

CONFIDENCIALIDAD Y USO DE HERRAMIENTAS INFORMÁTICAS



**FUNDACIÓN CANARIA PARA LA FORMACIÓN E
INSERCIÓN SOCIOLABORAL ATARETACO**

ECATAR CANARIAS, S.L.U.

ECOINSER CANARIAS, S.L.U.

SELECATAR, S.L.

Índice

1.	INTRODUCCIÓN.....	3
	INTRODUCCIÓN	3
	ÁMBITO DE APLICACIÓN	3
	VALORES.....	3
	OBLIGADO CUMPLIMIENTO.....	3
2.	INFORMACIÓN CONFIDENCIAL.....	4
	DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL	4
	PROTECCIÓN DE DATOS	4
3.	COMPROMISO DE CONFIDENCIALIDAD.....	6
	OBLIGACIONES DE CONFIDENCIALIDAD	6
	MEDIDAS DE SEGURIDAD.....	7
	NORMAS GENERALES.....	7
	USOS ESPECÍFICAMENTE PROHIBIDOS.....	9
	NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE INFORMACIÓN	10
	NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y MÓVILES	10
	USO DE MEMORIAS/LÁPICES USB (PENDRIVES)/TARJETAS SD O SIMILARES	11
	GRABACIÓN DE CDs Y DVDs O ANÁLOGOS	11
	IMPRESORAS EN RED, FOTOCOPIADORAS, FAXES U OTROS RECURSOS COMPARTIDOS.....	11
	DIGITALIZACIÓN DE DOCUMENTOS	12
	CUIDADO Y PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA	12
	PROTECCIÓN DE LA PROPIEDAD INTELECTUAL	12
	PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS.....	13
	SALIDA DE INFORMACIÓN POR MEDIOS ELECTRÓNICOS O ANÁLOGOS	13
	INCUMPLIMIENTO DE LAS OBLIGACIONES DE CONFIDENCIALIDAD.....	13
4.	USO DE HERRAMIENTAS INFORMÁTICAS Y REDES SOCIALES	14
	USO DE INTERNET, TELÉFONO Y CORREO ELECTRÓNICO	14
	USO DEL CORREO ELECTRÓNICO CORPORATIVO	14
	USO DEL ACCESO CORPORATIVO A INTERNET.....	15
	USO DE REDES SOCIALES	16
	INCUMPLIMIENTO O ABUSO DE HERRAMIENTAS INFORMÁTICAS.....	16

1. INTRODUCCIÓN

INTRODUCCIÓN

Con objeto de desarrollar y concretar las directrices de FUNDACIÓN CANARIA PARA LA FORMACIÓN E INSERCIÓN SOCIOLABORAL ATARETACO (G38370334), ECATAR CANARIAS, S.L.U. (B38807814), ECOINSER CANARIAS, S.L.U. (B76662923) Y SELECATAR SL (B38894465) (en adelante, ATARETACO) en lo referente al manejo de información y al uso de las tecnologías de la información y la comunicación, ATARETACO impone el cumplimiento de las siguientes obligaciones respecto al uso y acceso de información, las cuales deberán ser conocidas, aceptadas y respetadas.

ÁMBITO DE APLICACIÓN

La presente normativa interna es de aplicación a todas las personas empleadas, trabajadoras, colaboradoras de ATARETACO –sea cual fuere la modalidad de contratación de éstos o el empleador de los mismos- que tengan acceso a los datos contenidos en ficheros, sistemas de información y, en general, a cualquier información considerada como confidencial (en adelante, *las Personas*).

VALORES

La Política de *Uso de herramientas informáticas y Confidencialidad* de ATARETACO se basa en:

- Un comportamiento ético y conforme a la ley, en especial, con la normativa española de protección de datos.
- El respeto a la intimidad, la privacidad y al libre desarrollo de la personalidad.
- El cumplimiento de las normas que regulan el tratamiento de información y, en especial, evitar la comisión de delitos relacionados con tratamientos de información o uso de herramientas informáticas
- El respeto de los intereses de otras personas relacionadas con ATARETACO, incluidos clientes, proveedores, autoridades y la sociedad en general.

OBLIGADO CUMPLIMIENTO

Las personas comprendidas en el ámbito de aplicación del Código están obligadas a su cumplimiento, con respeto a los valores y principios que contiene y a seguir las pautas de comportamiento que establece. Todos las Personas de ATARETACO están obligadas a conocer esta normativa y a acatarla en base a lo previsto en el artículo 20.3 del Estatuto de los Trabajadores (*Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores*)

El incumplimiento de las previsiones de esta *Política Interna* podrá dar lugar a la comisión de las infracciones previstas en la normativa legal, laboral o en esta misma normativa interna. ATARETACO pondrá los medios necesarios para cumplir y hacer cumplir por los personas destinatarias del mismo lo previsto en esta normativa interna.

