordenador portátil, ordenador "fijo" o "sobremesa", tablet, intranet, sistemas de geolocalización GPS, teléfonos fijos y móviles o Smartphones, cuenta de correo profesional, etc.). Todas estas herramientas son de titularidad exclusiva de la Empresa y, por ende, serán consideradas como herramientas de trabajo, cuya finalidad exclusiva será la prestación de servicios laborales o profesionales contratados.

Dicho lo anterior, tal y como se expondrá a continuación, los trabajadores de Tecuni S.A. deberán usar las mencionadas herramientas exclusivamente para su uso exclusivo profesional, no permitiéndose el uso personal de las mismas.

Finalizada la relación profesional, el trabajador deberá devolver a la Empresa todas las herramientas antes citadas, pudiendo Tecuni S.A. revisar su contenido y, en su caso, darle el tratamiento que considere oportuno que incluye el formateo, al tratarse de herramientas de uso exclusivo empresarial.

Por defecto, los departamentos de Sistemas IT y/o Compras-Aprovisionamientos, ambos bajo la misma dirección dentro de la Unidad de Servicios Centralizados, entregará los equipos con el sistema operativo y el software estándar que todo empleado de Tecuni S.A. debe tener instalado. No se permiten al usuario las siguientes acciones:

- Instalar software sin licencia
- Reinstalar el sistema operativo
- Virtualizar el sistema operativo entregado en otra máquina física o virtual

Cualquier necesidad de software que se salga del estándar autorizado debe ser expresamente requerida al Departamento de Sistemas IT.

Los departamentos de Sistemas IT y de Compras-Aprovisionamientos se reservan el derecho de monitorizar el software instalado en los ordenadores corporativos y resto de herramientas de trabajo descritas (tablets, teléfonos móviles y fijos, sistemas de geolocalización, etc.), y en su caso, eliminar o requerir la eliminación de cualquier software no lícito que se detecte.

Además, y con carácter general, a realizar las labores de control y verificación de todo tipo de accesos y de contenidos o datos asociados a los que los trabajadores han utilizado o tenido acceso a través de cualquier herramienta informática de la empresa descrita anteriormente o incluso no descrita (relación no exhaustiva), sin ningún tipo de restricción dado que todas ellas son herramientas corporativas puestas a disposición profesional de trabajadores para su uso exclusivamente profesional.

No están permitidas las modificaciones del hardware del equipo corporativo por parte del usuario.

3 ACCESOS

3.1 Acceso del Usuario

Todo acceso a los equipos y sistemas de comunicación estarán controlados y autorizados por el responsable nombrado al efecto y que ejerce la figura de Administrador de Sistemas. Queda estrictamente prohibido para cualquier usuario intentar acceder a los documentos, sistemas o recursos tecnológicos a los que no tenga autorización expresa por parte del Administrador de Sistemas.

Todo usuario autorizado tiene acceso a los sistemas informáticos mediante un nombre de usuario y contraseña personal e intransferible, comprometiéndose a tratarla con la máxima diligencia y confidencialidad, siendo el único responsable del buen uso de la misma.

El usuario autorizado será responsable único y directo de todo lo ejecutado en el sistema bajo su nombre de usuario y contraseña. Asimismo, quedan estrictamente prohibidos los intentos, de cualquier naturaleza y por cualquier medio, que persiga la obtención de acceso a contraseñas de otros usuarios sin su consentimiento.

Queda prohibido divulgar por cualquier medio las claves de acceso a cualquiera de los servicios que se faciliten al usuario, quien se compromete a dar aviso al Administrador de Sistemas, de forma inmediata, de cualquier incidencia o anomalía detectada en los accesos a los sistemas de información o en la seguridad de los mismos.

