	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 1 de 9

1. Objetivo y campo de aplicación

El objeto de esta instrucción es establecer una guía para el usuario donde se establecen los principios que rigen de manera genérica las normas de seguridad relativas a los puestos de trabajo, tanto en cuestiones de seguridad física como lógica. Se incluyen en este apartado las políticas de dispositivos móviles y teletrabajo.

Se aplica a todo el personal autorizado para el tratamiento de información por la empresa.

2. Desarrollo

Esta guía establece las normas de seguridad a seguir por los empleados en su puesto de trabajo, esto incluye las normas de acceso tanto físicas como lógicas (acceso a las aplicaciones, intranet, correo electrónico, ...).

2.1. SEGURIDAD EN LOS PUESTOS DE TRABAJO

Control de acceso físico. Cada usuario tan solo puede acceder a las instalaciones, salas, ubicaciones..., de forma temporal o permanente, previa identificación, acreditación y durante el horario establecido.

Colocación de puestos e impresoras. Tanto las pantallas de los equipos como las impresoras deberán estar físicamente ubicadas en lugares o de manera que se garantice la confidencialidad.


Pantallas y protección de pantallas. Las pantallas de ordenadores deben estar colocadas de manera que se impida su visualización por personas no autorizadas. A estos efectos, se configuran en los equipos protectores de pantalla que, a la reanudación del uso, se desactiven con contraseña.

Se hará necesario cancelar todas las sesiones activas antes de finalizar la jornada laboral.

Puesto de trabajo despejado. Se habilitan armarios para guardar la información física que no esté siendo utilizada de tal manera que las mesas deben estar despejadas de información y otros materiales cuando los usuarios asignados no están en su puesto de trabajo.

Cuando no se estén usando, los papeles y los soportes informáticos deberán guardarse en locales cerrados y/o en los tipos de mobiliario de seguridad adecuados, especialmente fuera de las horas de trabajo.

Impresoras y faxes. Todos los puntos de entrada y salida de correo, así como las máquinas de fax e impresoras deben ser protegidas y estar custodiadas durante su uso para evitar accesos no autorizados a la información que puedan generar. Por tanto, cada usuario que tenga acceso a una impresora o fax debe asegurarse de que en sus bandejas de salida no quedan documentos

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 2 de 9

impresos que contengan información confidencial o secreta. Si las impresoras son compartidas, cada usuario debe retirar los documentos conforme vayan siendo impresos.

Equipo desatendido. Los ordenadores personales y terminales no se dejan desatendidos una vez completados los procesos de identificación y autenticación de usuario, permaneciendo bloqueados cuando no se estén utilizando.

Ficheros temporales. Se consideran ficheros temporales aquellos que están generados para atender a una finalidad concreta y limitada en el tiempo, mediante la extracción de datos de ficheros preexistentes, o como ficheros o documentos con tratamientos complementarios o preparatorios de otros.

Los ficheros temporales deben ser borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación, lo que es una obligación del usuario que lo ha generado.

Controles criptográficos. Siempre que la empresa permita la utilización de controles criptográficos, los administradores de sistemas proporcionarán los medios adecuados que permitan asegurar la confidencialidad, autenticidad y trazabilidad de las transacciones que los usen.

Los usuarios habilitados para utilizar certificados electrónicos deben estar autorizados expresamente por parte de la Dirección.

Si se efectúan entradas o salidas de datos mediante sistemas de transferencia de ficheros, a través de redes públicas o no protegidas, se recomienda su cifrado previo, de forma que solamente puedan ser leídos por su destinatario.


Uso del correo electrónico. El usuario sólo debe utilizar el correo electrónico que le facilite la empresa para los fines relacionados con las funciones y tareas que le han sido asignadas, sin permitirse el uso para fines privados.

El usuario es responsable de todas las actividades realizadas en sus cuentas de correo y respectivos buzones. No debe permitir la utilización del mismo a personas no autorizadas ni enviar mensajes a personas que no deseen recibirlo.