2. INFORMACIÓN CONFIDENCIAL

DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL

Tendrá la consideración de Información Confidencial toda la información de carácter económico, financiero, técnico, comercial, estratégico, administrativo o de otro tipo, que, en cualquier momento durante la vigencia de la relación profesional sea conocida o creada por las partes (ATARETACO y la personas que trabajan en la institución) en el marco de la ejecución de la prestación profesional o que le sea revelada por la otra parte de forma oral, escrita o en cualquier otro soporte, así como documentación de otro tipo, que haya sido clasificada como de propiedad exclusiva o confidencial o que, por su naturaleza o por las circunstancias en las que se produzca la revelación o creación, debe de buena fe estimarse como tal, incluyéndose aquí los datos de carácter personal a los que, en el desempeño de sus funciones dentro de ATARETACO, se tenga acceso.

PROTECCIÓN DE DATOS

DATOS A LOS QUE SE ACCEDA POR LA RELACIÓN CONTRACTUAL

Toda Persona que en desarrollo de su trabajo recabe datos de carácter personal de clientes, proveedores, otras empleadas o terceras en general para su incorporación a un fichero automatizado o papel, deberá hacerlo acorde con las directrices dispuestas por ATARETACO y por la normativa de Protección de Datos a la que deberá ajustarse en todo caso. Son actos prohibidos:

- Hacer uso de la información, que contenga datos personales con finalidades distintas al objeto de su tratamiento.
- Cualquier otra actividad expresamente prohibida en este documento o en las normas sobre protección de datos e Instrucciones de la Agencia de protección de Datos.
- Hacer uso de la información a la que se acceda con motivo del desempeño del puesto de trabajo fuera del entorno profesional.

INFORMACIÓN SOBRE EL USO DE LOS DATOS DE TRABAJADORES/AS POR PARTE DE FUNDACIÓN CANARIA PARA LA FORMACIÓN E INSERCIÓN SOCIOLABORAL ATARETACO, ECATAR CANARIAS, S.L.U., ECOINSER CANARIAS, S.L.U. Y SELECTAR, S.L.

Las Personas conocen que los datos de carácter personal que ATARETACO recabe de sus empleados/as serán utilizados para la gestión de la relación laboral y que éstos, en cumplimiento de las obligaciones legales, pueden ser comunicados a la AEAT y a la TGSS. Todas las Personas podrán ejercitar sus derechos reconocidos en la normativa española de protección de datos.

ATARETACO tratará la información que faciliten las Personas a lo largo de la relación laboral con el único fin de gestionar dicha relación laboral. Los datos proporcionados se conservarán mientras se mantenga la relación laboral o durante los años necesarios para cumplir con las obligaciones legales. Las Personas pueden conocer más sobre el tratamiento de sus datos comunicándolo a la dirección.

3. COMPROMISO DE CONFIDENCIALIDAD

OBLIGACIONES DE CONFIDENCIALIDAD

El Trabajador se obliga a conservar y tratar con la máxima diligencia y confidencialidad toda la Información Confidencial y, en particular, a no revelar a ningún tercero, sin el consentimiento previo de ATARETACO. En especial, los Trabajadores que en el desempeño de sus funciones profesionales, accedan, usen y/o traten Información Confidencial, incluidos datos personales que traten por motivos profesionales o a los que accedan fruto de su relación laboral con ATARETACO, quedan obligados al cumplimiento de las siguientes obligaciones:

