RocaJunyent

Normativa Interna de Medios Tecnológicos

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
24/10/2023	1.00	Grupo RocaJunyent	Primera versión del documento
21/11/2023	2.00	Grupo RocaJunyent	Adecuación de algunos puntos a los requisitos del despacho y régimen disciplinario
19/06/2024	3.00	Grupo RocaJunyent	Aclarar el punto 3 sobre el cumplimiento de este documento
12/09/2024	4.0	Grupo RocaJunyent	Introducir desarrollos Molins

Tabla de contenido

1. Propósito de la Política

La presente normativa interna tiene por objeto garantizar el buen uso de los medios, tanto los puestos a disposición por la organización de los usuarios, internos y externos, como los medios personales, en el desarrollo de sus funciones para GRUPO ROCA JUNYENT (ROCA JUYENT & SIGE), así como regular el tratamiento que ha de darse a la información y los datos personales de GRUPO ROCA JUNYENT y/o de sus clientes y proveedores en desarrollo de dichas funciones.

2. Alcance

Este documento se aplica a todos los profesionales, internos y externos, con acceso a los medios de GRUPO ROCA JUNYENT para el desarrollo de sus funciones y tareas profesionales, con independencia de su ubicación y titularidad de los mismos (proporcionados por la organización, de clientes o propios), en los términos y con la extensión que se indica en la presente Política.

Esta normativa extiende su aplicación a todos los usuarios que presten servicios directa o indirectamente en GRUPO ROCA JUNYENT. Esta normativa es de aplicación sin perjuicio de otras políticas existentes, en caso de contradicción, predominará la medida más restrictiva.

En caso de contradicción entre esta normativa y cualesquiera otras que puedan ser de aplicación al Profesional, predominará la medida, instrucción o pauta que sea más garantista y/o proteccionista con la información, los datos personales y/o los sistemas, en tanto exija niveles de seguridad más elevados.

3. Comunicación, información y aceptación

El presente documento debe ser puesto a disposición de todos los profesionales de la organización en el momento en que inicien su relación profesional con GRUPO ROCA JUNYENT, y es de obligatorio cumplimiento, así como la política de seguridad de la información y el resto de los procedimientos y las políticas del Sistema de Gestión de Seguridad de la Información (SGSI).

En caso de actualización, se facilitará la misma a todos los profesionales con la mayor brevedad posible. En ambos casos, se deberá obtener la correspondiente aceptación del documento.

La utilización de los documentos, información y datos personales, sistemas o servicios de GRUPO ROCA JUNYENT o puestos a disposición de los Profesionales por GRUPO ROCA JUNYENT o sus Clientes que no se ajusten a los procedimientos establecidos en la presente normativa podrá dar lugar a acciones disciplinarias, así como, en su caso, a reclamaciones de responsabilidad civiles y penales y/o de los daños y perjuicios ocasionados.

4. Uso de medios corporativos

Como regla general, los medios pertenecientes a GRUPO ROCA JUNYENT y proporcionados al personal por la misma únicamente se utilizarán para asuntos relacionados con la actividad de la organización y/o el cumplimiento de las obligaciones legales y/o laborales, pudiendo GRUPO ROCA JUNYENT realizar un control del uso de los mismos y adoptar las medidas de vigilancia que estime más oportunas para verificar el cumplimiento por el usuario de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a sus derechos. Dichas medidas se aplicarán de forma proporcional, idónea y no excesiva, bajo el principio de mínima intervención.

El disco duro del ordenador y el servidor del sistema informático de GRUPO ROCA JUNYENT no son medios idóneos para el almacenamiento de archivos privados, pues de conformidad con lo establecido en la presente Política debe tenerse en cuenta que GRUPO ROCA JUNYENT podrá

realizar un control de los medios corporativos.

Estos medios son personales e intransferibles.

El usuario es responsable de los medios que se le hayan facilitado para el desempeño de sus funciones. Por tanto, es el usuario el que debe garantizar la seguridad tanto de los medios puestos a su disposición como de la información que contienen. En ningún caso el usuario podrá participar, influir y/o permitir situaciones o acciones que se vinculen con el robo, hurto, mal uso, préstamo o venta de los medios asignados sin autorización previa expresa.

El uso y asignación de medios está inventariado y registrado, así como del software relacionado con los mismos. A la entrega de los medios se deberá firmar el documento correspondiente de registro de entrega de soportes**.**
En todo caso, con la entrega y firma de esta Política a los profesionales se pone de manifiesto el entendimiento de que los medios corporativos no constituyen, en todo o parte, medios privativos o personales de los usuarios.

Uso de Internet

El usuario seguirá las siguientes recomendaciones en relación con la navegación por Internet:

I. Verificar que las direcciones URL de destino son correctas.

II. Verificar la autenticidad de la página web, utiliza siempre protocolo seguro **HTTPS**, y verificar si el certificado está vigente.

