

# PROCEDIMIENTO DE CIBERSEGURIDAD EN USO DE INTERNET, SISTEMAS Y DISPOSITIVOS MOVILES DIGITALES

---

- 1. Objeto
- 2. Ámbito de aplicación
- 3. Responsabilidades
- 4. Desarrollo
- 5. Anexos
- 6. Referencias

DMANÁN CORPORACIÓN DMANÁN CORPORACIÓN

|                                       |                                                             |
|---------------------------------------|-------------------------------------------------------------|
| Motivo modificación: Creación del P02 |                                                             |
| Revisión: 00                          | Entrada en vigor: 01/09/2025<br>Responsable: Vanessa Chousa |

## 1. Objeto

El propósito de este documento es detallar el uso aceptable del equipamiento de sistemas de información de DMANAN. El uso no adecuado de sistemas y recursos exponen a DMANAN a riesgos que incluyen ataques de virus, compromiso de redes, sistemas, servicio y consecuencias legales. Las pautas y normas establecidas en este documento tienen como objeto proteger a los empleados, a los colaboradores y a DMANAN de estos riesgos.

Así mismo este documento pretende establecer medidas que proporcionen una dirección clara y organizada para alcanzar objetivos concretos en el ámbito de la Ciberseguridad en cuanto al uso del equipamiento y sistemas que nos permita maximizar la eficiencia de los recursos preventivos existentes, reducir el nivel de riesgo y asegurar que todo el personal involucrado, así como las terceras partes, trabajen de manera coordinada hacia la consecución de garantías en este ámbito relacionados con la ciberseguridad.

## 2. Ámbito de aplicación

El acceso a Internet está compartido por todo el personal al servicio de DMANAN. Las posibilidades de acceso y uso están destinadas y se configuran en función de la realización de las actividades laborales propias de cada empleado o persona al servicio del Grupo.

Los niveles de protección de la información instaurados por el Grupo son los legalmente requeridos además de haber instalado todas las medidas técnicas a su alcance para evitar la pérdida, alteración, mal uso, robo o acceso no autorizado a la misma. Aun así, los trabajadores deben ser conscientes de que las medidas de seguridad que se adopten no son inexpugnables por terceros, debiendo adoptar las medidas de precaución adecuadas en orden a evitar el acceso no consentido de terceros a los sistemas informáticos y de comunicaciones de terceros y en particular del Grupo.

Todas las herramientas informáticas son puestas por DMANAN a disposición de sus empleados, con fines exclusivamente laborales, por lo que las mismas deben ser utilizadas única y exclusivamente con esa finalidad, con las únicas excepciones previstas expresamente en el presente procedimiento.

Por ello, la Dirección de DMANAN se reserva el derecho de comprobar, cuando lo estime conveniente, si la utilización que están haciendo sus empleados de las herramientas informáticas puestas a su disposición se ajusta a dicha finalidad y a lo previsto en el presente procedimiento, mediante la realización de auditorías periódicas por profesionales dedicados al mantenimiento de estos dispositivos.

DMANAN únicamente podrá efectuar investigaciones sobre el uso que sus empleados realizan de los dispositivos electrónicos, correo electrónico e internet que ésta pone a su disposición cuando ello venga motivado por la denuncia de algún compañero o existan sospechas fundadas de su empleo con fines distintos para los cuales éstos son suministrados y que no obedezcan a lo establecido en el presente procedimiento. En mayor detalle al respecto la empresa se reserva el derecho de monitorizar el volumen de tráfico de internet así como los distintos sitios de internet visitados. El contenido específico de las transacciones no será

monitorizado salvo que exista sospecha de un uso indebido como anteriormente se expone. En tales casos las medidas a adoptar por DMANAN serán las idóneas, necesarias, proporcionadas y justificadas a tal fin y dentro de la legalidad vigente, según lo establecido en el punto 4.10 del presente procedimiento.

Queda contemplada la posibilidad de verificar periódicamente, en su caso a través de la contratación de empresas prestadoras de servicios de mantenimiento, que los ordenadores y los demás sistemas y dispositivos asimilados a éstos no se han utilizado con finalidades prohibidas expresamente en virtud de este procedimiento y, en particular, para verificar que no se ha descargado software ilegal o no autorizado, que no se han descargado contenidos prohibidos o que el correo electrónico se ha empleado de conformidad con lo establecido en la presente Política.