- a) Sólo tratarán y utilizará aquella Información Confidencial que sea necesaria para el desarrollo de las funciones profesionales propias del puesto que ocupa dentro de la estructura de ATARETACO.
- b) Seguir las instrucciones fijadas por ATARETACO, en todo lo que respecta al tratamiento de la Información Confidencial, no pudiendo utilizar y/o tratar dicha Información para fines distintos de los expresamente indicados.
- c) Cumplir con el deber de secreto respecto de la Información Confidencial a la que tenga o haya tenido acceso durante o como consecuencia del desempeño de las funciones profesionales en ATARETACO, teniendo dicho deber de secreto una duración indefinida, una vez extinguido el contrato.
- d) Tratar dicha Información confidencialmente, quedando expresamente prohibida cualquier tipo de comunicación, cesión, transferencia, almacenamiento, envío o entrega, no autorizadas expresamente, de cualquier Información Confidencial a la que tenga o haya tenido acceso en el desempeño de sus funciones profesionales, tanto en formato físico como en formato electrónico, ya sea a trabajadores de ATARETACO no autorizados para acceder a dichos datos, ya sea a terceros ajenos a la estructura organizativa de ATARETACO. Tampoco podrá grabar Información Confidencial en cualquier soporte, ni imprimirlos o extraerlos fuera de las dependencias físicas donde desarrolle sus funciones profesionales sin que exista justificación.
- e) Adoptar las medidas necesarias para evitar que terceros no autorizados puedan acceder a Información Confidencial y a limitar el acceso a tales elementos a los empleados autorizados que precisen disponer de ella para la ejecución de su trabajo, trasladándoles idéntica obligación de confidencialidad.
- f) En cumplimiento del deber de secreto profesional, los Trabajadores sólo podrán usar los datos relativos a la relación de ATARETACO con sus clientes a los que accedan por motivo de su relación laboral con fines profesionales dentro de sus funciones, absteniéndose de comunicar a terceras personas o empresas datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso.

- g) Ningún Trabajador deberá poseer, para usos no propios de su responsabilidad profesional, ningún material o información propiedad de ATARETACO, tanto ahora como en el futuro.

El uso de Información Confidencial contrario a lo establecido en esta Normativa y, en especial, de aquella que contenga datos de carácter personal, podrá devenir en sanciones internas, reservándose, además, ATARETACO las acciones judiciales (civiles, penales o de otro orden) oportunas. El Trabajador conoce que las prácticas contrarias a lo establecido en esta Normativa pueden ser consideradas, entre otras, como delitos tipificados en Código Penal de revelación de secretos, o relativos al mercado y a los consumidores e, incluso, contraria a lo establecido en la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

MEDIDAS DE SEGURIDAD

- ATARETACO facilita a los usuarios que así lo precisen, si se considerase necesario para el desempeño de sus funciones, los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que ATARETACO pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.
- En general, el ordenador personal será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos de ATARETACO, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.
- Este epígrafe concierne específicamente a todos los ordenadores personales facilitados y configurados por ATARETACO para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

NORMAS GENERALES

- Los equipos informáticos serán asignados por ATARETACO.
- Existirá un inventario actualizado de los equipos informáticos.
- A cada nuevo usuario que se incorpore a la organización y así lo precise, ATARETACO le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales.
- Los ordenadores personales deberán utilizarse únicamente para fines profesionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

- Únicamente el personal autorizado por ATARETACO podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de ATARETACO. Cuando se precise instalar dispositivos no provistos por ATARETACO deberá solicitarse autorización previa.
- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa de ATARETACO. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
- Salvo autorización expresa de ATARETACO, los usuarios no tendrán privilegio de administración sobre los equipos.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
- Los usuarios deberán notificar, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.
- Salvo aquellos ordenadores instalados en las zonas comunes de acceso a Internet, cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su correcto uso.
- El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta a ATARETACO de tales circunstancias.
- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
- El usuario será responsable de toda la información extraída fuera de la organización bien a través de dispositivos tales como memorias USB, etc., bien a través de servicios de almacenamiento de datos en nubes o sistemas similares. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.
- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata a ATARETACO, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por ATARETACO estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.
- Los Trabajadores que tengan acceso a Información Confidencial para su actividad, están en la obligación de la custodia de los mismos, así como a informar a su responsable de las incidencias que puedan ocurrir durante su tratamiento.

- Todos los documentos que sean impresos y que contengan datos de carácter personal, su retirada de las bandejas de las impresoras o fotocopiadoras, es responsabilidad de la persona que realiza dichos procesos, la pérdida o extravíos de estos documentos puede acarrear medidas de carácter disciplinarias o administrativas según correspondan.
- Toda documentación a la que tenga acceso, que contenga datos de carácter personal y que no sea necesaria su conservación, está en la obligación de destruirla, de forma tal que imposibilite la obtención de dichos datos. Los documentos en papel que contengan datos de carácter personal no pueden ser reutilizados, al menos, que se garantice su custodia y posterior destrucción una vez no sean necesarios.
- Las mesas/despachos de los Trabajadores, que contengan carpetas o documentos con datos de carácter personal, deben tener los mecanismos de control necesarios que permitan su recogida, almacenamiento y custodia una vez que abandonen el puesto, o concluya su jornada laboral.
- El Trabajador debe velar constantemente por la privacidad de los datos contenidos en los documentos, tomando las medidas necesarias para evitar que puedan ser leídos o vistos por persona ajena no autorizada, cumpliendo con el deber de secreto.
- Los documentos en papel deben estar colocados de forma ordenada en lugares adecuados para su conservación, localización y acceso permitiendo garantizar de forma eficiente su localización con el objeto de cumplir los plazos en el ejercicio de los Derechos de los Afectados.
- Las personas que manejen documentos que se encuentren en proceso de revisión, modificación o tramitación -ya sea previo o posterior a su archivo- deberán custodiarlos e impedir en todo momento que puedan ser accedidos por personas no autorizadas.

