DONTE GROUP

Política De Uso De Los Medios Tecnológicos

(Compliance)

Versión 3

(4 de abril de 2024)

- **Destinatarios**

Todas las personas que, sin excepción, estén vinculadas a Global Mensa, S.L. y sus sociedades dependientes[1], **en adelante** "**DONTE GROUP**", con vinculación laboral o, cuando aplique, mercantil.

- **Aprobaciones**

Órgano de gobierno[2]	**Entidad**	**Fecha**	**Fecha de documento que se deroga**
Consejo de Administración	Global Mensa, S.L.	23.12.2021	25.01.2018
Órgano de Administración	Inversiones Odontológicas 2016, S.L.U.[3]	07-01-2022	25.01.2018
Organo de Vigilancia	**DONTE GROUP, S.L.U.**	**04.04.2024**	25.01.2018
			25.01.2018

- **Control de cambios**

Elaborado por	**Comité de Compliance**
Área	**Compliance**
Modificaciones	• **Actualización y cambio de formato (corporativo).**

- **Control de versiones**

Registro de Versiones					
Versión	1	2	**3**	-	-
Fecha	25.01.2018	23.12.2021	**04.04.2024**	-	-

Este documento ha sido elaborado por DONTE GROUP en el marco del desarrollo de sus políticas internas. Queda prohibida su reproducción y divulgación, excepto para el uso que se especifica en su propio contenido.

[1] Global Mensa es matriz de DONTE GROUP, S.L.U. y sociedades dependientes (**definidas en algún caso como la "empresa" a los efectos necesarios en este documento)** y comprende, a los solos efectos de este documento, las marcas Vitaldent, SMYsecret y MAEX.

[2] Se entiende por Consejo u Órgano de Administración: órgano o conjunto de órganos de gobierno de una empresa que son responsables de la supervisión y gestión del negocio al más alto nivel y de la implantación del sistema de Compliance.

[3] Actualmente denominada DONTE GROUP, S.L.U.

Contenido

1. Introducción / 4
2. Objeto 4
3. Prevención de conductas prohibidas 5
4. Ámbito De Aplicación 6
5. Principios generales 6
6. Reglas relativas a equipos (hardware) 7
7. Uso de la red de área local y del sistema informático principal 7
8. Reglas relativas a software 8
9. Ciber-espionaje y hacking informático 8
10. Uso del correo electrónico 9
11. Uso de internet 9
12. Uso de los dispositivos móviles 10
13. Privacidad personal y control de uso 11
14. Almacenamiento de datos 12
15. Teletrabajo 12
16. Derecho a la desconexión digital 13
17. Comunicación 13
18. Aprobación 13
19. Anexo 1 (Documento A Suscribir Por Emplead@ Del Departamento De Sistemas) 14
20. Anexo 2 (Documento A Suscribir Por El Empleado Que Disponga De Teléfono Móvil De _____, S.L.) 16

1. Introducción [4] / [5]

1.1. Los recursos electrónicos y tecnológicos (en adelante, los Medios) de los que **DONTE GROUP** provee a su directiva y resto de plantilla, son herramientas a través de las cuales se puede enviar y recibir información tanto dentro de la Red **DONTE GROUP** como a todo el mundo exterior. El uso eficiente de estos Medios contribuye al éxito de **DONTE GROUP**, si bien para ello, es necesario que los Medios sean utilizados de manera que no se infrinjan la ley, el Código de Conducta de **DONTE GROUP** o cualquier otro de sus Protocolos, Manuales, Políticas o Procedimientos Operativos.

1.2. La naturaleza, provisión y disponibilidad de estos recursos requieren que se establezcan políticas relacionadas con el uso de los mismos de manera que se garantice su utilización correcta y óptima. Además de esto, es necesario proteger la información confidencial manejada a través de los Medios, salvaguardar la propiedad intelectual, prevenir supuestos de responsabilidad frente a terceros, y generar evidencias de las infracciones que se puedan cometer utilizando los Medios.

1.3. Los sistemas informáticos son un instrumento de trabajo sujeto al control de la empresa y, por tanto, se debe complementar con una política interna que regule su uso y siempre en consonancia con acuerdos colectivos y los principios de la LOPDGDD.

1.4. La importancia de una correcta regulación interna del uso de los medios informáticos en el ámbito laboral es aún mayor si cabe con la llegada del Real Decreto-ley 28/2020, de 22 de septiembre, es decir, la elaboración de una normativa privada que garantice una mayor seguridad en la prestación de servicios tanto a empresario como a personas trabajadoras, tanto en la prestación de servicios de forma presencial como remota.

2. Objeto

2.1. El objeto de esta Política de Uso de Medios Tecnológicos es definir las pautas y establecer responsabilidades sobre el uso de los Medios de **DONTE GROUP** utilizados para el tratamiento y la transmisión de la información que **DONTE GROUP** pone a disposición de su directiva y resto de plantilla para el desempeño de sus funciones.