Cualquier fichero que introduzca un usuario en la red corporativa o en su terminal a través de mensajes de correo electrónico que provenga de redes externas debe cumplir con los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

Cuando el usuario deba compartir información clasificada como CONFIDENCIAL por correo electrónico, esta irá en archivos protegidos por contraseña, que sólo se revelará a su destinatario por otro canal diferente, por ejemplo, presencial o telefónico.

Utilización de tabletas electrónicas u ordenadores portátiles. Todos los usuarios están obligados a eliminar de los mismos cualquier información que no vaya a ser utilizada, volcándose en los ficheros y carpetas corporativas de la empresa. Al igual que para el resto de los

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 3 de 9

ordenadores se configuran los protectores de pantalla que, a la reanudación del uso, se desactiven con la contraseña correspondiente.

Normas de acceso y uso de Internet. Cada usuario debe utilizar Internet exclusivamente para fines laborales, de acuerdo con las instrucciones impartidas por la empresa.

El usuario no debe modificar las configuraciones de los navegadores de los equipos, ni la activación de servidores o puertos sin autorización del Responsable del Sistema.

Tampoco está permitido acceder a imágenes o contenidos ilegales o contrarios a la moral y buenas costumbres. No está permitido el acceso, descarga o almacenamiento en cualquier soporte de páginas con estos contenidos, ni de formatos de imágenes, audio o vídeo, de archivos que pueden contener virus y códigos maliciosos y en general, de todo tipo de programas piratas o ilegales sin la autorización pertinente del Responsable del Sistema.

No se permite el acceso a listas, servicios o foros de chat o sitios similares.

No está permitido participar en actividades de propagación de cartas encadenadas, esquemas piramidales o similares.


No está permitido difundir contenidos ilegales o contrarios a la moral y buenas costumbres.

Se prohíbe efectuar ataques dirigidos para obstruir sistemas informáticos, o cualquier actividad que tenga por objeto la paralización del servicio por saturación de líneas, de la capacidad del servidor, o cualquiera similar.

2.2. USO DE LA INFORMACIÓN

Propiedad intelectual e industrial. Queda estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra protegida por los derechos de propiedad intelectual o industrial, así como la instalación de programas informáticos sin la correspondiente licencia.

Uso de la información. Dado que en el desarrollo de sus funciones los usuarios pueden estar en contacto con información afectada por el alcance, estos están obligados a respetar la confidencialidad requerida por la empresa para el tratamiento de la misma y a utilizarla en el estricto ámbito de sus tareas laborales, en consonancia con los cometidos propios de su cargo. Como usuario del Sistema de Gestión de la Seguridad de la Información (SGSI) y dependiendo del puesto en el que esté incorporado, cada usuario tiene acceso únicamente a aquellos datos, carpetas, documentos y recursos precisos para el desarrollo de sus funciones. Será el responsable de la custodia de la información y de los datos que almacene en su puesto de trabajo.

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 4 de 9

Soportes de información. Está terminantemente prohibida la copia, extracción o distribución de información incluida en el SGSI en cualquier tipo de soporte, salvo autorización expresa del Responsable del Sistema o la Dirección.

Seguridad de documentos. No está permitido extraer fuera de las sedes de la empresa cualquier información para la que el usuario no esté autorizado expresamente por el Responsable del Sistema o la Dirección.

Destrucción de los documentos al ser desechados. Previa autorización, cuando sea necesaria la destrucción de documentos por parte del personal, esta debe de ser realizada según el procedimiento de gestión, distribución, desechado y reutilización de soportes.

Se procederá, cuando sea posible a la trituración de la documentación en papel previa eliminación.

2.3. CLASIFICACIÓN DE LA INFORMACIÓN


Toda la documentación desarrollada y manejada por **VIARIUM** se encuentra inventariada y clasificada en el Listado de Documentos del Sistema y en el Cuadro de Comunicación de la organización. Tanto el documento, como su contenido y su uso, se agrupan de la siguiente manera:

Documentos públicos. Se trata de documentos que contienen información de **VIARIUM**, pero es información que puede o debe ser conocida por cualquier persona o parte interesada de la organización. Son ejemplos de documentos públicos la Política de Seguridad de la Información y la Declaración de Aplicabilidad.