El presente procedimiento tiene como destinatarios a los profesionales y empleados de DMANAN que hagan uso de cualquier herramienta y dispositivo informático previamente facilitado por la empresa.

En particular será de aplicación y obligado cumplimiento y vinculará a los siguientes grupos de personas y entidades:

- Miembros del Órgano de Administración, incluidos los miembros no ejecutivos
- A todos los empleados, mandos intermedios y directivos del Grupo, incluidos empleados temporales o bajo convenio de colaboración, voluntarios, becarios y trabajadores en periodos de formación con independencia de que perciban o no una remuneración.

La aplicación del procedimiento y todo documento derivado del mismo, en ningún caso podrá vulnerar las disposiciones legales aplicables, las cuales prevalecerán sobre aquellas normas internas que pudieran contradecirlo, salvo que estas establezcan requisitos de conducta más exigentes.

### 3. Responsabilidades

La aprobación del procedimiento por el Órgano de Administración del Grupo supone el sometimiento de todos sus miembros a las normas contenidas y, por tanto, el cumplimiento de este es responsabilidad de cada uno.

DMANAN ha creado en cada uno de los equipos informáticos empleados por su personal una cuenta de usuario específica para cada uno de ellos, que cuenta con una clave de acceso que será conocida por cada empleado en cuestión.

En el caso de que se produzca una incidencia de seguridad tal como pérdida de dispositivos, acceso no autorizados o comunicación de contraseñas sin la debida aplicación de lo detallado en el presente procedimiento deberá de comunicarse al Responsable de Sistemas en el plazo menos de 72 horas atendiendo a la normativa de protección de datos para la gestión y respuesta ante quiebras de seguridad.

A partir de aquí el procedimiento se distribuirá a todas las personas sujetas al mismo, para que conozcan su contenido y las responsabilidades que ello conlleva.

### **Equipo Humano**

- Conocer y cumplir el procedimiento, así como tomar sus decisiones de acuerdo con sus principios y normas.
- Comunicar de forma responsable cualquier indicio de existencia de actuaciones que contravengan lo dispuesto en mismo, en este caso comunicarlo al Compliance officer y a su superior inmediato
- Ser responsables tanto de la custodia y adecuada conservación de los equipos, como de su utilización de acuerdo con las instrucciones dadas por la compañía y, en particular, las que constan en el presente procedimiento.
- Utilizar el equipo informático puesto a su disposición por DMANAN de forma personal e intransferible, en atención a sus funciones.
- Cumplimiento de lo desarrollado en el punto 4 “Desarrollo” en lo que a conductas no permitidas se refiere, utilización de los programas y de los archivos informáticos (*software*), acceso y navegación por Internet, uso de correo electrónico o email y uso de teléfonos móvil.
- Poner en conocimiento del Comité de Compliance y del Responsable de Sistemas cualquier sospecha de uso no autorizado en cualquiera de los equipos que estén bajo su responsabilidad o en las claves de acceso de estos tal y como se detalla el inicio del presente punto.

### **Mandos intermedio y directivos**

Con carácter adicional, todos los mandos de la empresa tienen las siguientes obligaciones:

- Comunicar el procedimiento a sus equipos de trabajo.
- Liderar su cumplimiento a través del ejemplo.
- Apoyar a sus equipos en los dilemas éticos y de entendimiento que puedan surgir al respecto de todas las conductas y normas en el desarrolladas
- Corregir desviaciones detectadas en el cumplimiento del presente procedimiento.
- Establecer mecanismos que aseguren el cumplimiento del procedimiento en sus áreas de responsabilidad.
- Autorizar el suministro y acceso a las claves de los equipos a usuarios distintos a los responsables de los mismos por motivo de ausencias temporales, bajas, vacaciones, suplencias...etc., todo ello en coordinación con el Responsable de Sistemas.
- Garantizar que una vez dicho acceso deje de ser necesario, y en todo caso al reincorporarse el trabajador usuario de la cuenta cuya clave de acceso se ha suministrado, se le comunicará el acontecimiento de este acceso y se le advertirá de la necesidad de cambiar su contraseña, todo ellos en coordinación con el Responsable de Sistemas.

### **Comité de Compliance**

- Comprobación de la correcta aplicación del presente procedimiento.