2.2. A efectos de la presente Política, debe entenderse que:

2.2.1. El término “usuario” o “usuarios” utilizado a lo largo del documento comprende al personal laboral o de otra naturaleza de **DONTE GROUP** con contrato en vigor o en suspenso o con obligaciones postcontractuales trascedentes para esta política- y su contenido aplica en tanto se mantenga la cesión y uso de Medios Tecnológicos.

2.2.2. Cualquier referencia al contrato de trabajo, a plantilla o a la relación laboral, debe considerarse extensible a otros tipos de prestación de servicios de carácter civil o mercantil.

2.2.3. Entre los Medios Tecnológicos se incluyen: (a) equipos, servidores de aplicaciones, terminales de acceso remoto, ordenadores de mesa o portátiles, tabletas, faxes, dispositivos USB, discos duros externos y dispositivos similares o equivalentes, (b) cualquier aplicación o programa de software, redes y sistemas, incluyendo chatbots, aplicaciones de videoconferencia, etc., (c) servicios de Internet, Intranet, Redes Sociales, sitios de almacenamiento masivo (como dropbox, wetransfer, onedrive y similares),

[4] El uso en este documento del masculino o femenino referido a personas hace referencia a las personas físicas, sin distinción de género o identidad sexual.

[5] ”DONTE GROUP” define a Global Mensa, S.A. y sus filiales en territorio español.

correo electrónico y mensajería instantánea, (d) las cuentas que dan acceso al uso de hardware, software y sistemas de información, incluyendo los sistemas y servicios en nube contratados o usados por **DONTE GROUP**, (e) teléfonos fijos, teléfonos móviles, smartphones, GPS, etc., y (f) drones, robots, vehículos inteligentes y sensores. Debe entenderse comprendido en lo anterior cualquier otro elemento o innovación tecnológica que pueda adquirir **DONTE GROUP** en lo sucesivo, tales como programas basados en inteligencia artificial, herramientas basadas en tecnologías blockchain, etc.

3. Prevención de conductas prohibidas

3.1. Permitir que **DONTE GROUP** ejerza el debido control para tratar de prevenir que se utilicen los Medios para incurrir, entre otras, en conductas prohibidas tales como las que se relacionan a continuación:

3.1.1. Acosar o discriminar a personal en plantilla o a terceros.

3.1.2. Atentar contra la dignidad, la intimidad y otros derechos fundamentales de las personas en general, ya sean empleadas o terceros.

3.1.3. Difamar, calumniar, injuriar o cualquier otro atentado contra el buen honor, reputación e imagen de **DONTE GROUP**, de su personal o de terceros.

3.1.4. Revelar información confidencial, durante o con posterioridad a la terminación del contrato de trabajo o de prestación de servicio.

3.1.5. Violar la normativa sobre protección de datos en cualquiera de sus manifestaciones, y en especial en aquello que pueda representar un atentado a los derechos fundamentales de las personas.

3.1.6. Atentar contra la seguridad de **DONTE GROUP** y sus activos tangibles e intangibles (propiedad de bienes, derechos de propiedad intelectual e industrial, fondo comercial, reputación, buena imagen, etc.).

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

3.1.8. Realizar actos de competencia desleal contra **DONTE GROUP**.

3.1.9. Incumplirlos contratos o relaciones con terceros.

3.1.10. Transmitir, distribuir, almacenar, descargar, instalar, copiar, enviar o recibir cualquier clase de contenidos protegidos por los derechos de autor, marcas, signos distintivos, secretos comerciales u otros derechos de propiedad intelectual o industrial utilizados sin la debida autorización, o/y ofensivos o discriminatorios especialmente si su posesión o utilización constituye una acción ilegal.

3.1.11. Borrar, dañar, deterior, alterar, suprimir o hacer inaccesibles, de forma dolosa, datos informáticos o programas informáticos de **DONTE GROUP**.

3.1.12. Desarrollar cualquier otra conducta que suponga un incumplimiento del Código de conducta que rige en **DONTE GROUP**.

3.1.13. En general, realizar cualquier uso de los Medios contrario al ordenamiento jurídico nacional vigente en cada Estado, a la presente Política u otra normativa vigente en el seno de la Empresa.

4. Ámbito De Aplicación

Esta Política será de aplicación a la directiva y resto de personal de **DONTE GROUP** en España que utilicen o accedan a los Medios de **DONTE GROUP**, siendo de obligado cumplimiento, con independencia de su ubicación o puesto.