Documentos confidenciales. Igualmente, se trata de documentos que contienen información de **VIARIUM**, pero en este caso dicha información no debe ser conocida y utilizada por personas ajenas a la organización. La documentación la distribuye el propietario de la misma a aquellas personas que deban conocerla y manejarla y esta distribución queda registrada en el Control de la Distribución de la organización. Las personas a las que se les ha distribuido compartirán el documento con las limitaciones que se le hayan indicado y exclusivamente con la parte interesada con quien proceda.

Documentos secretos. Los documentos clasificados como secretos contienen información crítica de **VIARIUM**, que sólo debe ser conocida y utilizada dentro de su grupo de distribución. Queda terminantemente prohibido su conocimiento y uso fuera de este ámbito. Cuando el contenido y el uso deban limitarse a las personas a las que se han distribuido.

- Su control de acceso: sí requiere contraseña adicional a las credenciales de acceso. Esto quiere decir, que la información debe estar alojada en un sistema virtual o físico con control de acceso y seguridad.
- Su almacenamiento: dentro del perímetro de la organización y, a su vez, dentro del sistema virtual o físico determinado.

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 5 de 9

- c) La realización de copias: estará sujeto a la política de copias de seguridad de la organización. El documento no puede copiarse fuera del grupo de distribución dentro de la organización.
- d) El etiquetado de soportes: será necesario etiquetar los soportes físicos con cartelería de PERSONAL AUTORIZADO.
- e) Los repositorios estarán identificados como SECRETO (carpetas de email, carpetas de disco, ...). e) Su transmisión telemática: requiere encriptación (ZIP con contraseña por email y HTTPS para ficheros agregados a páginas web).

2.4. CONTROLES DE ACCESOS, IDENTIFICACION Y AUTENTIFICACION DE USUARIOS

Control de acceso a datos. Dado que en el desarrollo de sus funciones puede estar en contacto con información sensible de **VIARIUM**, deberá respetar su confidencialidad, y utilizarla en el estricto ámbito de sus tareas laborales, en consonancia con los cometidos propios de su cargo. Como usuario de los sistemas de información, dependiendo del puesto al que se incorpora, tendrá acceso únicamente a aquellos datos, carpetas, documentos y recursos precisos para el desarrollo de sus funciones. Será el responsable de la custodia de la información y de los datos de acceso a tu ordenador.

Sistema de control de acceso. Se le asignará un usuario y una contraseña a los ficheros informáticos, del que será responsable.

Si advirtiese o sospechase que sus claves han sido indebidamente conocidas o utilizadas por personas no autorizadas, deberá formular la oportuna notificación de incidencia en el plazo más breve posible, del modo y manera regulados en el registro de incidencias, que podrá solicitarse al Responsable del Sistema para su cumplimentación, y procederse inmediatamente a su cambio.


Con estos datos podrá acceder a:

- Cuenta de correo electrónico
- Intranet
- Sistema documental

Usted será el responsable de la custodia y buen uso de los datos de acceso.

Las contraseñas de acceso se sustituirán periódicamente, como máximo cada 6 meses, siendo las propias aplicaciones las que marca estos plazos. La sustitución de contraseñas se efectuará automáticamente y será el único conocedor de la misma.

La contraseña debe contener un mínimo de 8 caracteres y estar formada por cualquier combinación de letras, números y símbolos (solo caracteres basados en el estándar ASCII), y no puede contener tildes, espacios en blanco ni caracteres acentuados. La contraseña no debe haberse usado anteriormente para la misma cuenta.

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 6 de 9

Monitorización. Como medida de seguridad, este sistema y los servicios y la red en la que se soportan, pueden emplear programas de monitorización para identificar usos y accesos no autorizados. Al hacer uso de estos sistemas, el usuario consiente el uso de dichos medios de monitorización.