III. Evitar el almacenamiento de contraseñas por parte del navegador.

IV. No se descargarán ni ejecutarán programas, controladores, ni archivos descargados de origen desconocido, salvo autorización expresa por el Departamento IT.

V. Se prohíbe el acceso a direcciones URL de dudosa procedencia y de contenido que atente contra la moralidad de la organización.

VI. Analizar el **aviso de cookies** procurando no aceptar cookies innecesarias, aceptando únicamente las funcionales para una correcta navegación.

Es responsabilidad de los usuarios realizar un uso correcto de internet, siendo estos responsables en caso de mal uso, ya sea por negligencia o por utilización abusiva del servicio.

En todo caso, se prohíbe el uso de Internet con el objeto de acceder a páginas o direcciones de contenido ofensivo o atentatorio contra la dignidad humana o derechos fundamentales. En general, se prohíbe el acceso a cualquier dirección de Internet cuyo contenido vulnere la legislación vigente, pudiendo únicamente navegar por sitios web lícitos.

Uso de conexiones Wi-Fi y conexión a redes externas

La conexión a redes externas a la organización quedará reducidas a ocasiones en las que sea imprescindible y únicamente para la realización de las tareas relacionadas con la actividad laboral del usuario.

Al conectarse a estas redes externas, el usuario deberá hacer uso en todo momento de la VPN proporcionada por GRUPO ROCA JUNYENT. Bajo ningún concepto se emplearán **wifis públicas** para actividades de la organización, sin el uso de la VPN.

Para el acceso mediante wifis domésticas, se hará uso de la VPN para la realización de las actividades laborales del usuario.

En caso de que el Profesional se conecte desde medios que sean dispositivos móviles, es recomendable que únicamente active los servicios que vayan a ser utilizados y siga las pautas de navegación segura en el uso de internet.

Almacenamiento y uso de medios tecnológicos

Los medios puestos a disposición de los usuarios, por parte de GRUPO ROCA JUNYENT, quedan en todo momento bajo el cuidado y responsabilidad de los mismos.

I. Se evitará la utilización de los medios cerca de componentes líquidos, inflamables, etc.

II. Se evitará la exposición prolongada a altas temperaturas.

III. No se descuidarán si se emplean en espacios públicos, y siempre serán transportados a buen recaudo. También se evitará su almacenamiento en vehículos ni en zonas visibles o fácilmente accesibles. Siempre que sea posible se guardarán bajo llave y vigilados.

IV. Los medios tecnológicos (portátiles) están protegidos mediante cifrado (bitlocker).

V. Se prohíbe la alteración de la configuración de seguridad establecida, ni se realizarán modificaciones en el hardware o software.

VI. Se deberá notificar tan pronto como sea posible a Departamento IT de cualquier sospecha de vulneración del dispositivo en cualquiera de sus ámbitos.

Uso del puesto de trabajo

I. **Política de mesas limpias**. Se conoce como la obligación de guardar la documentación e información de “Uso Interno”, “Restringida / de grupo” y “Confidencial” al ausentarse del puesto de trabajo y/o finalizar la jornada laboral.

II. El almacenamiento de esta información deberá llevarse a cabo de acuerdo con el “Procedimiento de Tratamiento de la Información”:

   a. Uso Interno: A resguardo en muebles y/o archivadores.
   b. Restringida/de grupo: En una ubicación adecuada bajo llave, y con control de acceso.
   c. Confidencial: En una ubicación adecuada bajo llave, y con control de acceso.

III. **Política de escritorios limpios**. Existirá un bloqueo automático de sesión al no detectarse actividad de los usuarios por un corto período de tiempo. El usuario deberá cerrar sesión o bloquear la pantalla cuando se ausente o permanezca inactivo, y/o apagará el dispositivo cuando termine de utilizarlo.

IV. **Destrucción de información**. La información obsoleta se destruirá de forma segura, en concreto, se hará uso de las destructoras de papel dispuestas por la organización. El uso de papeleras que no destruyan la información para eliminar la información de “uso interno” o “confidencial” está prohibido ya que puede constituir un riesgo de seguridad.

V. **Antivirus y otras herramientas de detección**. La solución antimalware instalada en los dispositivos GRUPO ROCA JUNYENT es mantenida y actualizada de forma continua y

centralizada por parte de la organización. Cualquier ocurrencia relacionada con los mismos deberá ser comunicada a Departamento IT. Los usuarios tienen prohibido deshabilitar cualquiera de las medidas de seguridad implementadas en cualquiera de los medios proporcionados por la organización, salvo autorización expresa.

VI. **Uso de medios extraíbles**. Esta permitido el uso de medios extraíbles, siguiendo las pautas de seguridad, al introducir una unidad externa esta será encriptada, si el profesional declina su encriptación, solo podrá usar la unidad extraíble en modo lectura.

