Normas de uso de los recursos TIC y Seguridad

Métodos y Tecnología de Sistemas
y Procesos S. L. (MTP)

Versión 1.3
09/09/2019

Realizado por:	Revisado por:	Aprobado por:
Damián Fernandez	Comité de Seguridad	Mamdouh El Cuera (CEO)

CONTROL DE VERSIONES

Versión y Fecha	Escrito por Revisado por Aprobado por	Razón del cambio	Secciones cambiadas
Versión 1.0 12/08/2016	Responsable de Seguridad Comité de seguridad Juan Manuel Ferrer Cuesta Comité del Sistema de Gestión	Versión Inicial	
Versión 1.1 17/05/2018	Responsable de Seguridad Comité de seguridad Juan Manuel Ferrer Cuesta Comité del Sistema de Gestión	Cambio de nombre y unificación del documento de seguridad y políticas	
Versión 1.2 08/10/2018	Responsable de Seguridad Comité de seguridad Mamdouh El Cuera	Adecuación RGPD	
Versión 1.3 09/09/2019	Responsable de Seguridad Comité de seguridad Mamdouh El Cuera	Software (no) autorizado	Punto 15

ÍNDICE

1. INTRODUCCIÓN

Este documento contiene las normas y procedimientos que deben ser aplicados en el uso de los recursos de tecnologías de la información (a partir de aquí "recursos TIC") de Métodos y Tecnología de Sistemas y Procesos SL (a partir de aquí "MTP") y son de obligado cumplimiento. Se entenderá por recursos TIC los elementos identificados como tal, incluyendo entre otros: hardware, software, red corporativa, correo electrónico, sistemas de comunicación, acceso a Internet, etc

2. OBJETIVO

2.1. OBJETIVOS GENERALES

Estas normas tienen como objetivo cumplir la obligación establecida en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal relativa a la necesidad de disponer de un documento en el que se establezcan las obligaciones de los usuarios en materia de seguridad y uso de los sistemas informáticos. Asimismo, estas normas derivan de las obligaciones del control establecidas en el **artículo 31 bis del Código penal español** y reconocidas en el **artículo 20 del Estatuto de los Trabajadores**. De igual forma, emanan de los principios y obligaciones recogidas en la **política de seguridad de MTP**.

2.2. OBJETIVOS ESPECÍFICOS

Son también objetivo de estas normas:

- Cumplir el marco legal vigente.
- Aplicar al uso de los Sistemas de Información de MTP las funciones de vigilancia y control establecidas en el artículo 20.3 del Estatuto de los trabajadores y de la política de seguridad de MTP.
- Garantizar la seguridad de los sistemas.
- Proteger los datos personales que en ellos se encuentren.
- Proteger la intimidad y la dignidad de los trabajadores, así como el resultado de su trabajo.
- Proteger la información confidencial de MTP o de nuestros clientes.
- Proteger los activos de MTP.
- Proteger los Sistemas de Información de MTP.
- Garantizar la continuidad del trabajo en caso de ausencia o baja del trabajador.
- Prevenir supuestos de responsabilidad civil o penal de la empresa y sus directivos.
- Prevenir eventuales acciones judiciales.
- Informar a los usuarios de cuáles son las prácticas adecuadas y no adecuadas en el uso de los Sistemas de Información de MTP.

3. DEFINICIONES

A los efectos de este documento, las definiciones, expresiones y convenciones utilizadas a lo largo del mismo han de ser entendidos en el sentido indicado en el documento

4. ÁMBITO DE APLICACIÓN

El ámbito de aplicación de estas normas se extiende a los activos y/o recursos de MTP.

4.1. PERSONAS FÍSICAS Y JURÍDICAS

Estas normas son aplicables a todos los usuarios de los Sistemas de Información de MTP, con acceso a dichos Sistemas de Información propiedad de MTP.

4.2. EXCEPCIONES

De forma temporal o continuada seguridad informática podrá establecer excepciones a la aplicación de algunos puntos de estas normas y cursar autorizaciones temporales para el desarrollo de actividades que exijan un nivel de seguridad distinto al previsto en estas normas.