USOS ESPECÍFICAMENTE PROHIBIDOS

Están terminantemente prohibidos los siguientes comportamientos:

- Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el Trabajador sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del responsable del sistema, con el fin de que le asigne una nueva clave. Ante una baja o ausencia temporal del usuario, el responsable del departamento podrá solicitar al responsable del sistema la cesión de clave o datos a la persona por él designada.
- Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, vídeo, animaciones, etc.)
- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por ATARETACO, sin la previa autorización.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por ATARETACO.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa de ATARETACO.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE INFORMACIÓN

- Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.
- ATARETACO puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso limitado y compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa de ATARETACO.

NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y MÓVILES

- Los equipos portátiles y móviles serán asignados por ATARETACO.
- Existirá un inventario actualizado de los equipos portátiles y móviles. ATARETACO gestionará dicho inventario.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable de ATARETACO. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de ATARETACO para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de ATARETACO.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a ATARETACO o no autorizadas para ello.
- En general, los equipos portátiles no deberán conectarse directamente a redes externas (incluyendo la red o el acceso a Internet del usuario en su domicilio). ATARETACO puede proporcionar accesos remotos autorizados y configurados por ATARETACO a través de tarjetas móviles. Cuando este sea el caso, deberán realizar de forma obligatoria dicha conexión cuando requieran el acceso a Internet desde dichos equipos. En casos debidamente justificados y previamente autorizados por ATARETACO se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente Normativa General que resulten de aplicación.
- Los usuarios de equipos portátiles deberán seguir las instrucciones proporcionadas por ATARETACO, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.
- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada

fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).

- Como norma general, los equipos portátiles se configurarán por defecto con todos los canales, puertos y sistemas de comunicaciones de salida de información bloqueados (WiFi, Bluetooth, USB's, CD, DVD, tarjetas de red, etc.). Por petición justificada dirigida a ATARETACO, se podrán habilitar algunas o todas las funciones de salida de información.
- Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá a ATARETACO llevar a cabo estas modificaciones.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá a ATARETACO, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

USO DE MEMORIAS/LÁPICES USB (PENDRIVES)/TARJETAS SD O SIMILARES

- Con carácter general, el uso de memorias USB en ATARETACO no está autorizado. En su caso, la autorización deberá proporcionarla ATARETACO.
- Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización.
- En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por ATARETACO, que serán conformes a las normas de seguridad de la organización. Estas memorias USB serán de uso exclusivo en los puestos de usuario de ATARETACO, no debiendo ser usados fuera de éstos.
- Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. ATARETACO podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas de ATARETACO unidades de almacenamiento en red, que podrán usarse para tal propósito.
- La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento de ATARETACO, de forma inmediata.

GRABACIÓN DE CDs Y DVDs O ANÁLOGOS

- Con carácter general, el uso de equipos grabadores de CDs y DVDs en ATARETACO no está autorizado. En su caso, la autorización deberá proporcionarla ATARETACO.
- Por razones de seguridad, los equipos grabadores de CDs y DVDs de los puestos de trabajo podrán estar deshabilitados. En el caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y por ATARETACO.

IMPRESORAS EN RED, FOTOCOPIADORAS, FAXES U OTROS RECURSOS COMPARTIDOS

- Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer

uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por ATARETACO y, en su consecuencia, estén debidamente inventariados.

- Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.
- Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de ATARETACO.
- Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización precisa.
 - Dependiendo de la tipología de la información hallada, podrá abrirse el correspondiente incidente de seguridad.

DIGITALIZACIÓN DE DOCUMENTOS

- Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.
- Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento de ATARETACO

CUIDADO Y PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA

- La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.
- Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de ATARETACO, de forma que no sea recuperable la información que pudieran contener.
- Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.
- Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

- Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de ATARETACO sin la correspondiente licencia de uso.