VII. **Política de impresiones**. La organización pone a disposición de los profesionales el uso de impresoras y equipos multifunción, este servicio se centraliza a través de un servidor de impresión, para recoger los documentos impresos es necesario identificarse en los dispositivos de impresión.

VIII. **Comunicación de los incidentes en el puesto de trabajo**. Los usuarios deberán informar de cualquier incidente relacionado con el puesto de trabajo a su responsable directo, y/o a través de la herramienta de ticketing tales como:

a) Actividad sospechosa en el puesto de trabajo.
b) Alertas de virus/malware generados por el antivirus.
c) Llamadas sospechosas recibidas pidiendo información profesional y/o confidencial.
d) Correos electrónicos sospechosos (adjuntos con extensiones sospechosas, remitentes extraños, etc)
e) Pérdida de dispositivos portátiles y soportes de almacenamiento.
f) Borrado accidental de la información.
g) Alteración accidental de datos o registros.
h) Hallazgo de información en ubicaciones no designadas para ello.
i) Evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido.
j) Evidencia o sospecha de accesos no autorizados a los medios, sistemas informáticos o información confidencial por parte de terceros.

IX. **Configuraciones de los medios tecnológicos**. Los usuarios tienen prohibida toda modificación de la configuración aplicada por GRUPO ROCA JUNYENT sobre cualquier medio tecnológico, salvo expresa autorización.

Correo electrónico corporativo

El correo corporativo proporcionado a cada usuario por GRUPO ROCA JUNYENT será usado únicamente para la comunicación de aspectos relacionados con las actividades profesionales, y no podrá ser utilizado con fines profesionales o personales que no tengan que ver con la actividad de la organización. Las comunicaciones realizadas por esta vía en ningún caso se considerarán privadas o confidenciales.

Los usuarios deberán ser advertidos de que, al realizarse copias de seguridad de los correos electrónicos, no es posible distinguir entre los emails de carácter personal y los profesionales.

Se deberán seguir y aceptar las siguientes directrices en el uso del correo corporativo:

I. La contraseña de acceso deberá seguir las normas básicas de robustez definidas en este documento

II. La modificación de las configuraciones de seguridad aplicadas a los correos corporativas queda prohibida, salvo expresa autorización.

III. El usuario no debe aceptar documentos ni archivos adjuntos provenientes de direcciones desconocidas o que contengan un asunto u origen poco fiable. Se debe prestar especial atención a los siguientes indicios:

a) Extensiones de archivos adjuntos sospechosas (.exe, .bat, .js, .vbs, .ps1, .dll, .ms1, .bash, etc).
b) El archivo tiene una extensión familiar, pero está seguida de muchos espacios que no permiten ver la extensión real.
c) Tienen un nombre que invita a la descarga, o tienen nombres de aspecto aleatorio.
d) El icono del archivo no corresponde con el tipo del mismo.
e) El cuerpo del mensaje presenta cambios de aspecto con respecto a los mensajes recibidos previamente por ese mismo remitente.
f) El mensaje contiene una «llamada a la acción» que nos urge, invita o solicita pulsar enlaces, descargar o abrir archivos, o hacer algo no habitual.
g) Se solicitan credenciales de acceso a una web o aplicación.

IV. El usuario no abrirá correos spam ni sus adjuntos. Todos estos mensajes deberán eliminarse sin ser leídos para evitar que se detecte la cuenta de correo como “activa” y se sigan remitiendo correos spam.

V. Está prohibido configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo. Es preferible la extracción previa del adjunto y analizarlo con el antivirus.

VI. Al recibir un mensaje con un enlace se deberá revisar la URL antes de hacer clic, y se deberá asegurar que no existan caracteres que puedan parecerse entre sí en algunas tipografías, como 0 y O.

VII. Se deberá prestar atención a los correos electrónicos de remitentes sin identificar con los que no se ha tenido un contacto previo. Por otro lado, si el remitente es un contacto conocido, y existen indicios de suplantación de identidad se deberá contactar con éste por otro medio para confirmar su identidad.

VIII. Se evitará publicar direcciones de correo corporativos en páginas web y/o redes sociales, salvo en los canales y/o cuentas específicamente autorizadas para ello.

IX. Se evitará el uso de la cuenta de correo corporativo para la suscripción a servicios y plataformas no relacionadas con la actividad laboral del usuario.