5. Principios generales

5.1. Los Medios deben ser utilizados para fines profesionales, quedando prohibido alojar en los mismos información ajena a la actividad profesional del usuario. No obstante, **DONTE GROUP** permite el uso responsable y limitado para fines personales de estos Medios, si bien este uso personal debe ser ocasional y breve, y no debe interferir con las actividades normales de trabajo. En caso de existir riesgos relacionados con la ciberseguridad y protección de los medios o los datos, **DONTE GROUP** podrá limitar y/o controlar el acceso a los medios, infraestructuras, aplicaciones o redes externas.

5.2. En el uso de los Medios no debe tenerse expectativa alguna de privacidad. Dado que los Medios y la información contenida son titularidad de **DONTE GROUP**, como instrumentos de trabajo, ambos están sujetos en cualquier momento a la inspección, monitoreo y auditoría por parte de **DONTE GROUP**.

5.3. Los diferentes permisos de acceso a los Medios, las redes, sistemas, y a la propia información, ubicada en las instalaciones de **DONTE GROUP**, o en entornos contratados por **DONTE GROUP**, se otorgarán tras un proceso formal de aprobación que asegurará que cada usuario tenga acceso, únicamente, a los recursos e información necesarios para el desempeño de sus funciones.

5.4. Las conexiones remotas a la red de **DONTE GROUP** solamente se realizarán a través de los Medios destinados a tal fin, siendo éstos la única vía permitida de acceso, y siempre previa autorización del Departamento de Sistemas.

5.5. Todos los equipos de externos que pretendan conectarse de forma remota a la red de **DONTE GROUP** deberán tener implantados y correctamente actualizados los controles de detección, prevención y corrección de código malicioso, tales como sistemas de comprobación de la identidad (doble factor de autenticación, certificados digitales de confianza, etc.), VPN corporativa, herramientas de cifrado de datos o de los propios dispositivos, herramientas de borrado remoto e inhabilitación de los medios, etc.

5.6. Cada usuario deberá mantener el debido cuidado de los Medios que se le asignen, impidiendo el acceso de otras personas a las herramientas de trabajo que se le han asignado para su uso.

5.7. En consonancia con lo anterior los usuarios tampoco deben acceder a los Medios asignados a otros usuarios ni a la información profesional en ellos contenida, salvo autorización expresa y por necesidades de **DONTE GROUP**. En este caso, será necesario que, en la solicitud de acceso a los Medios asignados a otros usuarios, se especifique expresamente la necesidad que motiva dicho acceso.

5.8. Con carácter específico, deberá atenderse a la Norma de Seguridad de las Contraseñas y códigos privados de acceso que se encuentre vigente en cada momento. En caso de estar aplicada la política de renovación obligatoria de la contraseña (periodo de caducidad), todos los Medios se configurarán de forma que después un tiempo de inactividad, muestren el inicio de sesión exigiendo nuevamente la introducción de la contraseña para su desbloqueo. Esta acción siempre estará activa y queda prohibido deshabilitarla. Esta política podrá ser sustituida por otras que requieran la confirmación de la identidad usando otros mecanismos

distintos, en general de doble comprobación (como por ejemplo el doble factor de autenticación).

5.9. **DONTE GROUP** aplicará, en los términos previstos en la legislación vigente, la política de protección de datos y confidencialidad en correos electrónicos, documentos, archivos, archivos de voz o cualquier otro material de comunicación creado, recibido, guardado, transmitido o procesado usando los Medios de **DONTE GROUP**.

5.10. Cualquier robo o extravío de un Medio de **DONTE GROUP**, deberá ponerse inmediatamente en conocimiento del Departamento de Sistemas.

6. Reglas relativas a equipos (hardware)

6.1. Los equipos (o hardware) son el conjunto de elementos físicos o materiales que componen un sistema de información, tales como ordenadores de mesa o portátiles, impresoras, monitores, smartphones, dispositivos USB, discos duros externos, tarjetas de memoria, tabletas, teléfonos fijos, teléfonos móviles o dispositivos similares o equivalentes.

6.2. Son de aplicación las siguientes reglas:

6.1.1. Instalación y mantenimiento de equipos: el usuario no podrá realizar ningún cambio, manipulación o modificación sin la autorización expresa de la Dirección de Sistemas. La instalación de nuevos equipos deberá realizarse únicamente a través del departamento correspondiente, estando prohibida la instalación de cualquier elemento hardware adicional sin autorización de **DONTE GROUP**. Cualquier tipo de mantenimiento distinto deberá ser consultado y aprobado por la misma.

6.1.2. En caso de pérdida o robo de un dispositivo portátil que contenga información clasificada como sensible se debe informar de forma inmediata al responsable de los datos perdidos y al Departamento de Sistemas para permitir que se puedan tomar las medidas oportunas para minimizar los posibles impactos. Asimismo, se deberá interponer la correspondiente denuncia ante las autoridades competentes, informar al Departamento Jurídico y enviarle lo antes posible la copia de dicha denuncia.