- Los programas informáticos propiedad de ATARETACO o licenciados a ATARETACO están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa de ATARETACO.
- Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización de ATARETACO.

PROTECCIÓN DE LA DIGNIDAD DE LAS PERSONAS

Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

SALIDA DE INFORMACIÓN POR MEDIOS ELECTRÓNICOS O ANÁLOGOS

- Es contrario a lo establecido en la empresa el uso de servicios de almacenamiento de información en la nube sin la previa autorización de la dirección, salvo aquellos almacenamientos que se produzcan en una red corporativa.
- Salvo la existencia de una legitimación para ello, tal como el desempeño de la funciones y obligaciones asignadas al personal, queda expresamente prohibido la salida de información por medios electrónicos o análogos, a título indicativo no limitativo, correo electrónico, sea o no corporativo, servicios de almacenamiento de información online o similares.

INCUMPLIMIENTO DE LAS OBLIGACIONES DE CONFIDENCIALIDAD

El incumplimiento por parte del Trabajador de cualesquiera de los términos, condiciones y obligaciones de la presente comunicación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y ss. o un delito contra el mercado y los consumidores tipificado en los artículos 278 y ss. del Código Penal, y determinará la responsabilidad de aquel frente a todas las demandas, acciones y/o reclamaciones que contra ATARETACO puedan dirigirse o ejercitarse.

Dicho incumplimiento será calificado como una falta muy grave, pudiendo sancionarse en consecuencia de conformidad con las normas legales de aplicación.

4. USO DE HERRAMIENTAS INFORMÁTICAS Y REDES SOCIALES

USO DE INTERNET, TELÉFONO Y CORREO ELECTRÓNICO

ATARETACO pone en conocimiento de todos sus Trabajadores que el acceso al ordenador personal, a la red corporativa, a Internet, el uso de las líneas de teléfono y el servicio de correo electrónico son medios proporcionados como herramientas de trabajo y que estarán sujetas a los controles internos previsto que garanticen su correcta explotación y el uso adecuado del servicio, por lo que se reserva el derecho de controlar y, en los casos que considere necesario, inspeccionar sus contenidos. La utilización de este medio en contra de los intereses de ATARETACO originará las acciones y las sanciones correspondientes.

La navegación a través de Internet debe estar dirigida a aquellos sitios que sean necesarios para el cumplimiento de las labores propias de ATARETACO, por lo que se reserva el derecho de controlar el uso de la misma, así como de establecer los mecanismos que impidan la libre navegación.

La monitorización de dichos contenidos se hará con el máximo respeto a la intimidad y a la vida privada del trabajador.

USO DEL CORREO ELECTRÓNICO CORPORATIVO

- Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.
- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por ATARETACO.
- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.
- Se deberá notificar a través del canal de información cualquier tipo de anomalía detectada.
- Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia a través del canal de información.
- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.
- Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones

Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código

malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.

- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.
- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.
- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.
- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida.
- La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a ATARETACO o el reenvío automático del correo corporativo a buzones ajenos a la organización. Para ello se necesitará la autorización expresa a través del canal de información.

USO DEL ACCESO CORPORATIVO A INTERNET

El acceso corporativo a Internet es un recurso centralizado que ATARETACO pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

ATARETACO velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

- El acceso a Internet deberá ser autorizado a través del canal de información, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.
- Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
- Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por ATARETACO en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización a través del canal de información
- Deberá notificarse a través del canal de información cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

Quedan prohibidas las siguientes actuaciones:

- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.
- La descarga de programas informáticos sin la autorización previa a través del canal de información o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.

- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada a través del canal de información.

USO DE REDES SOCIALES

Es potestad de ATARETACO el uso de redes sociales para su promoción, información o con cualquier otra finalidad.

Queda prohibido el uso de imágenes, logos o información de ATARETACO en las redes sociales, incluso cuando éstas se hagan de forma privada. El uso de imágenes, logos o información de ATARETACO pueden constituir delitos contra la privacidad, contra la propiedad intelectual o de revelación de secretos, entre otros.

INCUMPLIMIENTO O ABUSO DE HERRAMIENTAS INFORMÁTICAS

El uso contrario a los principios establecidos en esta política puede constituir delitos tipificados en el Código Penal y determinará la responsabilidad de aquel frente a todas las demandas, acciones y/o reclamaciones que contra ATARETACO puedan dirigirse o ejercitarse.

El incumplimiento de lo previsto en este apartado será calificado como una falta muy grave, pudiendo sancionarse en consecuencia de conformidad con las normas legales de aplicación.