5. VIGENCIA Y ACTUALIZACIÓN DE LAS NORMAS

En el transcurso de la relación con la Entidad, todos los usuarios de MTP autorizados tienen la obligación de cumplir con lo establecido en este documento, así como con lo establecido en la política y normas generales de seguridad establecidas en la política de seguridad de MTP (disponible en la Intranet de MTP), debiendo mantenerse informados y cumplir con cualquier modificación de las mismas. El incumplimiento de las mismas podrá ocasionar una acción disciplinaria e incluso el despido o la resolución contractual.

En el caso de la comisión de una acción ilícita, se procederá a su comunicación a las autoridades competentes o al inicio de las acciones legales que en Derecho correspondan.

La Entidad se reserva el derecho a actualizar y modificar este documento de acuerdo con los cambios legislativos, la evolución de los sistemas, de los procesos asociados y de la seguridad relacionada con los Sistemas de Información, siendo las actualizaciones y modificaciones debidamente puestas en conocimiento de los usuarios de MTP autorizados.

Tanto este documento como sus posteriores modificaciones, deberán ser firmada por los usuarios de MTP.

6. MODELO DE USO

MTP ha optado por un régimen de uso restringido y monitorizado de los Sistemas de Información basados en la autorización expresa para todos los Sistemas de Información.

Ello significa que cualquier uso personal que no se halle expresamente autorizado deberá entenderse prohibido y que toda la actividad desarrollada en la red corporativa podrá ser monitorizada.

En el caso de autorizarse el uso de los Sistemas de Información para fines personales, de forma temporal o continuada, dicha autorización se entenderá referida a un uso personal no reservado. Ello significa que el trabajador autorizado sólo podrá realizar gestiones y comunicaciones para fines particulares y rutinarios que no entren en la esfera de su intimidad. Dicho uso personal deberá tener en cuenta que toda la actividad desarrollada en la red corporativa y los ordenadores conectados a la misma podría ser monitorizada y por ende, conocida por los administradores de sistemas y los directivos de MTP, cuando exista un indicio de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de estas normas que comprometa la seguridad del sistema.

7. IDENTIFICACION y AUTENTIFICACION DE LOS USUARIOS

Se prevendrá el acceso no autorizado a los servicios de red para los usuarios que no hayan sido legitimados.

Se usarán métodos seguros de autenticación para conexiones externas por parte de usuario autorizados.

Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en la red.

La información transmitida a través de redes de telecomunicaciones se hará de forma segura.

Con relación a las contraseñas se habrán de observar las siguientes normas:

- La contraseña de acceso al sistema caducará a los 90 días.
- El usuario será el encargado de modificarla en el momento de realizar el primer acceso al sistema, ya que se le solicitará automáticamente, caso contrario, será el usuario el encargado de realizar dicho cambio.
- Se evitarán nombres comunes, números de matrículas de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.

- Las contraseñas usadas en cualquier sistema o servicio serán como mínimo de 6 caracteres, combinando letras, número y símbolos como ¡”·$%&/()=?¿.
- Se usarán reglas nemotécnicas para la generación de contraseñas. Ejemplo: Hoy es lunes, 10 de Marzo de 2010. Contraseña: Hel10dMd2.
- No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.
- Se debe bloquear el equipo cuando no vaya a ser usado, o usar mecanismos automáticos, no dejándolo nunca desatendido.
- Se seguirá una política de puesto de trabajo despejado y mesas limpias, no dejando información confidencial o privada a la vista.
- Si se sospecha que la contraseña es conocida por otros usuarios, se procederá a informar al departamento de sistemas para su revocación y sustitución por una nueva.
- Existe habilitado un mecanismo para que no se pueda reutilizar las últimas 3 contraseñas que se usaron en el sistema.
- El número de intentos fallidos permitido antes del bloqueo de la cuenta, es de 3

8. USO DE CREDENCIALES DE ACCESO A LOS SISTEMAS

El usuario no podrá comunicar ni compartir con otra persona el identificador de usuario, la clave de acceso al sistema y el factor de autenticación adicional que posea para acceder a los sistemas de MTP o de sus clientes, como por ejemplo el teléfono móvil para obtener la clave de acceso OTP, la tarjeta de acceso, el token físico, etc.,. MTP presumirá que la actividad desarrollada con dicho identificador y/o factor poseído, y clave de acceso se realiza por el trabajador titular de los mismos, asumiendo éste la responsabilidad laboral, civil o penal que pueda derivarse de su uso.

Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento de Seguridad Informática, y solicitar la creación de una nueva clave. De igual forma, si el elemento poseído como Smartcards, tokens, etc., ha sido sustraído o perdido, deberá también notificarlo a Seguridad Informática para revocar su modo de acceso.

En la gestión y uso de las contraseñas se han de seguir las pautas de uso indicado en la política de seguridad de MTP.

El usuario autorizado para realizar teletrabajo deberá aplicar medidas adicionales de seguridad en el lugar donde se encuentre ubicado el equipo, para garantizar un nivel de confidencialidad similar al de las oficinas de la firma.

Los usuarios que accedan a los servidores de MTP a través de la VPN o de cualquier otro sistema de conexión remota, deberán tener especial cautela. Deberán seguir las normas establecidas en la política de seguridad de MTP en relación a este modo de acceso.

En caso de ausencia temporal, vacaciones, baja laboral, etc., del trabajador, y por motivos justificados el director del departamento podrá decidir seguir el protocolo de intervención del puesto de trabajo.

El uso, por parte de los usuarios, de los Sistemas de Información de MTP supone aceptar expresamente, que las personas designadas por MTP a tal efecto, puedan acceder a sus documentos de trabajo, ordenador, directorios del servidor y correo electrónico con la finalidad de garantizar la continuidad del trabajo.

9. ACTUACIONES PROHIBIDAS

El usuario está obligado a utilizar los Sistemas de Información de MTP y sus datos sin incurrir en actividades que puedan ser consideradas contrarias a la normativa vigente o bien infrinjan los derechos de MTP, clientes, de otros trabajadores y/o usuarios.

Están expresamente prohibidas las siguientes actividades:

- Compartir o facilitar el identificador de usuario y la clave de acceso a los Sistemas de Información de MTP a otra persona física o jurídica, incluido el personal de la propia empresa. Utilizar las claves de otros usuarios.
- Manipular o intentar modificar los ficheros LOG que registran la actividad del usuario o cualquier otro tipo de manipulación las claves y cualquier otro elemento de seguridad que intervenga en los procesos informáticos y telemáticos de MTP.
- Ocasionar daños total o parcialmente en los datos, programas o documentos electrónicos de MTP o de terceros.
- Las que deriven en ataques de denegación de servicio, difusión de virus o malware y a cualquier otra actividad de sabotaje de sistemas o potencialmente dañina.
- Introducir voluntariamente programas o ficheros del tipo que sean, que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de MTP o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos.
- Obstaculizar el acceso de otros usuarios a la red mediante el consumo masivo de los Sistemas de Información de MTP, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de MTP o de terceros.
- Intentar aumentar el nivel de privilegios propios o de otro usuario en el sistema.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la empresa, o cualquier otro tipo

de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.

- Instalar copias no autorizadas de cualquier programa.
- Borrar cualquiera de los programas (herramientas de seguridad, por ejemplo antivirus, firewall, etc.) instalados legalmente.
- Utilizar los Sistemas de Información de MTP, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario, salvo en el caso de que se cuente con autorización expresa para ello.
- Introducir contenidos obscenos u ofensivos y, en general, carentes de utilidad para los objetivos de MTP, en la red corporativa de MTP.
- Instalar puntos de acceso y redes inalámbricas no autorizadas (WiFi, bluetooth o similares).
- Acceder a redes inalámbricas (WiFi, bluetooth o similares) que no pertenezcan o estén administradas por la empresa sin la previa autorización de Seguridad Informática.
- Desactivar el salvapantallas que protege con contraseña el acceso no autorizado al ordenador del usuario cuando éste está encendido y el usuario se ausenta temporalmente de su puesto de trabajo.
- Desactivar el firewall, el sistema antivirus y los demás elementos de seguridad que protegen individualmente los ordenadores personales, especialmente los portátiles.
- Introducir en la red de MTP (pinchando en una toma de red) un PC sin autorización del Área Técnica de Sistemas y/o Seguridad Informática.

10. CONFIDENCIALIDAD DE LA INFORMACIÓN

El usuario no podrá enviar, sin la debida autorización, información confidencial de MTP al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación. Esta prohibición se extiende a la simple visualización presencial o remota de la información.