- Resolución de las dudas que le puedan surgir al personal para la correcta aplicación y cumplimiento del presente procedimiento.
- Recibir los avisos de incumplimiento del presente procedimiento, así como realizar las diligencias necesarias para el cumplimiento del mismo.
- Proponer si da a lugar, las sanciones o medidas disciplinarias que puedan proceder, consensuado con el órgano de administración de la correspondiente sociedad.
- Valorar los cambios que sean convenientes introducir en el presente documento.
- Dirigir las investigaciones que se realicen sobre la posible comisión de actos de incumplimiento de lo establecido en el presente documento.
- Informar periódicamente al Órgano de Administración del Grupo en relación con el seguimiento y cumplimiento de las normas establecidas en el presente procedimiento así que como la necesidad de la ampliación de recursos para dicho cumplimiento.

**Responsable de Sistemas y Equipo IT:**

- Salvaguardar las claves de acceso de todos los empleados
- Facilitar el uso de dichas claves a usuarios a petición de los mandos intermedios y directivos para el uso relacionado con él.
- Realización de auditorías o contratación de servicios externos para la realización de estas.
- Implantación de sistema de doble autenticación (MFA) y renovación de credenciales periódicamente.

**Órgano de administración:**

- Asegurar la disponibilidad de los recursos necesarios para el cumplimiento de lo establecido en el presente procedimiento.
- Resolver, si así lo requieren las circunstancias, posibles incumplimientos de los Códigos, Procedimientos y el Manual, así como cualquier comunicación que pueda llegar a través del canal de denuncias establecido.

Por tanto, es responsabilidad de las personas y entidades arriba mencionadas, cualquiera que sea la función desempeñada en el seno del Grupo, el hacer respetar y cumplir el presente procedimiento. Ninguna clase de incumplimiento de este será tolerado o ignorado.

Habida cuenta que todas las normas previstas en el presente procedimiento son de obligado cumplimiento por parte de todos los trabajadores del Grupo, la realización de cualquiera de las conductas descritas como prohibidas, sin perjuicio de la responsabilidad penal, civil o administrativa que genere para su autor, según los casos, constituirá una infracción disciplinaria, susceptible de ser sancionada como tal por el Grupo, tras el procedimiento previsto al efecto, siendo la sanción proporcional a la gravedad de la conducta infractora cometida y, en su caso, teniendo en cuenta la reiteración de la conducta infractora.

## **4. Desarrollo**

#### **4.1 CONDICIONES GENERALES DE CIBERSEGURIDAD EN EL USO DE INTERNET, SISTEMAS, CORREO ELECTRÓNICO Y DISPOSITIVOS MÓVILES:**

Todos los equipos informáticos que DMANAN pone a disposición de sus empleados son propiedad del Grupo, y su utilización por parte de los empleados queda limitada a **finés estrictamente profesionales**.

Los empleados que utilicen los equipos informáticos puestos a su disposición por DMANAN son responsables tanto de la custodia y adecuada conservación de los equipos, como de su utilización de acuerdo con las instrucciones dadas por la compañía y, en particular, las que constan en el presente procedimiento.

DMANAN ha creado en cada uno de los equipos informáticos empleados por su personal una cuenta de usuario específica para cada uno de ellos, que cuenta con una clave de acceso que será conocida por cada empleado en cuestión. Así mismo se ha facilitado otra serie de dispositivos tales como móviles o portátiles acordes con las necesidades de cada empleado para el desempeño de su trabajo, en los que se exigirá el total cumplimiento de lo especificado en las responsabilidades en el punto anterior, así como lo que a continuación se detalla.

Cada trabajador deberá utilizar el equipo informático puesto a su disposición por DMANAN de forma personal e intransferible, en atención a sus funciones.