El usuario se obliga a respetar los derechos de terceros en los sistemas de uso compartido, comprometiéndose a no acceder a la información privada de otros usuarios, sin su previa autorización. Asimismo, el usuario se compromete a no compartir ficheros o documentos de cualquier tipo con otros usuarios, sin implementar las medidas necesarias que garanticen la seguridad de la información y de los sistemas operativos. Toda suplantación de identidad será sancionada de acuerdo a la normativa vigente que resulte de aplicación.

3.2 Acceso del Administrador de Sistemas

El Administrador de Sistemas se obliga a actuar con absoluta diligencia, guardando total confidencialidad sobre los datos, documentos, y demás informaciones a las que pudiere tener acceso en el ejercicio de sus tareas. A título de ejemplo, pero no limitativo se pueden incluir los siguientes:

- Acceso a los equipos y sistemas de información para llevar a cabo tareas de mantenimiento
- Acceso a los equipos, sistemas de información y documentos electrónicos por motivos de seguridad
- Autorizar los accesos de los usuarios a los sistemas de información que requieren para el cumplimiento de sus tareas, así como a los equipos informáticos, de forma conjunta con el responsable de seguridad
- Acceso a los equipos, redes o sistemas de información por incidencias en la seguridad de la información

En cualquier caso, el Administrador de Sistemas tiene el deber de guardar con absoluta confidencialidad toda la información a la que tenga acceso para el cumplimiento de sus actividades, quedando estrictamente prohibido comunicarla o facilitarla, directa o indirectamente, a ningún tercero.

4 SEGURIDAD. CONFIDENCIALIDAD Y PROTECCION DE DATOS

En el presente documento Tecuni S.A. y el usuario se comprometen a guardar el secreto de las comunicaciones, respetar la privacidad, intimidad y confidencialidad de todos los datos e informaciones de la Empresa, almacenados en los recursos tecnológicos y sistemas de comunicación de la misma; y a

no ceder a terceros los datos e información, tanto los de Tecuni S.A. como aquellos de carácter personal, obtenidos en el cumplimiento de sus actividades directas o cualesquiera otras de ámbito empresarial.

Y en general a respetar y cumplir escrupulosamente la totalidad de preceptos contenidos en la Ley Orgánica de Protección de Datos de Carácter Personal, Reglamento General de Protección de Datos 2016/679 y demás normativa aplicable.

5 CONSECUENCIAS DERIVADAS DEL MAL USO DE LOS RECURSOS TECNOLOGICOS Y SISTEMAS DE COMUNICACION

El usuario se compromete a colaborar con el Administrador de Sistemas para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los recursos tecnológicos y sistemas de comunicación.

El daño o uso de los recursos tecnológicos y sistemas de comunicación derivado de carácter abusivo o simplemente que escape del permitido por Tecuni S.A., será sancionado con la eliminación del acceso a los mismos, la aplicación de las sanciones por el incumplimiento de los términos condiciones que emanen del contrato, además de las sanciones legales establecidas en la normativa laboral y convencional vigente aplicable.

En este sentido y dado que el incumplimiento de lo establecido en esta Política de Sistemas de Información se considera un incumplimiento muy grave, las sanciones previstas por la empresa podrán llegar incluso hasta el despido disciplinario.

Al margen de estas sanciones, Tecuni S.A. se reserva el derecho de imponer las restricciones o controles complementarios que pudiere considerar oportunos, respetando siempre y en todo momento la normativa vigente.

6 REVISIÓN DE LA POLÍTICA DE SISTEMAS DE INFORMACION

Aunque la presente Política tiene vigencia ilimitada en el tiempo, esta precisaría de revisión y adaptación en el caso que se produjeran cambios significativos en la estructura organizativa, técnica, operativa y/o definición de políticas de la empresa.

Es por ello que Tecuni S.A. se reserva el derecho de suspender, modificar o retirar esta Política, constituyendo una responsabilidad compartida por parte de los empleados de Tecuni S.A. revisar de manera regular sus contenidos, detectar áreas de mejora y proponer al Administrador de Sistemas los cambios que consideren oportunos.