Los usuarios de los sistemas de información corporativos deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves y demás datos a los que tengan acceso durante su relación laboral con MTP, y empresas pertenecientes al Grupo, tanto en soporte material como electrónico. Esta obligación de reserva continuará vigente tras la extinción del contrato laboral.

En el caso que, por motivos directamente relacionados con el puesto de trabajo, el usuario entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello disminuya derecho alguno de posesión, o titularidad o copia sobre la referida información. Asimismo, el trabajador deberá devolver dichos materiales a la empresa, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral.

El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y dará derecho a la empresa a exigir al usuario una indemnización económica.

Sólo las personas autorizadas podrán atender a encuestadores y cumplimentar cuestionarios en los que se solicite cualquier tipo de información relativa a la empresa.

Queda prohibida la instalación de programas descargados de Internet u obtenidos de cualquier otra fuente no fiable por el riesgo de que pueda contener programas que permitan monitorizar de forma no autorizada la actividad del usuario y enviar al exterior de MTP información confidencial.

Para limitar al máximo el riesgo de pérdida de información confidencial, es obligatorio guardar la información en los sistemas habilitados para ello por MTP. Por el mismo motivo se prohíbe el uso de soportes, pen drive, discos duros portátiles y cualquier otro dispositivo móvil que pueda almacenar información, sin autorización de Seguridad Informática. Los soportes autorizados deberán estar inventariados por el Área Técnica de Sistemas.

11. USO DEL CORREO ELECTRÓNICO

Los Sistemas de Información utilizados por cada usuario son propiedad de MTP.

Ningún mensaje de correo electrónico será considerado como privado o personal. Se considerará correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas, y, especialmente, Internet. Todos estos mensajes y sus ficheros adjuntos irán abiertos, con excepción de aquéllos que contengan datos personales de nivel alto o que, por cuestiones de seguridad, deban ir cifrados. La autorización para cifrar los mensajes y los ficheros adjuntos corresponderá a Seguridad Informática.

La empresa se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa y los registros del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la empresa como responsable civil subsidiario. Esta revisión sólo podrá llevarse a cabo cuando exista una sospecha razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de estas normas que comprometa la seguridad del sistema.

Para garantizar el uso eficiente de los Sistemas de Información no deberán realizarse las siguientes actividades:

- Enviar ficheros adjuntos (attachments) con juegos, música, imágenes, vídeo o cualquier material que no esté relacionado con el trabajo.
- Enviar mensajes con contenidos o ficheros adjuntos ofensivos o inapropiados que vayan en contra del Código de Ético de MTP.

- Enviar o reenviar mensajes de correo en cadena o de tipo piramidal (chain letters).
- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento expreso del destinatario (Spam).

El trabajador tampoco podrá acceder, leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin previa autorización. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).

Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial, control de virus, phishing y pharming.

Es responsabilidad del usuario mantener la base de datos de correo del servidor, borrando los correos antiguos y aquellos no indispensables. La información que deba ser conservada se guardará en los soportes establecidos para ello por el Área de Sistemas.

La transmisión de datos de carácter personal de nivel alto (como los datos de salud), o los datos de MTP, o de sus clientes, clasificados como confidenciales, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Antes de enviar un mensaje de correo electrónico, el remitente debe tener en cuenta que su contenido podrá ser utilizado como prueba por el destinatario en caso de reclamación.

No se deben reenviar mensajes ni documentos corporativos a cuentas privadas del trabajador o de sus familiares o amigos, ya que éstas no gozan del mismo nivel de seguridad. Tampoco se puede configurar la cuenta de correo corporativo para reenviar los mensajes recibidos a una cuenta de correo electrónico privada.

12. ACCESO A INTERNET

El uso de los sistemas de información de MTP para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de MTP y los cometidos del puesto de trabajo del usuario, salvo en el caso de que se cuente con autorización expresa para ello.

El acceso a debates en tiempo real (Chat-IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido. Igualmente está prohibido el uso de sistemas de mensajería instantánea como el Messenger, y la instalación de programas

que permitan el acceso a redes P2P (Peer to Peer), así como cualquier otro tipo de acceso a entornos o plataformas como redes sociales, que permitan el intercambio de ficheros sin la previa autorización de seguridad informática. Este tipo de programas pueden ayudar a superar los sistemas de defensa ante accesos no autorizados y son un canal de entrada de virus y troyanos.