##### **Conductas no permitidas:**

Como consecuencia con todo lo expuesto anteriormente, quedan expresamente prohibidas las siguientes conductas:

- La utilización de los equipos informáticos para cuestiones y actividades personales, ajenas a la prestación laboral y ello, aunque dicha utilización se lleve a cabo fuera del horario laboral y/o fuera de las instalaciones de la empresa.
- Revelar o compartir contraseñas, permitiendo a cualquier otra persona el uso de cuentas (esto incluye familiares o amigos si en alguna circunstancia el trabajo se realiza desde casa)
- La conexión de los equipos informáticos a otros sin contar con la autorización expresa y por escrito de DMANAN.
- Ausentarse del puesto de trabajo sin bloquear o desconectar el equipo informático.
- Permitir que otra persona ajena a DMANAN o que no cuente con la autorización del Grupo al respecto, de conformidad con lo previsto anteriormente para el uso de las claves de los equipos, manipule el equipo del empleado o extraiga de los mismos ficheros o cualquier otra información almacenada en el mismo.
- Descargar o archivar informaciones o documentaciones privadas o particulares no relacionadas con la actividad laboral o de la propia Empresa. En este caso el empleado no podrá esperar ningún tipo de confidencialidad en caso de que incumpla la presente prohibición en relación con los accesos que el resto del personal del Grupo pueda tener a los mismos.

#### **4.2 UTILIZACIÓN DE LOS PROGRAMAS Y DE LOS ARCHIVOS INFORMÁTICOS (SOFTWARE):**

Todos los programas, archivos y documentos incluidos en los sistemas y equipos informáticos de DMANAN son propiedad de la misma y deben utilizarse con una finalidad exclusivamente profesional, sin que, en consecuencia, puedan ser utilizados para un uso personal o privado, y sin que los empleados puedan albergar algún tipo de expectativa de privacidad respecto a su contenido o en cuanto al uso que hagan de los mismos, incluyendo también todos los documentos impresos en papel.

El empleado es consciente de que cualquier intento de descarga y/o envío masivo de archivos y documentos propiedad de DMANAN podrá ser notificada a éste, pudiendo tomar las medidas que estime oportunas en atención al perjuicio causado a el Grupo, al margen del régimen sancionador contemplado en el P07 Procedimiento de RRHH.

Dado que es posible que otros compañeros de trabajo puedan acceder a los equipos de un empleado en los casos en los que así se encuentre justificado por el presente procedimiento DMANAN recomienda a sus empleados no alojar ningún tipo de información ni documento de carácter personal o que contenga datos de esta índole en los mismos. DMANAN no será responsable por los incumplimientos que sus empleados realicen de esta recomendación, en cuyo caso, no podrá garantizar la privacidad de la información de este tipo albergada en sus equipos.

Cuando un empleado detecte la necesidad de emplear un programa informático que no esté instalado en su equipo deberá comunicárselo al Responsable de Sistemas para que expertos informáticos analicen la viabilidad de instar el referido, absteniéndose de realizar cualquier instalación por su cuenta. El Responsable de Sistemas consultará con el órgano de administración esta cuestión si el programa informático solicitado no se encuentra dentro de aquellos previamente autorizados por el mismo.

#### **4.3 ASPECTOS CLAVES EN INTERNET, REDES Y SISTEMAS:**

##### **A. Criterios generales:**

El acceso a Internet y al navegador existente en los equipos informáticos de cada puesto de trabajo se configuran como herramientas de trabajo facilitadas por DMANAN para un mejor desempeño de las funciones laborales encomendadas. En ningún caso se pueden modificar las configuraciones de los navegadores del equipo, ni la activación de servidores o puertos sin autorización.

Por ello, los empleados que tengan acceso a la red de Internet sólo podrán realizar conexiones a través de la referida red que obedezcan a fines estrictamente profesionales, todo ello con el fin de obtener el mayor aprovechamiento posible de los recursos informáticos.

Como excepción, los empleados podrán emplear la conexión a Internet suministrada por DMANAN para usos personales, siempre que dicho uso sea excepcional y existan razones urgentes o de especial gravedad que justifiquen dicho empleo y no dispongan de una conexión personal en ese momento. No obstante, nuevamente DMANAN recomienda a sus empleados no efectuar este tipo de conexiones ya que no puede garantizar la privacidad de las mismas. El empleado ha de ser consciente de que las búsquedas personales que efectúe a través de los equipos y conexión a Internet de DMANAN pueden ser conocidas por ésta.

En el caso de que alguno de los usuarios detecte o sospeche de cualquier tipo de incidencia en seguridad en cualquiera de los dispositivos que tenga a disposición, deberá de manera urgente comunicarlo al Responsable de Sistemas dejando en stand by el dispositivo hasta que el Equipo de IT verifique el correcto funcionamiento y la ausencia de amenazas.

