PROTOCOLO DE USO DE DISPOSITIVOS

GRUPO ACRISMATIC

PROTOCOLO DE USO DE DISPOSITIVOS

CONTROL DE CAMBIOS					
Revisión	**Fecha**	**Sección afectada**	**Realizado**	**Revisado**	**Aprobado**
0.1	22.12.2022		Cuatrecasas	E. Mateu	
	13.06.2023				C.Officer

ÍNDICE DE CONTENIDOS

1. CONSIDERACIONES DE CARÁCTER GENERAL

El objetivo principal de este protocolo es garantizar que las personas que hagan uso de los dispositivos tecnológicos de GRUPO ACRISMATIC lo hagan de forma adecuada, responsable y lícita, protegiendo la información del Grupo, de sus empleados, proveedores y clientes, cumpliendo la ley respecto a seguridad y protección de datos personales.

Mediante la aplicación de lo contenido en este Protocolo se consigue que en el Grupo se trabaje con eficiencia y productividad, evitando un uso inadecuado de los mismos que genere daños para la entidad que pueden llegar a ser de extrema gravedad, incluyendo responsabilidades penales para la propia sociedad.

Mediante un correcto uso de los dispositivos tecnológicos **se consigue:**

✓ Atender las necesidades del Grupo garantizando la productividad mediante el aprovechamiento del tiempo de trabajo.

✓ Establecer controles para evitar que se utilicen los dispositivos tecnológicos para incurrir en **conductas particularmente prohibidas recogidas en el ANEXO A** de este Protocolo**.**

✓ Verificar el correcto cumplimiento de las obligaciones de los usuarios, poner fin a las conductas prohibidas y sancionar a los usuarios que hayan incurrido en las mismas.

El término **"usuario"** o **"usuarios",** utilizado a lo largo del presente Protocolo, comprende a cualquier persona autorizado a usar los dispositivos tecnológicos del Grupo.

Entre los dispositivos tecnológicos se incluyen:

- Equipos, servidores de aplicaciones, terminales de acceso remoto, ordenadores de mesa o portátiles, PDAs, tabletas, faxes y dispositivos similares o equivalentes.
- Cualquier aplicación o programa de software, redes y sistemas.
- Servicios de Internet y correo electrónico.
- Las cuentas que dan acceso al uso de hardware, software y sistemas de información.
- Teléfonos fijos, teléfonos móviles, tablets, blackberries GPS, etc.

Debe entenderse comprendido en lo anterior cualquier otro elemento o innovación tecnológica que pueda adquirir el Grupo.

El presente Protocolo es de obligado cumplimiento para todos los usuarios y por ello será entregado a cada uno de los usuarios, debiendo leer atentamente su contenido y firmar el pleno conocimiento del mismo.

Para resolver cualquier consulta que se pueda plantear sobre lo contenido en este Protocolo podrán dirigirse al Departamento de Informática, superior jerárquico o al Compliance Officer si fuera necesario.

2. REGLAS DE USO DE LOS DISPOSITIVOS TECNOLÓGICOS

- Los dispositivos tecnológicos son herramientas de trabajo, debiendo ser utilizados únicamente para el desarrollo de sus actividades profesionales y evitando su uso particular, salvo de forma excepcional y justificada.

- Los usuarios son conocedores de la existencia de las **medidas y medios de control** por el Grupo del uso de los dispositivos tecnológicos para verificar el correcto cumplimiento de la prestación laboral y el uso que se les da a las herramientas tecnológicas, siempre de conformidad con los principios de legitimidad, oportunidad y proporcionalidad.

- El uso de los dispositivos tecnológicos **está sujeto a posible control y por ello no existen expectativas de intimidad, confidencialidad y secreto de comunicaciones** aun cuando estén haciendo un uso ajeno a lo profesional.

- En particular, los usuarios han de tener presente que **los correos y otras comunicaciones electrónicas se consideran documentación del Grupo, y por tanto propiedad de ésta**. En este sentido, los citados materiales pueden ser: (i) objeto de los requerimientos y peticiones de información de los órganos de seguridad, (ii) relevantes para las investigaciones internas realizadas por el Grupo, o bien (iii) aportados en los litigios en los que el Grupo sea parte.