El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información y utilidades como FTP, etc. se limita a aquéllos que contengan información relacionada con la actividad de MTP o con los cometidos del puesto de trabajo del usuario, salvo en el caso de que se cuente con autorización expresa para ello de su Responsable. MTP podrá establecer filtros para garantizar el cumplimiento de esta obligación.

Si un usuario precisa estas herramientas para un uso profesional justificado, deberá solicitar que se habilite técnicamente un acceso temporal a Internet para poder utilizarlas, con excepción de los programas P2P, que no podrán ser utilizados en ningún caso, debido a su especial riesgo.

La empresa se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa. Esta revisión sólo podrá llevarse a cabo cuando exista una sospecha razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de estas normas que comprometa la seguridad del sistema.

Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial, control de virus, phishing y pharming.

13. CONTROL Y MONITORIZACIÓN DE LAS COMUNICACIONES ELECTRÓNICAS

MTP vigilará el cumplimiento de estas normas de forma constante, registrando la actividad de la red corporativa, manteniendo estadísticas y patrones de uso y efectuando rastreos ocasionales del uso de Internet y del tráfico de correos electrónicos con el fin de evitar cualquier perjuicio derivado del incumplimiento de la presente norma. También podrá proceder a la revisión y monitorización de los Sistemas de Información de MTP, con la misma finalidad.

MTP puede comprobar en cualquier momento los Sistemas de Información de la firma y las comunicaciones electrónicas generadas tanto por motivos de negocio como por motivos personales en el ámbito de la legislación aplicable. Esto incluirá, aunque sin restringirse sólo a ello, el acceso y revisión de los contenidos de los servidores, cuentas de correo electrónico, discos duros, mensajes de texto, el sistema de telefonía, buzón de voz y registros de telefonía móvil.

Con los fines citados, el control puede incluir la monitorización y registro de:

- Navegación web: Navegación por la web utilizando los servicios y sistemas de MTP, incluida la URL (dirección web) a la que se accede, fecha, hora, duración del acceso, páginas visitadas y/o descargadas.
- E-mail: Cualquier mensaje (incluidos ficheros adjuntos) enviados o recibidos por o en los equipos de MTP. Los mensajes (incluidos ficheros adjuntos) enviados o recibidos pueden ser bloqueados a discreción del administrador del sistema cuando se considere que son demasiado grandes, o que pueden ser un mensaje de tipo spam u otro tipo de correo dañino que puedan interferir el funcionamiento de la red informática o que puedan ser considerados como amenazantes, molestos u ofensivos.

A continuación se relacionan los controles que de forma continuada, puntual o excepcional pueden ser aplicados a los Sistemas de Información de MTP, como por ejemplo:

- Control del contenido de los mensajes de correo electrónico.
- Control de remitentes y destinatarios de los mensajes de correo electrónico.
- Control del contenido del ordenador del trabajador.
- Control de las áreas privadas del servidor.
- Control de los logs y estadísticas de uso.
- Conservación de los logs durante un plazo determinado.
- Control del historial de navegación.
- Control de los patrones estadísticos de uso de los Sistemas de Información.
- Cámaras de videovigilancia.
- Registro de llamadas.
- Grabación de conversaciones telefónicas.
- Acceso a documentos de trabajo en caso de ausencia o baja del trabajador.
- Acceso al buzón de e-mail en caso de ausencia o baja del trabajador.
- Control especial previo al despido (Protocolo de despido).
- Control especial previo a la baja voluntaria (Protocolo de baja voluntaria).
- Medidas de seguridad y controles del Reglamento de la RGPD.
- Bloqueo de acceso a páginas web no autorizadas.
- Control del firewall.
- Control del Proxy.
- Herramientas de monitorización del sistema.
- Herramientas de creación de pistas de auditoría y evidencias.
- Servicio externo de forensic readyness.
- Perfiles estadísticos y patrones de conducta individualizados.
- Mensaje mensual con estadísticas individuales de consumo de recursos.
- Configuración de alertas ante patrones de uso o cambios sospechosos.
- Comprobación periódica del funcionamiento de las medidas de control.
- Otros controles que se consideren necesarios.