B. Condiciones de utilización de la conexión a Internet:

El acceso y la utilización de la red *Internet* deberán realizarse atendiendo a las siguientes reglas y criterios de actuación:

- Queda terminantemente prohibido el acceso a páginas *Web* de contenido ofensivo, inapropiado, pornográfico, erótico o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social,
- Queda terminantemente prohibido el uso de páginas *Web* para perpetrar cualquier tipo de fraude o piratería de software o ficheros multimedia.
- Queda terminantemente prohibido el uso de páginas *Web* vulnerando derechos de copia (copyright)
- Tampoco se permite la utilización de Internet para participar en juegos de azar, sorteos o subastas, o para aquello que pueda suponer un perjuicio para su reputación y/o cargas económicas.
- Queda terminantemente prohibido utilizar programas o plataformas de compartición de ficheros en Internet, así como utilizar redes públicas de mensajería instantánea distintas a las definidas como corporativas por DMANAN.
- La Dirección de DMANAN se reserva la facultad de instalar los mecanismos técnicos necesarios para impedir el acceso a determinadas páginas *Web*. Si por motivos estrictamente profesionales fuera preciso al acceso a alguna de dichas páginas, el empleado deberá solicitar autorización de acceso al *Compliance Officer* o *Comité de Compliance*
- El hecho de que la Dirección de DMANAN no haya bloqueado el acceso a una determinada página *Web* no implica que el acceso a la misma sea válido.
- Es obligación de DMANAN dar cumplimiento al contenido de la normativa en materia de propiedad intelectual o industrial, por lo que los empleados deberán comprobar cuidadosamente, antes de utilizar información proveniente de la red, si la misma se encuentra protegida por las normas de las expresadas leyes.
- Queda terminantemente prohibido el acceso a debates en tiempo real (*Chat*), mensajería electrónica y similares con una finalidad ajena a la profesional.
- Queda prohibida la descarga desde la red de Internet de cualquier clase de programas o aplicaciones con una finalidad ajena a la profesional. En caso de incumplimiento de esta norma, el usuario acepta liberar a DMANAN de cualquier responsabilidad en caso de reclamación, litigio, pérdidas, daños o gastos

relacionados con la utilización indebida de Internet. La excepción a esta interdicción de carácter general está representada por la posibilidad de que los técnicos y mantenedores de los equipos informáticos descarguen e instalen actualizaciones necesarias y programas gratuitos o de uso libre, así como aquéllos otros para los que se cuente con la oportuna licencia de uso adecuada a los fines para los que se van a utilizar.

### C. Actividades de redes y sistemas

Las siguientes actividades están, sin excepción, estrictamente PROHIBIDAS:

- Cometer violaciones de los derechos de cualquier persona o compañía protegida por derechos de copia, secreto de comercio, patente, propiedad intelectual o industrial, o por cualquier otra norma similar.
- Efectuar copias no autorizadas de material protegido por derechos de autor, incluyendo, pero no limitándose, a la digitalización y distribución de fotografías de libros, revistas u otras fuentes protegidas.
- Exportar software, información técnica, software de encriptación o tecnologías que violen cualquier norma vigente.
- Introducir programas maliciosos dentro de la red o los servidores (por ejemplo, virus, gusanos, troyanos, bombas lógicas, etc.).
- Utilizar equipamiento de DMANAN para obtener o difundir material inapropiado o que viole cualquier norma vigente.
- Realizar ofertas fraudulentas de productos o servicios desde una cuenta de DMANAN.
- Provocar brechas de seguridad o interferencias en las redes de comunicaciones. Las brechas de seguridad incluyen, pero no se limitan, el acceso a datos para los que el empleado no tiene autorización o la entrada en un servidor o cuenta para la que el empleado no tiene el acceso autorizado, excepto que estas tareas estén incluidas en el transcurso de operaciones de trabajo.
- Proceder al escaneo de puertos o de seguridad, salvo que estén permitidos expresamente por el área de seguridad de la organización.
- Ejecutar cualquier tipo de monitorización de red que intercepte datos no destinados al empleado, excepto que esta actividad se efectúe con motivo de su prestación de servicios.
- Sobrepasar la autenticación o seguridad de cualquier host, red o cuenta, excepto que estas tareas estén incluidas en el transcurso de operaciones de trabajo.
- Interferir o denegar servicios, excepto que estas tareas estén incluidas en el transcurso de operaciones de trabajo.
- Suplantar la identidad de otros trabajadores para acceder al sistema.
- Acceder a ficheros o programas cuyo acceso no le haya sido permitido.
- Emplear la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