X. Los usuarios de GRUPO ROCA JUNYENT deberán seguir las siguientes pautas en el envío de correos electrónicos:

a) No se facilitarán datos personales o financieros a personas desconocidas.
b) No se responderá al correo no solicitado (spam).
c) Se eliminarán los mensajes masivos innecesarios (felicitaciones, chistes, etc.).
d) Se evitará participar en el reenvío de correo no solicitado.
e) No se divulgarán direcciones de correo a terceros sin consentimiento de sus titulares.
f) No se podrá reenviar correos electrónicos corporativos a cuentas personales. Tampoco se utilizarán sistemas de mensajería ajenos a los dispuestos por GRUPO ROCA JUNYENT.
g) se utilizará la copia oculta cuando se envíen mensajes a múltiples destinatarios: el profesional se enviará el correo a si mismo y pondrá en copia oculta al resto de destinatarios. la copia oculta impide que los destinatarios vean a quién más se ha enviado el correo y se evitará comunicar a terceros, direcciones de correo que

pueden ser consideradas datos personales y cuyo uso únicamente está autorizado para los fines para los que fue recabado

En el caso de bajas de los profesionales o fin de la relación, se disponen las siguientes actuaciones:

I. **Fin de la relación por baja definitiva**: Se llevará a cabo una redirección de la cuenta de correo por un periodo de entre 3 y 6 meses a una dirección de correo solicitado por el Socio responsable. Adicionalmente se configurará un mensaje automático para avisar que esta cuenta ya no está operativa.
II. **Bajas por enfermedad**: Se llevará a cabo una redirección de la cuenta de correo por un periodo de entre 3 y 6 meses a una dirección de correo solicitado por el Socio responsable. Adicionalmente se configurará un mensaje automático para avisar que esta cuenta ya no está operativa.

El departamento IT llevará un control de las cuentas redirigidas para avisar a los responsables del fin de esta redirección.

Instalación de aplicaciones

No se permitirá a los usuarios, la instalación o actualización del software presente en sus dispositivos. La instalación de software y/o aplicaciones en los dispositivos tecnológicos se debe hacer previo consentimiento a través de un ticket al Departamento IT.

No se utilizará software sin licencia bajo ningún concepto. El uso de software debe quedar limitado, en cada caso, al uso permitido por la licencia adquirida, siendo el usuario responsable de cualquier posible vulneración de la Propiedad Intelectual y /o otros derechos que puedan corresponder al titular de la licencia o al propietario del software.

Cuando resulte adecuado por el uso que vaya a realizarse, se implementarán mecanismo de seguridad como un Sandbox, que permitan disponer de un entorno aislado del resto del sistema operativo para ejecutar programas de forma segura y sin comprometer los dispositivos.

Está prohibida la instalación de software proporcionado por clientes de GRUPO ROCA JUNYENT o por GRUPO ROCA JUNYENT en medios distintos a los autorizados. La instalación de software y/o aplicaciones titularidad de los Proveedores y/o Clientes de GRUPO ROCA JUNYENT se debe hacer previo consentimiento de GRUPO ROCA JUNYENT y del Cliente o Proveedor y cumpliendo estrictamente las políticas de éstos y la presente normativa en lo que resulte de aplicación.

Uso de los servicios en la nube

Solo se permite el almacenamiento de la información perteneciente o relacionada con las actividades de GRUPO ROCA JUNYENT en las nubes dispuestas y/o expresamente autorizada por ésta. Estará prohibido el almacenamiento de información en otras localizaciones no autorizadas por GRUPO ROCA JUNYENT tales como nubes gratuitas.

La información almacenada en la nube corporativa de GRUPO ROCA JUNYENT deberá ser clasificada de acuerdo con el tipo de información, y deberá proteger la misma de acuerdo con su nivel de clasificación. Para más información consultar la “Política de Tratamiento de la Información” y/o el apartado de “Uso de información corporativa” presente en este documento.

En caso de que sea necesario eliminar información, ésta deberá ser eliminada de forma segura de acuerdo con lo dispuesto en la “Política de Tratamiento de la Información” y/o el apartado de “Uso de información corporativa” presente en este documento.

La nube corporativa está configurada de modo que se garantice la confidencialidad, integridad y disponibilidad de la información profesional y/o confidencial al máximo nivel posible. Queda prohibido deshabilitar la configuración de la nube corporativa, salvo autorización expresa. El personal técnico podrá revisar la nube corporativa periódicamente para garantizar su actualización.

5. Uso de los dispositivos personales (BYOD)

El uso de los dispositivos personales está autorizado para la realización de las actividades laborales de los profesionales de GRUPO ROCA JUNYENT, en los términos que se prevén a continuación.

Los usuarios podrán instalar en sus dispositivos los diferentes servicios proporcionados por GRUPO ROCA JUNYENT, tales como, el correo corporativo y el MFA.

La dirección de la organización comunica que la instalación de servicios corporativos en dispositivos personales de los usuarios no es obligatoria. Aquellos que consientan en instalar estos servicios serán responsables de proteger y salvaguardar toda información que pueda ser almacenada y gestionada por los mismos.

Los usuarios serán susceptibles de medidas disciplinarias si incurren en infracciones determinadas por este orden:

- El convenio de oficinas y despachos a nivel autonómico.
- Real Decreto 1331/2006, de 17 de noviembre, por lo que se regula la relación laboral de carácter especial de los abogados que prestan servicios en despachos de abogados, individuales o colectivos.
- Estatuto de los trabajadores.