Todas estas actuaciones se realizarán cumpliendo con la normativa aplicable en cada momento, y con el máximo respeto a la dignidad del trabajador, de acuerdo con las facultades de vigilancia y control establecidas en el artículo 20.3 del Estatuto de los Trabajadores. Los controles automatizados se realizarán de forma continuada y sin restricciones. Los registros efectuados de forma manual sólo podrán llevarse a cabo cuando exista una sospecha razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de estas normas que comprometa la seguridad del sistema, o que pueda comportar riesgos o perjuicios para los activos protegidos descritos en estas normas.

El trabajador da su consentimiento expreso para que la empresa pueda acceder al contenido de su cuenta de correo electrónico, documentos de trabajo, historial de navegación por Internet, logs, contenido del disco duro y del servidor y a cualquier otra área pública o privada de los Sistemas de Información de la firma, en los supuestos, con el alcance y con las finalidades descritos en estas normas.

A estos efectos, la empresa dispone de los protocolos y procedimientos de actuación necesarios para asegurar que el acceso a la información no vulnerará, en ningún momento, la dignidad del usuario afectado por el control.

Del mismo modo, si los administradores de la red detectan un incumplimiento de estas normas están autorizados a comunicárselo al usuario así como al departamento de recursos humanos para que le den el curso apropiado.

MTP colaborará con las fuerzas y cuerpos de seguridad del Estado, informando o contestando a sus requerimientos de información sobre cualquier circunstancia que pueda ayudar a la investigación de un delito, una falta o una infracción administrativa.
La utilización de los Sistemas de Información de MTP presupone el conocimiento y la aceptación de las presentes normas.

14. SEGURIDAD FÍSICA Y DEL ENTORNO

Se prevendrá todo tipo de acceso físico no autorizado, daños o intromisiones en las instalaciones y en la información de MTP.

Se tomarán las medidas de seguridad necesarias para evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades de MTP.

No se dejarán puestas llaves en puertas, armarios o cajones ni se dejarán puertas o ventanas abiertas cuando no haya nadie en la oficina.

Los portátiles estarán asegurados físicamente a los puestos de trabajo mediante cables de seguridad, o sistemas equivalentes, siempre que estos equipos no estén bajo supervisión del usuario o personal a cargo del equipamiento, sea cual sea la ubicación del puesto de trabajo (empresa o cliente).

Si el aseguramiento físico no es viable, los portátiles serán llevados en todo momento con la persona asignada al uso del mismo, no dejándolos bajo ningún concepto en la oficina cuando dicha persona se ausente de la misma y esta quede vacía.

En caso de realizar teletrabajo, el empleado se asegurará de disponer de un entorno de trabajo adecuado y proteger los sistemas de los que es responsable.

15. PROPIEDAD INTELECTUAL E INDUSTRIAL

Queda establecido que toda la información que se genera, procesa y almacena en este sistema de información es propiedad de MTP.

Los usuarios son responsables de respetar los controles implantados y utilizar la información sólo con los fines para los que se les autorizó el acceso. El hecho de obtener acceso a cierta información, no les confiere el derecho alguno de dar acceso a otras personas ni a disponer de la misma de modo no autorizado.

Los usuarios prestarán toda su atención en proteger la información a la que tienen acceso en cualquiera de sus soportes presentados o generados (papel, soportes magnéticos…).

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial. MTP tiene una lista de aplicaciones informáticas y sistemas operativos, autorizados y licenciados para su instalación, ejecución y uso en los ordenadores y demás Sistemas de Información por parte de los usuarios.

El software licenciado a favor de MTP no puede ser instalado ni utilizado en ordenadores o dispositivos que no sean propiedad de MTP. Es decir, no se permite copiar software licenciado a favor de MTP en dispositivos informáticos personales, aunque el software vaya a emplearse para la actividad de MTP.

No deben emplearse los Sistemas de Información de MTP para descargar, copiar, alterar, modificar, mezclar o manipular ningún medio electrónico, datos o software que pudiera contravenir la legislación sobre derechos de la propiedad intelectual. La carga, descarga e intercambio no autorizados de software, música, cine y cualquier otro contenido digital a través de plataformas P2P (Peer to Peer) o cualquier otro medio de transmisión de datos a través de Internet constituye un delito contra la propiedad intelectual, por lo que el usuario no podrá realizar ninguno de dichos actos.