6.1.3. En las instalaciones de **DONTE GROUP** se debe trabajar con Medios de **DONTE GROUP**. En caso de que fuera necesario introducir o utilizar Medios ajenos, estos deberán cumplir con los requisitos técnicos y de seguridad que se establezcan.

6.1.4. La utilización en las instalaciones de **DONTE GROUP** y durante el tiempo de trabajo de cualquier Medio tecnológico propio del trabajador ha de hacerse con la debida moderación y respetando las reglas establecidas en esta Política, y siempre que no perjudique las responsabilidades de trabajo y la contribución a la productividad.

6.1.5. Queda prohibida la conexión de los Medios propios del trabajador a la red corporativa salvo que medie autorización expresa del Departamento de Sistemas.

7. Uso de la red de área local y del sistema informático principal

7.1. El acceso tanto a la red de área local como al sistema informático principal, se realiza mediante un identificador de usuario (PÚBLICO) y una contraseña (CONFIDENCIAL). Cada usuario del sistema es el único responsable de mantener la confidencialidad de su contraseña. No está permitido dar a conocer contraseñas personales a compañeros del mismo departamento, de la misma clínica u otras personas. En caso de que la contraseña sea conocida fortuita o fraudulentamente por personas no autorizadas, el usuario deberá comunicarlo como incidencia al Departamento de Sistemas y proceder inmediatamente a su cambio.

7.2. En particular, las contraseñas, que tendrán 8 caracteres (como mínimo y debe de contener una mayúscula, un número y un carácter especial), deberán ser cambiadas periódicamente a los efectos de garantizar al máximo su seguridad. Con esta finalidad, cada 45 días, la red requerirá obligatoriamente el cambio de la contraseña al usuario.

7.3. Sin perjuicio del bloqueo automático, pasado cierto tiempo, es responsabilidad del usuario cerrar todas sus sesiones de trabajo en el sistema, cuando hace una pausa para comer o va a ausentarse de su puesto de trabajo durante un tiempo por el motivo que fuera. Esto evitará que alguien le pueda suplantar y use indebidamente su sesión de trabajo y su contraseña.

7.4. El sistema o política de protección por contraseña podrá ser complementado o sustituido por otros (como identificación biométrica, doble factor de autenticación, certificados digitales, etc.)

8. Reglas relativas a software

8.1. El software es el conjunto de elementos lógicos de un sistema de información (aplicaciones, programas, sistema operativo, bases de datos, etc).

8.2. Cada equipo contendrá las aplicaciones y programas necesarios para facilitar el correcto desempeño de las funciones de los usuarios a los que se destina. Asimismo, para evitar posibles daños causados por virus informáticos y multas por uso indebido de software o infracciones de derechos de propiedad intelectual de terceros, se prohíbe:

8.2.1. la instalación de software no corporativo o no autorizado expresamente.

8.2.2. programas ajenos a **DONTE GROUP**

8.2.3. software sin licencia, a través de disquetes, CD's, DVD's u otros soportes externos a **DONTE GROUP**, incluido Internet. En general no se podrá descargar o instalar ningún tipo de software sin el consentimiento expreso del Departamento de Sistemas;

8.2.4. copiar sin autorización el software o aplicaciones instalados en los Medios o tratar de descompilarlos, acceder a su código fuente o acceder por medios no autorizados a las mismas.

8.2.5. utilizar software que permita inhabilitar o dejar sin efecto las medidas de seguridad y controles establecidos por la Empresa o realizar acciones destinadas a saltarse dichos controles.

8.2.6. la conexión a los Medios (por ejemplo, dispositivos, equipos, etc.) de otros componentes como módems, routers de comunicación, dispositivos de almacenamiento USB, pen-drives, CD's, DVD's, etc., excepto aquellos debidamente autorizados y suministrados por **DONTE GROUP** (en este sentido, **DONTE GROUP** puede instalar de forma automática, o exigir al usuario, herramientas de cifrado y control selectivo).

8.2.7. realizar acción de mantenimiento sobre las aplicaciones en ninguna de las fases de su ciclo de vida, salvo autorización expresa del Departamento de Sistemas.

9. Ciber-espionaje y hacking informático

9.1. Se prohíbe cualquier práctica de ciber-espionaje dirigida a apoderase de información clave y secreta no autorizada de terceros (incluidos los competidores), información clasificada como secreto de empresa, datos de carácter personal, información comercial sensible, propiedad industrial, propiedad intelectual, etc.

9.2. Se prohíbe cualquier práctica relacionada con el hacking informático, es decir, con el acceso sin autorización a sistemas informáticos de terceros con el propósito de alterar o eliminar sus archivos.