GRUPO ROCA JUNYENT recomendará a todos los usuarios que instalen servicios de la organización en sus dispositivos móviles a seguir las buenas prácticas que se expondrán a continuación:

I. La información perteneciente a la organización se almacenará en los dispositivos personales solo en última instancia y por extrema necesidad.

II. Se recomendará el uso de soluciones antimalware en los dispositivos personales, recomendándose en mayor medida el uso de soluciones completas.

III. Se recomendará el uso de buenas prácticas en la navegación a través de Internet.

IV. Se recomendará configurar el bloqueo automático de los dispositivos por contraseña.

V. Se recomendará el uso de buenas prácticas en la instalación de software en sus dispositivos, y únicamente de fuentes veraces y fiables.

VI. Se recomendará el uso de buenas prácticas en el uso de correo electrónico tanto corporativo como personal.

VII. Se recomendará la implementación de las actualizaciones de seguridad de los dispositivos.

Bajo ningún concepto se permitirá a terceros acceder a la información y servicios presentes en los dispositivos personales.

En todo caso, se deberá informar inmediatamente de la pérdida o robo del dispositivo personal y colaborar con GRUPO ROCA JUNYENT en la detección del mismo, y/o en su caso en la mitigación de las consecuencias si la información se ve afectada.

Se informa que en GRUPO ROCA JUNYENT se mantiene un servicio MDM (Mobile Device Management), utilizado principalmente para la gestión de los dispositivos corporativos.

En el caso de hacer uso de la cuenta corporativa en un dispositivo propio, el sistema podrá preguntar al usuario si quiere adscribirse a dicho servicio en el primer acceso en el dispositivo. Esta adscripción es en todo momento voluntaria, y la aceptación de la misma por parte del usuario es una autorización expresa del mismo para que el servicio MDM monitorice dicho dispositivo.

Si el usuario cambiará de parecer en lo referente a este servicio deberá comunicarse con Departamento IT, vía ticket.

GRUPO ROCA JUNYENT no se hace responsable de cualquier daño o perjuicio, que la instalación de cualquier software y servicios corporativo pueda hacer a los dispositivos personales.

Tras la finalización de la relación laboral con GRUPO ROCA JUNYENT, el usuario deberá devolver toda información perteneciente a la organización, y deberá eliminar todo software y servicio corporativo de sus dispositivos personales.

6. Uso de la información corporativa

La información es uno de los activos principales de GRUPO ROCA JUNYENT y ha de ser protegida correctamente. La información se puede encontrar en todo tipo de soportes, ficheros, programas y aplicativos.

Toda información nacida como resultado de las actividades laborales de GRUPO ROCA JUNYENT es propiedad de la misma, y se reserva todos sus derechos sobre ella.

Toda información cedida a GRUPO ROCA JUNYENT como resultado de sus relaciones con sus profesionales, clientes y proveedores deberá ser protegida y almacenada con el mayor nivel de confidencialidad posible, y será solo accesible, únicamente, para aquellas personas autorizadas expresamente por la organización.

El objetivo de esta sección es definir los criterios de clasificación de los activos de información para garantizar una gestión eficaz de su seguridad en GRUPO ROCA JUNYENT a partir de sus criterios de confidencialidad, integridad y disponibilidad.

Clasificación de la información

Por su nivel de confidencialidad, la información en GRUPO ROCA JUNYENT se podrá clasificar como:

I. Público. Información sin ninguna necesidad de restricción de acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización.

II. Ejemplos: Información de las webs, redes sociales, folletos comerciales…

III. Uso Interno. Información a la que sólo debe tener acceso el personal de GRUPO ROCA JUNYENT. Si se filtrará a terceras partes, podría tener consecuencias para la empresa.

IV. Ejemplos: Desarrollos, proyectos, configuraciones de los sistemas…

V. Restringida/de grupo: En GRUPO ROCA JUNYENT, todo documento creado dentro del sistema de información viene restringido por defecto, pudiendo ser visualizado por todos los

profesionales del departamento, pero ser únicamente modificado por aquel personal perteneciente al grupo de trabajo del redactor inicial.

VI. Confidencial. Información a la que sólo determinadas personas y/o departamentos (Socios del despacho) dentro de la organización pueden tener acceso. Si se filtrara a terceras partes, podría tener consecuencias serias para la organización.

Ejemplos: Contabilidad, contratos, tanto con clientes como con profesionales, datos de servicios a clientes (contraseñas, parámetros de proyectos…)

En función de la clasificación que reciba la información, será preciso aplicar las medidas de seguridad oportunas para garantizar que ésta se mantenga en el nivel de confidencialidad adecuado, integridad y disponibilidad.