Deben respetarse los acuerdos y licencias de propiedad intelectual e industrial que la empresa tenga con terceros.

La empresa es la titular de los derechos de propiedad intelectual e industrial sobre las obras e invenciones creadas en el seno de la relación laboral o como fruto de una obra colectiva.

Listado de software autorizado por defecto:

Navegadores web: Chrome, Firefox
Compresores: 7-Zip
Ofimática: LibreOffice
Cliente SSH: Putty
Cliente FTP/SCP: WinSCP

Todo software no incluido en este listado deberá ser previamente autorizado por Sistemas mediante petición vía Helpdesk

16. INCIDENCIAS

Es obligación de todos los usuarios de MTP comunicar a seguridad informática cualquier incidencia que se produzca en los sistemas de información a que tengan acceso.

Dicha comunicación deberá realizarse inmediatamente y, en cualquier caso, en un plazo de tiempo no superior a una hora desde el momento en que se conozca dicha incidencia.

Toda incidencia en materia de seguridad deberá comunicarse, siguiendo el procedimiento establecido. Dicha notificación será realizada a través de:

- Utilizando la herramienta HelpDesk categorizando el registro como "Seguridad"
- El correo electrónico sistemas@mtp.es en caso de indisponibilidad de la herramienta anterior

En caso de incidencia grave o potencialmente grave, se utilizarán canales de comunicación adicionales a los anteriores que garantices el inmediato conocimiento de los implicados (por ejemplo el teléfono o buzones de correo adicionales).

El usuario que detecte la incidencia debe tener en cuenta los requisitos relativos a la seguridad de la información propios del proyecto, servicio o grupo en el que desempeñe su trabajo. En caso de duda o desconocimiento de estos requisitos específicos, la incidencia será comunicada adicionalmente al responsable de la persona.

Una vez recibida el Responsable de Seguridad será el encargado de darle seguimiento, completar las notificaciones establecidas en el procedimiento correspondiente, establecer las acciones para su corrección y comunicar al usuario la resolución o estado de la misma.

17. PROTECCIÓN DE DATOS

Es obligación de todo usuario que acceden a datos personales en soporte informático, en papel o cualquier otro soporte, respetar la normativa aplicable en esta materia, manteniendo la máxima confidencialidad sobre dichos datos y aplicando las medidas de seguridad establecidas en este documento, en la política de seguridad de MTP y en la RGPD.

No podrán crearse ficheros de datos personales sin la autorización del responsable de proteger los datos.

No se podrá cruzar información relativa a datos de diferentes ficheros o servicios con el fin de establecer perfiles de personalidad, hábitos de consumo o cualquier otro tipo de preferencias, sin la autorización expresa del responsable de proteger los datos.

No podrá realizarse 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.

Deberán cumplirse las medidas de seguridad establecidas para el tratamiento y la conservación de datos personales de forma automatizada o no automatizada, en soporte informático o en papel.

El usuario da su consentimiento para:

- Tratar los datos de carácter personal que queden registrados en los Sistemas de Información de MTP con las finalidades establecidas en estas normas, incluyendo la elaboración de patrones estadísticos.
- Tratar los datos de desempeño profesional, carrera, evaluación, coaching, pruebas psicotécnicas, y restantes datos relacionados con la gestión del capital humano.
- Tratar los datos de salud relativos a bajas laborales y control de absentismo que la legislación vigente permita gestionar a los servicios médicos corporativos y al departamento de recursos humanos.

18. CONTINUIDAD DEL NEGOCIO

Todos los empleados colaborarán en la oportuna reanudación de todos los servicios críticos para MTP en caso de una contingencia grave, ayudando de estar forma a que se restablezcan la mayoría de los servicios en el mínimo tiempo posible.

19. SOPORTES DE INFORMACIÓN

Cualquier soporte de información, informático, en papel o de cualquier otro tipo, que un usuario localice en los locales de MTP o sus inmediaciones que tenga la apariencia de haber sido extraviado, será entregado de forma inmediata a Seguridad Informática.