9.3. Todo el personal del Departamento de Sistemas, es decir, cualificado en términos de conocimientos informáticos, así como cualquier otra persona que tenga acceso a los Sistemas de **DONTE GROUP**, por razón de su cargo, deberá aceptar y obligarse con las manifestaciones expuestas en el **Anexo 1** de esta política.

10. Uso del correo electrónico

10.1. El correo electrónico (en inglés: *electronic mail*, comúnmente abreviado e-mail o email) puesto a disposición de su directiva y resto de personal por **DONTE GROUP** es para uso profesional. En ningún caso deberá utilizarse para enviar cualquier tipo de datos o información de **DONTE GROUP** o relativos a los negocios de éste o de sus franquiciados o pacientes fuera del ámbito de los mismos, si no es por motivos estrictamente profesionales.

10.2. Las comunicaciones electrónicas deberán ajustarse a un uso ético y responsable, evitando en todo momento la utilización de palabras provocativas, ofensivas o incendiarias. Se deberán revisar íntegramente todos los mensajes antes de enviarlos.

10.3. Queda estrictamente prohibido que las comunicaciones electrónicas incluyan contenidos que puedan considerarse ofensivos, perjudiciales, difamatorios o despectivos, incluyendo a título enunciativo que no limitativo, comentarios o imágenes de índole sexual, racista o discriminatorio o que por su contenido y naturaleza sean susceptibles de ofender a alguien por razón de nacimiento, raza, país de origen, género, orientación sexual, religión, opinión, creencias, discapacidad o cualquier otra condición o circunstancia personal o social legalmente protegida.

10.4. **DONTE GROUP** puede monitorizar de forma automática los emails recibidos o enviados con el fin de:

10.4.1. Evitar la entrada o difusión de programas maliciosos (virus, malware, etc.).

10.4.2. Evitar la suplantación de identidad.

10.4.3. Evitar la fuga o envío erróneo de información potencialmente sensible (datos de pacientes, DNIs, números de tarjeta de Crédito, códigos de identificación de la Seguridad Social, códigos de cuentas bancarias, etc.).

10.4.4. Evitar el correo Spam (entrante o saliente) para reducir el riesgo de colapso de las líneas de comunicación o la entrada de los dominios de **DONTE GROUP** en las listas globales de spam.

10.5. Los correos electrónicos masivos, en general, entrañan problemas de gestión, dado que, entre otros efectos, pueden colapsar la red. Por ello, las comunicaciones con contenido general o destinadas a grandes grupos de personas dentro de la organización, deberán ser preferentemente canalizadas por medio de otras herramientas de difusión distintas del correo electrónico (circulares, noticias, anuncios, etc.).

11. Uso de internet

11.1. La directiva y resto de plantilla de **DONTE GROUP** deberán hacer un uso adecuado y responsable de Internet mientras estén utilizando los Medios puestos a su disposición por **DONTE GROUP**. El Departamento de Sistemas se reserva el derecho a bloquear o restringir el acceso a ciertos contenidos o páginas web.

11.2. La directiva y resto de personal de **DONTE GROUP** están sujetos, entre otras, a las siguientes normas:

11.2.1. No se deberá utilizar Internet para acceder o visitar páginas web de contenido pornográfico, racista o sexista o discriminatorio o que sean ofensivos para otras personas.

11.2.2. No se deberá acceder, mostrar, guardar, distribuir o editar contenidos de carácter sexual desde equipos provistos por **DONTE GROUP**.

11.2.3. No se deberá utilizar Internet para descargar software de entretenimiento ni juegos, tampoco se deberá acceder a juegos en Internet.

11.2.4. No se deberá utilizar Internet para difundir por cualquier medio mensajes difamatorios, de carácter sexual, racista o discriminatorio o que puedan resultar ofensivos para otras personas.

11.2.5. No se deberá utilizar Internet para acceder a sitios de chat o foros públicos para uso personal.

11.2.6. No se podrán hacer comentarios no autorizados previamente en chats públicos en nombre de **DONTE GROUP**.

11.2.7. No se deberá utilizar la dirección de correo de **DONTE GROUP** cuando se acceda a algún foro público o página web a no ser que su finalidad sea proveer información técnica o empresarial directamente relacionada con la prestación de servicios para **DONTE GROUP**.

11.2.8. No se deberá utilizar Internet para descargar o instalar software que no esté legalmente registrado y para el que se haya adquirido licencia de uso.

11.2.9. No se deberá utilizar Internet para incurrir en cualquier actividad ilegal: distribución de virus, intento de adquisición ilegal de datos de terceros, accesos no autorizados a entornos protegidos, etc.

11.2.10. No se deberá utilizar Internet para descargar archivos de video o audio para uso personal; tampoco se deberá utilizar Internet para acceder a contenidos streaming (audio y video online) excepto por motivos profesionales.