Medidas generales

En ningún caso, se revelará información a terceros y/o usuarios no debidamente identificados. Son habituales las prácticas de ingeniería social en las que se intenta obtener información confidencial mediante engaños a los usuarios de una organización por lo que el respeto de este principio es fundamental para salvaguardar la información de la organización.

Si fuera necesario la transmisión de información con proveedores en el desarrollo de las actividades de la organización, el usuario realizará comprobaciones por distintos medios para verificar en todo momento la autenticidad del contacto.

Por otro lado, los usuarios deben aceptar un compromiso de confidencialidad relativo a cualquier información a la que tenga acceso durante la realización de sus funciones en/para GRUPO ROCA JUNYENT. Esta obligación de confidencialidad tiene validez durante todo el tiempo que dure el vínculo profesional con GRUPO ROCA JUNYENT, y aún finalizado este, durante el tiempo determinado en lo documentos firmados por el usuario/organización al inicio de su relación con GRUPO ROCA JUNYENT.

Tras la finalización de la relación laboral con GRUPO ROCA JUNYENT, el usuario/organización deberá devolver toda aquella información y dispositivos en su posesión pertenecientes a GRUPO ROCA JUNYENT. Además, les serán revocados todos los accesos y cuentas que le fueran proporcionadas durante la prestación de sus servicios para GRUPO ROCA JUNYENT.
Para el caso de que no se produjera tal devolución o al producirse se detectasen desperfectos derivados de un uso abusivo o no autorizado por parte del usuario, GRUPO ROCA JUNYENT se reserva el derecho a tomar las medidas que considere necesarias para el resarcimiento por parte del usuario de los daños que se hayan producido en relación con los dispositivos.

Ninguno de los soportes de información pertenecientes a GRUPO ROCA JUNYENT son medios idóneos para el almacenamiento de archivos privados, pues de conformidad con los establecido en las Políticas de GRUPO ROCA JUNYENT debe tenerse en cuenta que la organización podrá realizar un control de los medios corporativos.

Información Confidencial

Para la protección de la información confidencial, se establecerán como mínimo controles de acceso a la misma y, en la medida de lo posible, herramientas criptográficas que cifren los datos y la información. Así mismo, se procurarán protocolos seguros en las comunicaciones para todos los usuarios de los servicios.

Se tendrá especial precaución en la contratación de servicios externos que traten información confidencial o datos personales. Se deberá hacer uso en todo momento de canales de comunicación seguros y autorizados por la organización.

También se debe tener en cuenta el uso de nuevos servicios, como los chats de inteligencia artificial, a la hora de incluir información confidencial en los chats. Para ello GRUPO ROCA JUYENT ha establecido un grupo de trabajo y unas buenas prácticas de uso a través del documento: **ChatGPT – Límites y pautas.**

Se evitará el almacenamiento de la información confidencial en los dispositivos finales de los usuarios, siendo la mejor práctica el almacenamiento de la misma en los gestores de documentación dispuestos y autorizados por GRUPO ROCA JUNYENT.

Se prohíbe el uso de la información que se hubiese podido obtener por la condición trabajador de GRUPO ROCA JUNYENT, y que no sea necesaria para el desarrollo de sus funciones.

Todos los compromisos asumidos en materia de confidencialidad deberán mantenerse, incluso después de extinguida la relación laboral con GRUPO ROCA JUNYENT, en los términos previstos en el correspondiente contrato de trabajo.

Datos de clientes, proveedores y/o terceros

Toda la información proporcionada por clientes y proveedores deberá ser clasificada como confidencial, incluyendo datos de carácter personal, y deberá ser protegida y gestionada con las medidas acordes a su clasificación.

Se seguirán las siguientes pautas en relación con el manejo de la información de clientes y proveedores:

I. Sólo se accederá únicamente a los datos personales necesarios para la realización de sus funciones laborales en GRUPO ROCA JUNYENT.

II. La información de clientes, proveedores y/o terceros no podrá ser cedida ni compartida, salvo previa autorización.

III. Cuando los datos de carácter personal hayan dejado de ser útiles para los fines que fueron recabados u obtenidos, o su tiempo de retención haya expirado, deberán ser eliminado de manera segura, y a través de las herramientas y metodologías autorizadas por GRUPO ROCA JUNYENT.

Todos los Profesionales de GRUPO ROCA JUNYENT deben ser conscientes de los derechos de propiedad intelectual y/o industrial de terceras partes. Su uso inadecuado está prohibido. Ninguna persona de GRUPO ROCA JUNYENT podrá adquirir secretos de terceros o usarlos sin la debida autorización, de acuerdo con la normativa vigente, y específicamente:

Contraseñas

La definición de unas buenas prácticas en la generación y gestión de contraseñas es vital para una correcta seguridad de los accesos a los diferentes servicios de la organización. Por ello, a continuación, se desglosan aquellos criterios que se deben tener en cuenta en la gestión de credenciales de acceso:

I. Las credenciales de acceso son confidenciales y no pueden ser publicadas ni compartidas.

II. Se debe evitar los usuarios y contraseñas por defecto que traen los sistemas y equipos por lo que, se deberá realizar una modificación de los mismos tras el primer acceso.