El uso de dispositivos de almacenamiento de información distintos a los homologados, inventariados y autorizados por MTP deberá ser autorizado expresamente por Seguridad Informática.

Los portátiles deben asegurarse con un cable de seguridad siempre que sea posible en cualquier lugar en el que se utilicen, y deberán guardarse en un armario bajo llave durante la noche o cuando no se usen durante un periodo prolongado de tiempo.

Los portátiles y todos los dispositivos móviles en general no deben guardarse ni siquiera de forma temporal en un coche o en un lugar de acceso público.

Debe informarse de inmediato sobre cualquier robo o pérdida de hardware. En caso de robo o pérdida de un ordenador o cualquier otro dispositivo móvil, deberá notificarse a Seguridad Informática.

Al finalizar la relación laboral o de cualquier otra índole con MTP, se deberán devolver todos los dispositivos TI asignados en el transcurso de la relación con la Entidad. Estos dispositivos deben ser devueltos en buen estado y con todos los periféricos.

20. DOCUMENTOS EN FORMATO PAPEL

Las mesas deberán mantenerse despejadas y libres de documentos, especialmente en las salas de reuniones y lugares de paso.

Los expedientes confidenciales y los documentos de trabajo deberán ser guardados en un lugar seguro, como por ejemplo un armario con llave, cuando no se estén utilizando, evitando así cualquier acceso no autorizado.

Todo documento que pueda contener datos personales, información de MTP, sus clientes, sus trabajadores, sus productos o cualquier otra información confidencial, deberá ser destruido de forma segura, utilizando destructoras de papel o depositándola en el interior de los contenedores destinados a tal efecto.

21. NORMAS RELATIVAS AL CUMPLIMIENTO DEL MARCO LEGAL VIGENTE

El obligación del usuario respetar toda la normativa legal vigente y publicada relacionada con la utilización, gestión y uso de los sistemas de información de MTP.

Asimismo, cualquier empresa, subcontratada por MTP para la realización de proyectos, obras o servicios se compromete formalmente a respetar el marco legal establecido, siendo esta condición indispensable para su contratación.

Se identifica como marco legal vigente la siguiente normativa:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- Real Decreto 994/1999, del 11 de junio de 1.999, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley Orgánica 15/1999, de 13 de diciembre de 1.999, de Protección de Datos de Carácter Personal L.O.P.D.C.P. que contempla lo previsto en el apartado 4 del artículo 18 de la Constitución, para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de 1.999, de Protección de Datos de Carácter Personal.
- Real Decreto 1332/1994, de 20 de junio por el que se desarrollan determinados aspectos de la Ley Orgánica 5/92 de 29 de octubre de Regulación del Tratamiento Automatizado de datos de carácter personal.
- Instrucciones emanadas de la AEPD (Agencia Española de Protección de Datos) del Estado y autonómicas, en aquellas comunidades en las que exista tal organismo y MTP disponga de oficinas.
- Ley de Protección Jurídica de Programas de Ordenador.
- Ley de Propiedad Intelectual.
- Convenios colectivos Aplicables y Legislación Laboral.
- Normativa Autonómica y Local (Ordenanzas Municipales).
- Así como cualquier otra del Ordenamiento Jurídico que pudiera resultar aplicable.

Sin menoscabo de lo anterior y cuando la información que se custodia esté relacionada estrechamente con datos personales de clientes, empleados u otras personas, se aplicará especial celo en su protección.

Se considerará de especial observancia la aplicación del marco legal vigente relacionado con los datos de carácter personal.

MTP se reserva cualquier derecho de actuación legal en situaciones de incumplimiento de la normativa vigente.

AL FIRMAR ESTE DOCUMENTO, USTED ADMITE QUE LO HA LEÍDO, ENTENDIDO Y ESTÁ DE ACUERDO CON SU CONTENIDO; Y SE COMPROMETE A CUMPLIR TODOS LOS TÉRMINOS Y CONDICIONES DESCRIPTOS Y SUS CONSIGUIENTES REGLAMENTACIONES Y POLÍTICAS OPERATIVAS.

HE LEÍDO, ENTIENDO Y ESTOY DE ACUERDO CON LAS CLÁUSULAS

Nombre y Apellidos	Firma
En ,a de de	