11.2.11. No se podrán conectar a redes públicas o privadas (aeropuertos, hoteles, etc.), sin el uso de herramientas específicas de cifrado y privacidad (VPN o similar).

11.3. El tiempo dedicado por los usuarios a navegar por Internet podrá ser controlado por el Departamento de Sistemas, a petición del Departamento de Recursos Humanos, al objeto de evitar un uso excesivo o no autorizado del mismo por parte de los usuarios.

11.4. El Departamento de Sistemas se reserva el derecho a bloquear o restringir el acceso a ciertos contenidos o páginas web.

12. Uso de los dispositivos móviles

12.1. Todos los dispositivos móviles puestos a disposición de la directiva y resto de personal están registrados y cuentan con la configuración y software necesario para su uso. Dicho software está debidamente licenciado por **DONTE GROUP**, estando prohibido la descarga o instalación de otros softwares distintos, salvo autorización expresa del Departamento de Sistemas.

12.2. El uso de dispositivos móviles personales y su sincronización con la red y sistemas de **DONTE GROUP** estará permitido siempre que: (i) su finalidad sea estrictamente profesional; (ii) haya

sido previamente autorizado por el Departamento de Sistemas; y (iii) el usuario acceda a la aplicación de esta Política al dispositivo personal.

12.3. Respecto al uso de los dispositivos móviles:

12.3.1. No deberán dejarse abandonados en ningún momento en lugares públicos;

12.3.2. Deberán guardarse, junto con todos sus componentes, en lugares seguros;

12.3.3. Durante la realización de viajes y desplazamientos deberán mantenerse siempre bajo control. En caso de tener que conectarse mediante el uso de redes públicas (wifis en aeropuertos, hoteles, etc.), será obligatorio el uso de software de cifrado específico (VPN o similar).

12.3.4. No deberán realizarse copias de seguridad de la información contenida en los mismos;

12.3.5. En caso de desplazamiento fuera del espacio económico europeo, deberá ponerse en conocimiento del Departamento de Sistemas;

12.3.6. No deberán llevarse a reparar a servicios técnicos no autorizados por el Departamento de Sistemas; y

12.3.7. En caso de robo o pérdida, deberá ponerse en conocimientos inmediato del Departamento de Sistemas, quien dará las correspondientes instrucciones.

12.4. En particular, el usuario deberá aceptar y obligarse a las manifestaciones detalladas en el Anexo 2 adjunto a esta política.

13. Privacidad personal y control de uso

13.1. Los Medios de **DONTE GROUP** se ponen a disposición para un fin estrictamente profesional y, por ello, no se deberá tener ninguna expectativa de privacidad personal en el uso de dichos Medios. Así, atendiendo a las circunstancias concurrentes y por razones estrictamente laborales, determinadas áreas debidamente autorizadas, pueden precisar tener acceso a los datos almacenados en las estaciones de trabajo de un empleado o empleada, por lo que no se debe esperar una privacidad absoluta de los datos almacenados en los puestos informáticos.

13.2. **DONTE GROUP** podrá adoptar las medidas que considere oportunas de vigilancia y control de sus Medios para verificar el cumplimiento de sus obligaciones laborales, incluido el cumplimiento de la presente Política, que puede incluir, si ello es necesario, la monitorización de los citados Medios. Asimismo, y para garantizar la seguridad de la red de **DONTE GROUP**, **DONTE GROUP** podrá supervisar el uso de los sistemas informáticos, incluido el acceso a Internet, especialmente cuando se constate la existencia de virus informáticos causados por el acceso a Internet o la utilización de determinados programas por parte de los usuarios.

13.3. Dentro de las medidas que podrá adoptar **DONTE GROUP** para ejercitar su potestad de vigilancia y control, así como para mantener la seguridad e integridad de sus Medios, se reserva el derecho a controlar y supervisar el acceso y uso de la red propiedad de **DONTE GROUP**.

13.4. La facultad de vigilancia tendrá como principales reglas generales las siguientes

13.4.1. Control de carácter regular, preventivo y aleatorio, tendente a identificar cualquier utilización de aquellos medios contrarias a las reglas establecidas en esta Política, y muy en especial violaciones de derechos fundamentales de las personas o de obligaciones que puedan poner en riesgo la seguridad y patrimonio de **DONTE GROUP** o de su personal.

13.4.2. Con carácter investigador y específico, cuando **DONTE GROUP** tenga indicios del uso de los Medios para la realización de conductas o actos contrarias a la Política aquí establecida.

13.4.3. En equipos, búsqueda automática o manual si en los equipos se almacena Software ilegal o no autorizado (incluyendo búsquedas automáticas o manuales términos libres que pudieran revelar conductas indebidas como acoso, discriminación, competencia desleal, revelación de secretos, etc.).