- El objeto del correo electrónico es facilitar la transmisión de información relacionada con el Grupo. Conviene tener presente que los correos, al igual que cualquier otro escrito, únicamente deben generarse cuando resulte necesario, y que deben ser precisos, completos y estar redactados con detenimiento y profesionalidad.

- Toda la información y/o documentos de trabajo que sean realizados en el ámbito del Grupo **deberán ser guardados en el servidor habilitado** al efecto, y solo excepcionalmente, previa autorización del responsable directo del Departamento, se almacenarán de forma local en los equipos.

- Queda **prohibido instalar, sin autorización del Departamento de Informática**, cualquier **programa o aplicación informática** a iniciativa propia del usuario, aun en el caso de que cuente con licencia o sea software libre.

- Queda **prohibido el acceso y uso de software no licenciado o "pirata"** (conducta ilícita que conlleva graves responsabilidades de tipo penal y civil, además de poner en riesgo evidente tanto los equipos informáticos como la información que contienen).

- **No se puede realizar ninguna acción de instalación y configuración**, **mantenimiento, reparación y destrucción sobre las aplicaciones** salvo autorización expresa del superior jerárquico o, en caso de duda, del Compliance Officer y, en todo caso, será el Departamento de Informática quien se encargue de ello.

- Para luchar contra códigos o programas maliciosos que tengan como objetivo infiltrarse en el ordenador sin conocimiento del usuario con la finalidad de dañar la seguridad de

esta máquina o de otros sistemas, se deberá **extremar las precauciones cuando utilice Internet o el correo electrónico**, evitando la apertura de correos, descarga o utilización de software o archivos de origen desconocido o no corporativo.

- Se deberá proceder al **análisis de los ordenadores** con el antivirus corporativo cuando sospeche de la existencia de código malicioso.

- Sé deberán **usar los mecanismos de seguridad** descritos en el **ANEXO B** del presente Protocolo para evitar el robo o pérdida de los dispositivos y/o de la información relacionada con la actividad empresarial.

- Para el correcto funcionamiento de los sistemas informáticos, habrán de observarse las pautas establecidas en el **ANEXO C** a la hora de crear una contraseña segura, sólida y que dificulte el descifrado, evitando así que usuarios no autorizados utilicen métodos manuales o herramientas automatizadas para adivinar las contraseñas.

- Estará **prohibido el uso del correo electrónico** para:

    i. Simular la pertenencia a una entidad distinta del Grupo.

    ii. Iniciar o participar en la propagación de cartas encadenadas o acciones análogas.

    iii. Utilizar buzones privados de correo ofrecidos por cualquier proveedor de Internet para fines profesionales relacionados con el Grupo.

    iv. Utilizar el correo electrónico como herramienta de comunicación con fines de venta u otros de naturaleza comercial independiente a los del Grupo.

    v. Enviar o solicitar mensajes, archivos o materiales con contenidos de carácter explícitamente sexual, de discriminación, que puedan llegar a ser ofensivos, difamatorios, amenazantes o insultantes para cualquier persona.

    vi. No se permite que los usuarios redireccionen automáticamente los correos recibidos en cuentas de correo corporativas a cuentas de correo no corporativas, y viceversa. Excepcionalmente, y siempre previa autorización del Compliance Officer, podrá hacerse, ocupándose el departamento informático de ejecutar dicho redireccionamiento.

    vii. Salvo causas justificadas (enfermedades, largos desplazamientos, etc.), y siempre previa y expresa autorización de los usuarios afectados, y con previa y expresa comunicación al Compliance Officer, ningún usuario podrá acceder a la cuenta de correo asignada a otro usuario.