III. Se establecerán sistemas de doble factor para el acceso a los servicios que contengan información confidencial.

IV. Se evitará el almacenamiento de contraseñas en soporte físicos tal que en papeles o post-its.

V. No se comunicarán credenciales por correo electrónico ni mensajes, así como tampoco en formularios o sitios webs.

VI. No se empleará la misma contraseña para servicios diferentes, ni para uso profesional y doméstico.

VII. Las contraseñas deberán ser creadas de acuerdo con los siguientes criterios:

a) Deberán tener una longitud mínima de 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales.
b) No debe contener palabras sencillas, nombres propios, datos fácilmente relacionables con el usuario o referencias al servicio de acceso.
c) No se emplearán claves fácilmente adivinables o públicas.

VIII. Se deberá rotar las contraseñas de acceso de forma periódica. No se podrán reutilizar contraseñas ya utilizadas.

IX. El número de intentos de autenticación estará limitado.

Almacenamiento de la información

La información confidencial y de uso interno será almacenada en los medios y soportes autorizados por GRUPO ROCA JUNYENT. Se evitará en todo momento el almacenamiento de información en los dispositivos finales de los usuarios, y en los dispositivos personales o BYOD.

En todo momento, únicamente se permitirá el acceso a los datos confidenciales y/o de carácter personal a aquellos usuarios que precisen de ellos para la realización de sus actividades laborales en/para GRUPO ROCA JUNYENT.

Se recomendará la limitación del uso de soportes de almacenamiento extraíbles, y en caso de uso, se han establecido medidas para su cifrado o uso en modo lectura.

7. Comunicación de incidencias

En caso de producirse alguna de las situaciones como pérdida, robo, hurto o fuga de información que potencialmente pueda suponer o derivar en una brecha de seguridad deberá comunicarse inmediatamente este hecho al responsable del departamento, así como al CAU o al Departamento IT a través de ticket o correo electrónico, si lo anterior no fuera posible.

El usuario en cuestión será responsable en caso de no comunicar cualquiera de dichas situaciones. La comunicación deberá efectuarse mediante un canal escrito pudiendo emplearse las plataformas dispuestas por la organización (portal de gestión de tickets, correo electrónico), y se deberá dejar constancia documental de dicha comunicación siguiendo el procedimiento de Comunicación y Gestión de incidencias.

8. Control de la actividad laboral

El control de la actividad laboral está establecido por la legislación vigente, desde GRUPO ROCA JUNYENT se establecen controles de seguridad que permiten ejercer las facultades de inspección y control que estime más oportunas para verificar el cumplimiento por el usuario de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a sus derechos.

Control de medios tecnológicos corporativos

I. Podrá existir, de acuerdo con la jurisprudencia y normativa vigente en cada momento, un control de los equipos informáticos por parte de GRUPO ROCA JUNYENT para:

a) La necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los usuarios.
b) La protección del sistema informático y de los sistemas de información de GRUPO ROCA JUNYENT, que puede ser afectado negativamente por determinados usos.
c) La prevención de responsabilidades que para GRUPO ROCA JUNYENT pudieran derivar también algunas formas ilícitas de uso frente a terceros.
d) En el marco de una investigación interna, siempre que esté justificado y no existan medidas menos invasivas a adoptar.

II. El medio de control empleado deberá ser, en todo caso, estrictamente proporcionado.

III. Atendiendo a lo establecido anteriormente, y siempre de conformidad con criterios de proporcionalidad, necesidad e idoneidad, la revisión de los recursos informáticos corporativos podrá realizarse tanto si su usuario es aún miembro de GRUPO ROCA JUNYENT como en caso de que haya finalizado su relación laboral o mercantil.

IV. GRUPO ROCA JUNYENT podrá controlar, siguiendo lo establecido en la normativa y jurisprudencia vigentes en cada momento, los medios tecnológicos corporativos para verificar el cumplimiento por el usuario de sus obligaciones y deberes laborales.

V. GRUPO ROCA JUNYENT realizará copias de seguridad de forma periódica de todos los datos almacenados en los recursos TIC.