13.4.4. Correo electrónico (y a la información contenida en los mismos), búsquedas automáticas o manuales de términos que pudieran revelar conductas indebidas como acoso, discriminación, competencia desleal, revelación de secretos, etc.

13.4.5. Internet y de la Intranet, acceso automático al registro de las páginas web abiertas por el usuario para detectar contenidos ajenos a la actividad de **DONTE GROUP** y búsqueda de términos que pudieran revelar conductas indebidas como acoso, discriminación, competencia desleal, revelación de secretos, etc.

13.5. Las investigaciones que deban llevarse serán realizadas por el personal interno o externo designado por **DONTE GROUP** y, no teniendo obligación de informar a la persona investigada.

13.6. Durante el transcurso de dichas investigaciones o de las investigaciones recogidas en el Protocolo sobre el Canal de Denuncias e Investigaciones Internas, las personas investigadas podrán verse privados del acceso a los Medios de **DONTE GROUP**.

14. Almacenamiento de datos

14.1. Todos los datos relativos a los negocios de **DONTE GROUP** se almacenarán preferentemente en los lugares designados por **DONTE GROUP** en lugar otros medios (por ejemplo ordenadores portátiles).

14.2. Con objeto de almacenar o transmitir información confidencial, tal como ésta se define en las Instrucciones sobre Información Confidencial, y en estricto cumplimiento de lo establecido en la presente Política, todo el personal deberá hacer uso de sistemas técnicos de encriptación para con ello evitar el acceso no autorizado a dicha información confidencial por terceros.

14.3. En particular, los correos electrónicos enviados o recibidos por medio del servidor de correo de **DONTE GROUP**, para evitar la pérdida de la información contenida en los mismos, se almacenará una copia de seguridad completa de todos los elementos. Dicha copia de seguridad se destinará tanto a la debida atención de las relaciones internas y con terceros de **DONTE GROUP**, como al control del cumplimiento por parte de los usuarios de esta política.

15. Teletrabajo

15.1. El uso de medios de **DONTE GROUP** en un entorno de teletrabajo queda regulado por los mismas políticas y obligaciones.

15.2. El usuario que teletrabaje pondrá especial cuidado en no exponer datos sin cifrar en la red privada, siendo obligatorio el uso de software específico de protección (VPN) para la conexión a la intranet de **DONTE GROUP** o a la internet pública.

15.3. El usuario deberá mantener las medidas comunes y modernas de protección de sus elementos de red (en especial enrutadores, amplificadores de red, etc.), en especial: uso de

cifrado WPA2 o superior, protección del router y el acceso a las redes inalámbricas (WIFI) o cableadas con contraseñas "fuertes" y complejas.

15.4. En caso de no poder garantizar las medidas básicas de protección, el usuario de verá comunicarlo al Departamento de Sistemas para implantar medidas o equipos alternativos o adicionales de protección o control.

16. Derecho a la desconexión digital

16.1. Los usuarios de los Medios de **DONTE GROUP** no deberán estar conectados a los mismos fuera de sus horas de trabajo, siempre que durante este tiempo no tengan que cumplir con alguna obligación o responsabilidad propias de su puesto de trabajo.

16.2. **DONTE GROUP** está comprometidas con el bienestar de su personal y reconocen el derecho a la desconexión digital como elemento fundamental para lograr una mejor ordenación del tiempo de trabajo en aras del respeto de la vida personal y familiar. De este modo, y con carácter general, se procurará no enviar comunicaciones ni realizar llamadas fuera de la jornada laboral.

16.3. Cuando se deba desarrollar de forma excepcional o recurrente (convenientemente autorizada) el trabajo a distancia, incluyendo el llevado a cabo en el domicilio particular, o la distribución del tiempo de trabajo contemple ambas modalidades (presencial y a distancia -flexible-), también se estará sometido a lo expuesto respecto a la desconexión digital, con las particularidades que puedan contemplarse.

17. Comunicación

La aprobación de esta Política se comunicará a todo el personal, sin excepción, incluyendo a aquellos terceros que, or motivos de trabajo tengan acceso a medios internos, de **DONTE GROUP**. Asimismo, la Política estará disponible en la Intranet de **DONTE GROUP**.

18. Aprobación y entrada en vigor

18.1. De acuerdo con el punto 18.3 de esta misma Sección, al introducirse cambios menores pero necesarios, esta revisión de la Política de Uso de Redes Sociales ha sido aprobada por el Órgano de Vigilancia de Cumplimiento Normativo de Global Mensa, S.L y de sus sociedades filiales con fecha 4 de abril de 2024.

18.2. Este Protocolo debe mantenerse actualizado, y para ello debe revisarse de forma ordinaria anualmente, y de forma extraordinaria, cada vez que se produzcan variaciones en la legislación aplicable.