- El **acceso a Internet** o a cualquier otra red de ordenadores se deberá realizar a través de las conexiones permitidas, habilitadas y configuradas por el responsable de Sistemas. Cualquier otra conexión diferente está terminantemente prohibida. Queda terminantemente **prohibido el uso de Internet** para:

i. Acceder, hablar o escribir en redes sociales, foros, chats o aplicaciones similares, salvo que exista una relación directa y demostrable con el desempeño de las funciones.

ii. Acceder a páginas web o sitios de Internet de contenidos pornográficos, xenófobos o destinados a fomentar o hacer apología de la violencia.

iii. Acceder o tratar de acceder a intranets o redes internas de competidores, clientes y/o proveedores (salvo, en los dos últimos casos, que se cuente con autorización de éstas previa, expresa y escrita al efecto).

iv. Descargar y/o instalar en los equipos software, ficheros ejecutables o bases de datos desde Internet. Si lo necesitara el usuario para el desempeño de sus funciones, deberá solicitar autorización al Responsable de su Departamento o, en su defecto, al Compliance Officer.

v. Utilizar software de descarga o intercambio de archivos o ficheros extremo a extremo (*Peer to Peer*) así como cualquier otro software de descarga de música, películas, vídeos y/o juegos o servicios de reproducción multimedia con fines de ocio.

vi. Enviar correos de carácter profesional o relacionados con el Grupo desde direcciones de correo privadas del usuario (cuentas Hotmail, Gmail o cualesquiera otras similares o análogas).

- Se debe usar los programas antivirus corporativos y sus actualizaciones, para prevenir que el material descargado desde Internet o facilitado por un tercero pueda destruir o corromper los datos informáticos. Quedando **expresamente prohibido**:

i. Intentar acceder, leer, borrar, copiar o modificar los archivos de otros usuarios sin el conocimiento y consentimiento de su autor, o en su caso, del Grupo.

ii. Intentar acceder a áreas restringidas de los sistemas informáticos del Grupo, de sus otros usuarios o de terceros.

iii. Destruir, alterar, inutilizar o dañar los datos, programas o documentos tecnológicos del Grupo, de sus otros usuarios, o de terceros.

iv. Intentar aumentar el nivel de privilegios de un usuario en el sistema.

v. Intentar descifrar las claves, sistemas, algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del Grupo.

vi. Obstaculizar voluntariamente el acceso de otros usuarios a los equipos y sistemas del Grupo, por el consumo masivo de los recursos informáticos y telemáticos, así como realizar acciones que dañen, interrumpan o generen errores en dichos equipos y sistemas.

vii. Introducir programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los recursos informáticos.

viii. Introducir, reproducir o distribuir programas informáticos no autorizados expresamente por el Grupo, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros.

ix. Poner a disposición de terceros no autorizados los equipos y el software suministrados por el Grupo.

- En lo que respecta a la **propiedad intelectual e industrial**:

  i. Se comprobará si de acuerdo con (i) las leyes nacionales internacionales y con (ii) las licencias y autorizaciones obtenidas por el Grupo, pueden efectivamente hacer uso de tal información. En caso de duda, los usuarios evitarán su uso y se pondrán en contacto con el Compliance Officer para ver si es posible la descarga y/o utilización respetando la normativa en materia de propiedad intelectual e industrial.

  ii. Salvo autorización del responsable del Departamento, queda prohibida la copia de programas, aplicaciones, documentos o cualquier tipo de material propiedad del Grupo en ordenadores o soportes privados.

- En referencia al **uso de teléfonos móviles:**

  i. La concesión de un dispositivo móvil será examinada individualmente. Lo solicitará el responsable directo de la persona que lo reciba, que evaluará la necesidad real para el desarrollo de la actividad profesional del empleado.

  ii. Todos los empleados que tengan derecho al uso de móviles corporativos, deben firmar la hoja de responsabilidad en el momento de la entrega y devolverlo al área que hace la entrega.

  En caso de robo o pérdida del dispositivo, el empleado deberá enviar de inmediato un correo electrónico al responsable de su departamento y una incidencia al Departamento de informática para el bloqueo del dispositivo y la línea. Una vez entregado el nuevo terminal al trabajador, éste recibirá instrucciones de uso del mismo nuevamente. A fin de justificar el robo, el trabajador debe siempre presentar denuncia ante la autoridad local competente, de lo contrario se procederá a aplicar el convenio en materia de régimen sancionador. En caso de que se pacte con el trabajador la asunción de la deuda generada por la pérdida del teléfono, las devoluciones de los importes de los dispositivos robados, perdidos o dañados serán hechas por el importe de la última factura de compra del mismo modelo.