Las siguientes actividades se encuentran expresamente prohibidas:

- Compartir o facilitar el identificador de usuario y la clave de acceso facilitados por la empresa a otra persona física, incluido el personal de la propia empresa. En caso de incumplimiento de esta prohibición, el usuario será el responsable de los actos realizados por la persona física que utilice de forma no autorizada el identificador del usuario.
- Falsear los registros del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad.

2.5. GESTIÓN DE INCIDENCIAS

Debe reportar cualquier debilidad fallo y/o amenaza, observada o sospechada, respecto a la seguridad de los sistemas, datos, programas o servicios de la empresa, y aquellas incidencias producidas en la realización de sus tareas utilizando para ello el formulario de registro de incidencias.

A modo de observación se aconseja incluir en el registro de incidencias todo mensaje que aparezca en pantalla, así como seguir las indicaciones que posteriormente el Responsable del Sistema le ofrecerá.


2.6. NORMAS DE SEGURIDAD APLICABLES A DISPOSITIVOS MÓVILES Y TELETRABAJO

Dispositivos móviles. Entre los equipos móviles se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria, USB y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.

El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente con autorización.

Se debe tener especial cuidado cuando los equipos móviles se encuentran en vehículos (incluyendo automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la Organización.

La persona que se lleva dispositivos móviles fuera de las instalaciones debe cumplir las siguientes reglas:

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 7 de 9

- El dispositivo móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando sea utilizado en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.

Teletrabajo. Se deben tener en cuenta las siguientes consideraciones:

- Protección de los dispositivos móviles, de acuerdo a lo indicado en la sección anterior.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de teletrabajo.
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.

Propiedad de los activos. Por propiedad de los activos se entiende la cesión por parte de la organización de aquellos elementos (generalmente dispositivos móviles) de su infraestructura, a los empleados para su utilización en el desempeño de sus tareas asignadas. A todos los efectos, el uso esperado de estos activos será de aplicación exclusiva dentro del ámbito de la actividad de la organización y respetará los límites y condiciones establecidas en esta instrucción técnica y, de forma general, cumplirá con la cultura y las políticas de seguridad de la información de **VIARIUM**.


La propiedad del activo por parte del empleado comienza con la entrega del mismo por parte del Responsable del Sistema y finaliza con su retirada en perfecto estado y condiciones de funcionamiento. La duración de la propiedad quedará registrada en la **RE-006 FICHA DE PERSONAL** y podrá ser consultada por cualquier empleado accediendo a la misma desde la aplicación de soporte al Sistema de Gestión TQNET.

2.7. ACEPTACIÓN FUNCIONES Y RESPONSABILIDADES

Todo el personal afectado por el alcance (interno y externo) debe de conocer, aceptar y cumplir tanto la política de seguridad de este sistema como lo indicado en este procedimiento. Por ello, se facilitará una copia de la presente guía para su firma al inicio de la prestación del servicio, además de los compromisos de confidencialidad y no competencia adicionales que sean necesarios en cada caso.


Como personal de **VIARIUM**, tiene las siguientes obligaciones:

- Cumplir estrictamente las obligaciones establecidas sobre seguridad de la información, dimanantes del presente documento, y de las Instrucciones que al

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 8 de 9

efecto se le facilitan a través de la herramienta de gestión documental de la empresa.