18.3. Cualquier modificación de este Protocolo está sujeta a la aprobación previa del Consejo de Administración. salvo que revista una importancia menor, en cuyo caso deberá ser aprobada por la Comisión de Cumplimiento y Auditoría y/o el Órgano de Vigilancia.

19. Anexo 1 (Documento A Suscribir Por Emplead@ Del Departamento De Sistemas)

El Emplead@ declara que en el desarrollo de sus funciones para las que ha sido contratado:

a) No se apoderará por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197 del Código Penal vigente[6].

b) No difundirá, ni revelará, ni cederá los secretos de _____, S.L., por acceso o por descubrimiento.

c) No se apoderará de soportes informáticos ni los destruirá sin la autorización escrita del director del departamento de Sistemas.

d) No perjudicará intencionalmente, ni por medio de un conflicto de intereses, a un usuario.

e) No perjudicará intencionalmente a cualquier otro informático o cualquier otra entidad informática.

f) No perjudicará a otros en el curso de sus actividades de Investigación y Desarrollo.

g) Trabajará promoviendo el respeto de la profesión.

h) En el desempeño de las funciones asumidas, cumplirá con todas las leyes, reglamentos y requisitos legales aplicables y no llevará a cabo ninguna actuación que pueda suponer responsabilidad o sanción alguna para él o para _____, S.L.

---

[6] ***Artículo 197.1 del Código Penal**, El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*

***El artículo 278 del Código Penal** sanciona un tipo de delito constituido por los elementos siguientes: (1) la acción delictiva consiste alternativamente, en el apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos; o el empleo de algunos de los medios o instrumentos del apartado 1 del art. 197 del C.P., (2) tal acción delictiva ha de tener por finalidad descubrir un secreto, esto es, algo que conocen una o varias personas que tiene o tienen interés en que no lo conozcan los demás, particularmente los que se dedican a la misma clase de actividad y, (3) ha de tratarse de un secreto de empresa, ya que abarca no solo los relativos a la técnica de los procedimientos de producción, sino también los relativos al comercio u organización del negocio de que se trate.*

***Si los hechos descritos en los apartados 1 y 2 del artículo 197del CP se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros**, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.*

i) Acepta que _____, S.L. tendrá derecho a auditar el cumplimiento de las manifestaciones anteriores, directamente o a través de un especialista.

Nombre:	
Cargo:	
Firma:	
Fecha:	

20. Anexo 2 (Documento a suscribir por quien disponga de teléfono móvil de _____, S.L.)

El Emplead@ declara que en el desarrollo de sus funciones para las que ha sido contratado:

a) Al utilizar el dispositivo móvil[7] que me ha sido entregado para el desarrollo de mi actividad laboral en nombre de _____, S.L. reconozco que la información confidencial de _____, S.L., y de terceros, será almacenada en mi dispositivo personal y que puede ser difícil distinguir entre dicha información y mis datos.

b) Certifico que he leído la Política de Uso de los Medios Tecnológicos y acepto que se aplique a mi dispositivo móvil y a quedar obligado por esos estándares. También acepto que _____, S.L. instale las aplicaciones apropiadas en mi dispositivo móvil para garantizar que las medidas de seguridad identificadas por _____, S.L. están activas en mi dispositivo móvil.

c) En caso de que mi dispositivo móvil se pierda o sea sustraído o robado, acepto y me obligo a notificar de inmediato al Departamento de Sistemas de _____, S.L. y les autorizo a borrar remotamente todos los datos y aplicaciones del dispositivo móvil. Entiendo que esto puede resultar en la pérdida de datos personales si no están adecuadamente protegidos.

d) Renuncio a cualquier derecho que pueda ostentar y que esté en conflicto con lo recogido en esta manifestación.

e) En el desempeño de mis funciones y en relación con el uso del dispositivo móvil que me ha sido entregado, no llevaré a cabo ninguna actuación que pueda suponer responsabilidad o sanción[8] alguna para mi o para _____, S.L.

Nombre:	
Cargo:	
Firma:	
Fecha:	

[7] *Los recursos electrónicos y tecnológicos de los que **DONTE GROUP** provee a su plantilla son herramientas a través de las cuales se puede enviar y recibir información tanto dentro de la Red de **DONTE GROUP** como a todo el mundo exterior. El uso eficiente de estos Medios contribuye al éxito de **DONTE GROUP**, si bien para ello, es necesario que los Medios sean utilizados de manera que no se infrinjan la ley, el Código de Conducta de **DONTE GROUP** o cualquier otro de sus Protocolos, Manuales, Políticas o Procedimientos Operativos.*

[8] *Espiar el móvil de otro está tipificado en nuestro Código Penal como un delito de descubrimiento y revelación de secretos (artículo 197del Código Penal).*