  Se recuerda que el uso de los teléfonos móviles y tarjetas SIM corporativas se limitan al ámbito laboral o casos de urgencia. El empleado deberá cuidar el aparato y no hacer mal uso del mismo.

- En cuanto al uso de **ordenadores portátiles:**

  i. Todos los empleados que tengan derecho al uso de un ordenador portátil deben firmar el documento justificativo para la posesión de equipo en el momento de la

entrega. Este formato se entregará al Departamento de RRHH para su archivo en el expediente del empleado.

En caso de robo o pérdida del equipo, el empleado deberá notificar inmediatamente al responsable de su departamento y enviar una incidencia al Departamento de informática para que se ejecute la acción apropiada, y dará las instrucciones para recibir el nuevo portátil.

ii. Toda la información generada o instalada en el ordenador portátil corporativo será considerada como propiedad de la compañía y no del empleado que la ha creado.

El trabajador se compromete a:

- Trabajar desde el servidor de la empresa el cual hace diariamente copias de seguridad de la información.

- Cuidar y velar por la limpieza y el mantenimiento de los equipos.

- Mantener el portátil en un lugar seguro cuando esté en uso fuera de la oficina

3. COMUNICACIÓN DE INCIDENCIAS DE SEGURIDAD

El usuario afectado deberá comunicar de inmediato la incidencia a su superior jerárquico, quien a su vez pondrá en conocimiento del Departamento de Informática la incidencia acaecida para, en su caso, poder tomar las medidas oportunas al respecto. El superior jerárquico advertirá asimismo al Compliance Officer.

Tienen la consideración de incidencias de seguridad que afectan o pueden afectar al sistema informático del Grupo, entre otros los siguientes sucesos:

- Pérdida de contraseñas de acceso a los sistemas de información.

- Uso indebido de contraseñas.

- Acceso no autorizado por parte de un usuario del Grupo a algún fichero o documento al que no tiene permisos, excediendo así su perfil.

- Pérdida de soportes informáticos con datos de carácter personal.

- Pérdida de datos por mal uso de las aplicaciones informáticas.

- Ataques a la red.

- Infección de los sistemas de información por virus u otros elementos dañinos.

4. FINALIZACIÓN DE LA RELACIÓN CON EL USUARIO

Se le denegará el acceso a los dispositivos tecnológicos y deberá devolver cualesquiera de los que disponga a la finalización de la relación laboral del empleado por cualquier causa con el Grupo.

Se podrá **denegar el acceso a dichos dispositivos**, como medida cautelar, en los supuestos que legalmente procedan (por ejemplo, en caso de apertura de expediente contradictorio por comisión de falta muy grave por parte de un usuario que sea empleado del Grupo, si la naturaleza de la falta imputada guarda relación con las conductas prohibidas en este Protocolo).

5. CONFIDENCIALIDAD

El usuario conoce la naturaleza confidencial de los trabajos y operaciones que desarrolla en el desempeño de sus funciones en el Grupo.

Se deberá **guardar la máxima confidencialidad y secreto**, durante la vigencia de su relación y sin limitación temporal, incluso una vez extinguida su relación con el Grupo.

El usuario está obligado a **no revelar información** de cualquier naturaleza, obtenida como consecuencia de la relación mantenida con el Grupo, y en particular datos, resultados, planes, inversiones, análisis, proyectos, precios, objetivos, diseños, aplicaciones, métodos, procedimientos y fórmulas creados, y/o diseñados, y/o adquiridos, y/o utilizados por el Grupo en su actividad, información referida a la operativa de la empresa o cualquier especie de secreto empresarial de la misma (como por ejemplo, secretos e informaciones de carácter comercial, lo cual incluye todo lo que afecte a la organización interna y administración o funcionamiento de la empresa o a las relaciones entre la misma y cualquier tercero). En general, todos los conocimientos que tengan carácter no público.