VI. En el marco de su facultad de control de la actividad del empleado, GRUPO ROCA JUNYENT estará legitimado para realizar, entre otras, las siguientes intervenciones:

a) Control de los contenidos guardados, de los flujos de información, de la carga y descarga de archivos, documentos, programas, entre otros, así como de las tareas realizadas en los ordenadores de mesa, dispositivos portátiles, tabletas, teléfonos móviles, sistemas en la nube, mensajería instantánea o cuentas de correo corporativos de los empleados de GRUPO ROCA JUNYENT.

b) Intervención de líneas telefónicas, sistemas de voz IP y sistemas de mensajería instantánea, titularidad de GRUPO ROCA JUNYENT y de las asociadas a los recursos TIC puestos a disposición de los empleados del Grupo mercantil como, por ejemplo, control de identidad de los destinatarios o remitentes de las llamadas y mensajes, escucha o acceso al contenido de las llamadas y mensajes, entre otros.

c) Control de la geolocalización de los dispositivos.

d) Monitorización y comprobación de sesiones de acceso a internet mediante el chequeo de los archivos LOG del servidor.

e) Revisión de los mensajes del correo electrónico, no pudiendo distinguir entre emails de carácter personal y profesional.

f) Instalación de micrófonos y cámaras en ciertas estancias comunes.

g) Registros sobre el usuario, efectos personales y recursos productivos privativos.

h) Medidas contra el hacking o allanamiento informático como, por ejemplo, la identificación y autentificación de usuarios, credenciales, etcétera.

i) Controles específicos en materia de propiedad intelectual como, por ejemplo, la revisión de terminales, inventario de licencias de uso, listas de programas homologados, etcétera.

VII. Así mismo, para los dispositivos que lleven incorporados sistemas de geolocalización, podrán ser localizados por el GRUPO ROCAJUNYENT, a través del Departamento de IT, únicamente en caso de pérdida o robo.

9. Controles específicos

Medidas contra el hacking o allanamiento informático

GRUPO ROCA JUNYENT adoptará medidas específicas contra el *hacking* o allanamiento informático, por ejemplo, con ánimo descriptivo, pero no exhaustivo, a través de la identificación y autentificación de usuarios y gestión de credenciales de usuarios, así como de todas aquellas medidas de seguridad, técnicas, organizativas o de gestión que puedan ser aplicables para garantizar la seguridad.

Medidas contra el fraude a través del correo electrónico

Los usuarios deberán tener en cuenta las siguientes medidas, para no ser presas de determinadas conductas de fraude que se pudieran dirigir contra la organización o contra terceros:

I. En el caso que un Cliente, Proveedor o cualquier tercero con el que se tenga relación informe a una persona trabajadora de GRUPO ROCA JUNYENT sobre el cambio de cuenta bancaria a la que realizar transferencias o cualquier otro tipo de operación de carácter económico, dicha persona trabajadora pedirá que se le mande una confirmación por correo electrónico, con copia a su superior jerárquico.

II. Cuando una persona trabajadora de GRUPO ROCA JUNYENT solicite una transferencia u otra operación económica vinculada a una cuenta distinta de las habituales, deberá poner en copia a su superior jerárquico. Por otra parte, se informará previamente a Clientes, Proveedores y terceros que las transacciones realizadas a cuentas bancarias de GRUPO ROCA JUNYENT distintas de las habituales han de confirmarse por correo electrónico a quién solicita la transferencia, con copia a su superior jerárquico.

Propiedad intelectual

En cumplimiento de la normativa sobre propiedad intelectual, GRUPO ROCA JUNYENT adoptará los controles específicos necesarios para evitar eventuales infracciones de derechos de autor.

A título de ejemplo, GRUPO ROCA JUNYENT estará facultado para realizar los siguientes controles:

I. Revisar los terminales mediante programas de auditoría de red o de puesto de trabajo.
II. Realizar inventarios de licencias de uso.

III. Elaborar listas de programas homologados.

IV. Velar por la correlación entre las licencias existentes y los programas instalados.

V. Verificar el control de contenidos y bases de datos.

10. Régimen disciplinario

Los usuarios serán susceptibles de medidas disciplinarias si incurren en infracciones determinadas por este orden:

- El convenio de oficinas y despachos a nivel autonómico.
- Real Decreto 1331/2006, de 17 de noviembre, por lo que se regula la relación laboral de carácter especial de los abogados que prestan servicios en despachos de abogados, individuales o colectivos.
- Estatuto de los trabajadores.
- Políticas internas y protocolos del GRUPO ROCA JUNYENT
- Si la conducta realizada por el usuario está tipificada en el Código Penal o en cualquier otra ley complementaria, y en consecuencia es constitutiva de delito, se pondrá en conocimiento de las autoridades competentes a fin de que procedan de acuerdo con lo establecido en la legislación vigente.
- Así mismo, el incumplimiento de este protocolo comportará de forma preventiva, la inmediata suspensión del servicio prestado y/o el bloqueo temporal de sistemas, cuentas o acceso a la red con el fin de garantizar su buen funcionamiento.

En todo caso, si la conducta realizada por el miembro ha causado algún daño o perjuicio al Grupo mercantil, a otros usuarios o a cualquier persona o entidad, el miembro deberá indemnizar a los perjudicados por el importe del daño o perjuicio causado.

Aprobado por el Consejo de Administración de ROCA JUNYENT, S.L.P. el 26 de octubre de 2024.