- Respetar la confidencialidad de información manejada por **VIARIUM**, evitando su envío o difusión al exterior o a personas no autorizadas, por cualquier medio o soporte.
- Guardar la máxima reserva y no divulgar, directa o indirectamente, por sí o por personas o entidades interpuestas, los datos, documentos, metodologías, claves, contraseñas, programas y demás información a la que tengan acceso durante su relación laboral con **VIARIUM**.
- Utilizar o poseer únicamente los materiales o información de **VIARIUM** que sean precisos para el ejercicio de sus funciones, y dentro del ámbito de su relación laboral.
- Devolver a **VIARIUM** a la finalización de su relación laboral, cualquier tipo de datos o informaciones a las que haya tenido acceso por cualquier medio o soporte, con ocasión de su trabajo.
- Utilizar el correo electrónico conforme a las normas de **VIARIUM**.
- Cumplir las normas de **VIARIUM** para el acceso a Internet.
- No comunicar ni divulgar sus identificadores de usuario y claves de accesos, comunicando al respecto las posibles incidencias que se produzcan.
- No acceder a recursos, programas, datos o informaciones a las que no esté expresamente autorizado, por ser precisas para el ejercicio de sus funciones.
- No realizar copias de información en cualquier tipo de soporte sin la autorización previa del responsable, ni utilizarlas para fines ajenos a los de su trabajo.
- No dañar, alterar, destruir o inutilizar los datos, programas o documentos de **VIARIUM**.
- Abstenerse de intentar descifrar las claves, sistemas o algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de **VIARIUM**.
- Comunicar inmediatamente cualquier incidencia de la que tenga conocimiento al Responsable del Sistema.
- Utilizar adecuadamente la red corporativa, los recursos y sistemas de **VIARIUM**, sin introducir programas no autorizados, programas ilegales, virus, macros, applets o cualquier otro dispositivo que puedan causar alteraciones en los mismos.
- Abstenerse de crear ficheros con datos personales sin la previa autorización del Responsable del Sistema.
- Impedir la acumulación de información sobre datos personales, de forma que se evite la posibilidad de realizar valoraciones sobre la personalidad de los titulares de los datos.
- Cualquier otra obligación que resulte de la política de seguridad de **VIARIUM**, de las Instrucciones de Seguridad, de sus procedimientos de actuación y de la normativa vigente.
- Está completamente prohibido el envío de información/ documentación a través de las herramientas establecidas para online meetings.
- Se prohíbe el uso de herramientas de IA para consultar o documentar metodología.

	INSTRUCCIÓN TÉCNICA	IT-70-01
	PROTOCOLO DE SEGURIDAD DE LA INFORMACIÓN	Revisión 00
		Confidencial
		Página 9 de 9

2.8. CONDUCTA EN EL ENTORNO DE TRABAJO

Como personal de **VIARIUM** tiene las siguientes obligaciones:

- Cumplir con sus obligaciones de forma profesional, responsable y celosa, procurando la excelencia de desempeño.
- Facilitar a sus superiores información veraz y explicar con total transparencia sus decisiones y comportamientos profesionales.
- Proteger el patrimonio de la empresa utilizándolo sólo en la ejecución de los procesos de negocio y asegurando su uso eficiente.
- Informar de cualquier comportamiento que esté en conflicto con este manual de buenas prácticas y código de conducta. Se garantiza la confidencialidad y protección jurídica de quien informa, de acuerdo con la reglamentación propia, y un trato justo a sobre quién se informa.
- Respetar e incentivar los valores de **VIARIUM** promoviendo la cooperación, la responsabilidad individual y aceptando la diversidad.
- Procurar desarrollar y actualizar de forma continua sus conocimientos y competencias y sacar el mejor provecho de las acciones de formación promovidas por la empresa.

2.9. CONSECUENCIAS DEL INCUMPLIMIENTO

Aquel personal interno que en el tratamiento diario de la información objeto de este alcance, no lleve a la práctica lo indicado en las políticas, normas, procedimientos o cualquier documento del presente SGSI que le sea de aplicación a su puesto de trabajo, puede poner en peligro la seguridad de la información y los sistemas que la tratan.

Por ello, en caso de incumplimiento grave de cualquiera aspecto contenido en los citados documentos, el trabajador podrá ser objeto de la apertura de un expediente disciplinario en los términos y condiciones establecidos en el convenio y según lo indicado en el procedimiento seguridad ligada a los recursos humanos. Incluso puede conllevar a despido procedente si el incumplimiento persiste.