Se deberá devolver la siguiente documentación en el momento en que un trabajador finaliza su relación con el Grupo, con independencia de la causa, haya sido o no dicha documentación clasificada como información confidencial[1]: todos los memorándums, listas, medios tecnológicos o magnéticos, archivos, listados de clientes, proveedores y empleados, correspondencia, documentos, material informático, listados de datos, códigos, diseños y dibujos, así como cualquier otro tipo de documento o material de cualquier naturaleza (y todas las copias de los mismos) realizados o compilados por el trabajador durante la vigencia de su relación con el Grupo.

6. FACULTAD DE VIGILANCIA DEL USO ADECUADO DE LOS DISPOSITIVOS TECNOLÓGICOS

El Grupo podrá acceder y controlar todos los dispositivos tecnológicos y el uso de los mismos, siempre de conformidad con la Ley aplicable en cada momento, con el fin de vigilar que se cumpla con lo previsto en este Protocolo y, en particular, de controlar debidamente que los usuarios no incurran en ilícitos penales (en particular, delitos contra la intimidad y allanamiento informático, tipificados en el artículo 197 del Código Penal), u otras conductas prohibidas en el presente Protocolo.

Las Medidas y métodos de control que practicará la empresa (el Compliance Officer, con apoyo técnico del Responsable de Informática o de la empresa con la que el Grupo

[1] El término "información confidencial", a los fines del presente Protocolo, comprenderá, pero sin limitarse a la misma, toda información obtenida del Grupo, que afecte a conocimientos o materias considerados como reservados, o que formen o hayan formado parte de las deliberaciones internas del Grupo, sin incluir hechos de general y público conocimiento.

tenga externalizados sus sistemas de información) se hará de conformidad con lo establecido en el procedimiento de Medidas y métodos de control que forma parte del *compliance* penal implementado en GRUPO ACRISMATIC.

ANEXO A. CONDUCTAS PARTICULARMENTE PROHIBIDAS

Se consideran conductas particularmente prohibidas las consistentes en:

- Acosar o discriminar.

- Revelar información confidencial o violar la normativa sobre protección de datos.

- Atentar contra la seguridad del Grupo y sus activos tangibles e intangibles (propiedad de bienes, derechos de propiedad intelectual e industrial, fondo comercial, reputación, buena imagen, etc.)

- Poner en riesgo la seguridad y la estabilidad de los equipos, los sistemas, o la información contenida en ellos.

- Realizar actos de competencia desleal contra el Grupo.

- Llevar a cabo conductas de violación de otros derechos de la empresa o de terceros.

- Incumplir los contratos o relaciones entre el Grupo y sus usuarios.

- Llevar a cabo conductas de transmisión, distribución, almacenamiento, descarga, instalación, copia, visión, envío o recepción de cualquier clase de contenidos ofensivos o discriminatorios especialmente si su posesión o utilización constituye una acción ilegal: esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, signos distintivos, secretos comerciales u otros derechos de propiedad intelectual o industrial utilizados sin la debida autorización.

- Atentar contra el buen honor e imagen del Grupo, de sus empleados o de terceros.

- Realizar cualquier otra conducta contraria al ordenamiento jurídico (incluidos ilícitos penales, administrativos, civiles…), al presente Protocolo, al Código Ético o a otro tipo de normativa interna vigente en el seno de la empresa).

ANEXO B. RECOMENDACIONES PARA USUARIOS DE DISPOSITIVOS TECNOLÓGICOS Y DE LAS MEDIDAS DE SEGURIDAD

1. Mantenimiento de equipos

Se deben realizar pequeñas operaciones de mantenimiento, para el correcto funcionamiento y el rendimiento óptimo de los equipos.

Se debe apagar completamente, al finalizar la prestación de servicios diaria, todo el equipamiento personal (CPU + Monitor + Periféricos) con el fin de ahorrar energía y alargar su vida útil.

2. Medidas de seguridad para los dispositivos portátiles

El usuario de dispositivos portátiles habrá de tener en cuenta las siguientes medidas de seguridad:

- No deberá exponer los dispositivos portátiles a cambios bruscos de temperatura, que degradarían su calidad y rendimiento.

- Deberá proteger los dispositivos portátiles del polvo, la suciedad y las exposiciones directas al sol.

- En ningún caso, deberá consumir bebidas o alimentos mientras esté usando dispositivos portátiles.

- Los dispositivos portátiles deberán mantenerse alejados del agua o de cualquier otro líquido conductor de la electricidad. Si, a pesar de todo, los citados dispositivos se mojasen, se deberá proceder, de inmediato, a apagarlos y desconectarlos, en su caso, de la toma eléctrica de red, ya que puede existir peligro de descarga.

- Deberá trasladar los dispositivos portátiles en bolsas o mochilas protegidas y bien cerradas durante su transporte.

- Deberá colocar los dispositivos fuera del alcance de imanes o de cualquier otra fuente de emisiones magnéticas.

3. Medidas de seguridad para viajar con dispositivos portátiles

Siempre que tenga que trasladar cualquier dispositivo portátil, el usuario debe tomar las siguientes medidas de seguridad:

- No se dejaran a la vista los dispositivos portátiles en coches u otros medios de transporte que resulten poco seguros.

- Mantendrá el dispositivo portátil consigo y no lo dejará abandonado o fuera de su tutela en ningún momento. Evitará facturarlo y, en caso de que se le obligue a hacerlo, deberá llevar consigo durante el viaje una copia de los datos albergados

en el dispositivo a transportar y preguntar al personal de la compañía de transporte si le pueden ofrecer alguna garantía o protección especial.

- En caso de pérdida o robo de un dispositivo portátil se debe informar de forma inmediata al responsable de los datos perdidos y al Compliance Officer para permitir que se puedan tomar las medidas oportunas para minimizar los posibles impactos.

ANEXO C. NORMAS Y RECOMENDACIONES DE USO DE CONTRASEÑAS

1. Normas de uso de contraseñas

- La contraseña es personal e intransferible, y por tanto no deberá ser revelada, ni por teléfono, ni por e-mail, ni a responsables ni a personal dependiente. Se deberá desconfiar de cualquier mensaje de correo electrónico en el que le soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla, pues casi con total seguridad se tratará de un fraude. El Grupo en ningún caso solicitará este tipo de información.

- No se debe hablar de las contraseñas en lugares comunes, donde exista facilidad de ser escuchado por terceras personas.

- En los periodos de vacaciones, la contraseña no debe ser compartida con ningún otro profesional.

- En caso de que una contraseña se encuentre comprometida o se piense que pueda estarlo, se debe proceder inmediatamente a cambiarla, aunque no se haya cumplido el plazo de caducidad.

- Las contraseñas nunca deben dejarse por escrito ni almacenadas en lugares en que pueda ser de fácil acceso a terceras personas.

- No utilizar la opción de "Guardar contraseña" para evitar reintroducirla en cada conexión.

2. Recomendaciones a la hora de introducir contraseñas

- Una contraseña segura debe contener, al menos, una variación de más de un carácter de los siguientes: mayúscula, minúscula, número, letra y símbolo.

- No deben utilizarse repeticiones de caracteres seguidos, ni de mayúsculas o minúsculas.

3. Normativa de construcción de contraseñas

- Salvo autorización expresa, o en el caso de usuarios compartidos, la duración máxima de la contraseña en el Grupo será de 3 meses.

- La longitud mínima de la contraseña será de ocho caracteres, utilizando obligatoriamente caracteres pertenecientes a tres de los cuatro grupos que se indican a continuación:

    - Letras mayúsculas
    - Letras minúsculas
    - Números
    - Símbolos

- El sistema almacenará una serie de contraseñas y, por tanto, al cambiar la contraseña no podrá reutilizarse una usada anteriormente.

- Para evitar ataques se bloqueará la cuenta cuando el sistema detecte que se intenta acceder al mismo utilizando un programa de generación de contraseñas,

- En caso de que la cuenta resultara bloqueada, el profesional deberá ponerse en contacto con el departamento autorizado para proceder a su desbloqueo.