#### **4.4 USO DE CORREO ELECTRÓNICO O E-MAIL:**

##### **4.4.1 Criterios generales:**

El correo electrónico constituye una herramienta de trabajo facilitada por la Dirección de DMANAN a sus empleados con el fin de desempeñar más eficientemente sus funciones laborales. Como consecuencia de lo anterior, se dotará de una dirección individual de correo electrónico a cuantos puestos de trabajo requieran razonablemente de su utilización, siendo facultad de DMANAN la organización de este y el sistema que deba seguirse, con libertad absoluta para decidir sus condiciones.

Cada empleado será responsable de su propia dirección de *e-mail* y de que la misma sea utilizada con arreglo a las prescripciones del presente Protocolo.

El correo electrónico deberá ser utilizado con fines estrictamente profesionales, por lo que el empleado que haga uso de este no puede albergar alguna expectativa de privacidad o secreto en las comunicaciones.

Los emails dirigidos a varios destinatarios deben ser remitidos observando la confidencialidad y para esto solo se podrán incorporar direcciones en copia (campo CC) cuando se ha obtenido autorización de la persona titular de la cuenta de email o bien cuando ello sea necesario por la naturaleza del trabajo que se esté realizando.

Ningún empleado deberá permitir la utilización de la cuenta y/o el correspondiente buzón por personas no autorizadas.

##### **4.4.2.- Uso privado o personal del correo electrónico:**

Los empleados no podrán utilizar el correo electrónico para fines personales, salvo que existan razones urgentes o de especial gravedad que justifiquen la utilización de este medio para contactar con el hogar familiar, concertar citas inmediatas o transmitir recados urgentes.

La utilización excepcional del correo electrónico para fines personales deberá prolongarse el menor tiempo posible.

En los envíos de carácter personal se indicará, en el apartado referente al asunto del correo, tal carácter con la palabra, en mayúsculas, "PERSONAL", que se podrá acompañar de cualquier otra indicación.

La no inclusión de este distintivo en los correos conllevará automáticamente la consideración de estos como relacionados con la actividad empresarial, quedando DMANAN liberada de cualquier responsabilidad en orden al control y confidencialidad de dichos correos. No obstante siempre se aplicará a aquellos correos recibidos y leídos, nunca a los NO leídos.

En el caso de cese de la actividad por parte de un empleado, en el mismo momento de su cese se le permitirá la posibilidad de acceder a su cuenta de correo para recuperar toda aquella información de carácter personal que pudiera tener almacenada. Lo mismo deberá hacerse con otra información almacenada en el buzón y que se necesite por la empresa para su funcionamiento, extrayéndola antes de su partida y, si es posible, en presencia del titular de la cuenta.

DMANAN podrá tener conocimiento de las salidas de correos electrónicos por parte de sus empleados a cuentas no profesionales, pudiendo requerirle a éstos una justificación acerca del uso realizado para fines personales. Asimismo, DMANAN podrá establecer alertas que le informen del envío de correos electrónicos con archivos adjuntos de gran tamaño o envíos masivos de aquéllos.

#### **4.4.3.- Condiciones de utilización del correo electrónico:**

En la utilización del correo electrónico deberán observarse las siguientes reglas:

- Queda prohibido el envío y recepción a través del correo electrónico de aplicaciones, archivos y documentos no relacionados con el trabajo del empleado.
- Queda prohibido el envío de mensajes o imágenes de carácter ofensivo, inapropiado, pornográfico, erótico o discriminatorio por razones de género, etnia, opción sexual, discapacidad o cualquier otra circunstancia personal o social, así como aquellos que puedan constituir cualquier tipo o forma de acoso entre compañeros de trabajo.
- Queda prohibida la utilización del correo electrónico para promover el acoso sexual o laboral, juegos de azar, sorteos, subastas, descargas de video o audio y cualesquiera otros materiales no relacionados con la actividad profesional.
- Los empleados deberán abstenerse de enviar mensajes masivos o con ficheros adjuntos de gran tamaño y evitar los mensajes encadenados en la medida de lo posible.
- Los empleados deberán extremar la diligencia y precaución necesarias para evitar la entrada de virus, principalmente como consecuencia de la utilización de archivos de procedencia externa llegados a través del correo electrónico.
- Queda terminantemente prohibida la apertura de cuentas de correo personal utilizando para ello los equipos informáticos de DMANAN. Se entiende que en ocasiones los empleados puedan necesitar acceder a su correo personal o realizar tareas no relacionadas con el trabajo utilizando los equipos proporcionados por la empresa. No obstante, es importante recordar que dichos dispositivos y la red interna están destinados principalmente a fines laborales. Por ello, se informa que, al utilizar los equipos y la red de la empresa para acceder al correo personal u otras actividades, no se puede garantizar la privacidad de dichas comunicaciones. La empresa, en cumplimiento con sus políticas de seguridad y normativas aplicables, puede monitorear las actividades que se realicen a través de sus dispositivos y red, siempre con el objetivo de proteger los intereses de la organización y cumplir con los requisitos legales como se señala más adelante.
- Se configurará una respuesta automática en el correo cuando se vaya a producir una ausencia del puesto de trabajo, durante el plazo que estimado de ausencia. En dicho mensaje automático de ausencia no se mencionará la situación personal del titular de la cuenta, por respeto a su intimidad y privacidad.

Asimismo, durante dicha ausencia se le solicitará que reenvíe los correos a otra dirección de correo (por ejemplo al correo de la persona que le sustituya, al correo

del superior jerárquico o a la dirección de correo genérica del departamento), pero en ningún caso se desviará automáticamente el tráfico de la cuenta de correo de la persona ausente, mediante la configuración de una regla de correo, a otra cuenta de correo diferente.

- Asimismo, DMANAN se reserva el derecho a instalar programas para controlar el tráfico de correos electrónicos de contenido prohibido o potencialmente peligroso, utilizando a tal efecto software especialmente desarrollado para la detección de “spam”.

Queda terminante y explícitamente prohibido:

- Utilizar correos electrónicos personales para realizar comunicaciones vinculadas a la relación laboral.
- Participar en la propagación de cartas encadenadas, esquemas piramidales o similares.
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la entidad.
- Utilización no autorizada o falsificación las cabeceras de correo electrónico (ej: intento de suplantación de la información).
- Difundir contenido ilegal o contrario a la moral y las buenas costumbres.
- Efectuar ataques, con objeto de imposibilitar u obstruir sistemas informáticos, dirigidos a un empleado o al propio sistema de correo, así como, el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga por objeto la paralización del servicio por saturación de las líneas, de la capacidad CPU del servidor, del espacio en disco de servidores o terminales o cualquier otra práctica similar.
- Enviar a foros de discusión, listas de distribución y/o newsgroups, mensajes que comprometan la reputación de la entidad.
- Enviar correos no solicitados desde las redes de DMANAN o desde cualquier otro proveedor de servicio con el fin de publicitar servicio ofrecidos por DMANAN.

#### **4.5.- USO DE DISPOSITIVOS MÓVILES**

##### **4.5.1.- Uso de teléfonos móviles particulares durante la jornada laboral**

El uso de teléfonos móviles particulares (así como otros dispositivos que puedan asimilarse a éstos, como es el caso de los «*smartphones*» y las «*tabletas*» que puedan ser utilizadas como teléfonos móviles) durante la jornada laboral no está permitido para usos particulares, salvo en los momentos de descanso y salvo en circunstancias personales excepcionales del trabajador.

Se recomienda que los teléfonos móviles particulares se mantengan guardados o en modo vibración, o bien con un tono bajo que no interrumpa el desarrollo normal de las actividades laborales ni perturbe a los compañeros. Se permite la utilización de señales lumínicas para avisos de entrada de mensajes, siempre que no interfieran con el trabajo.

En cuanto a las llamadas personales, se sugiere que, en la medida de lo posible, se atiendan en momentos apropiados sin abandonar las instalaciones de DMANAN. En situaciones excepcionales, el trabajador podrá comunicar su necesidad al superior inmediato, quien evaluará las circunstancias personales y podrá otorgar el permiso necesario para ausentarse temporalmente del puesto de trabajo.

Está expresamente prohibido conectar el móvil (la tableta u otros dispositivos con conexión a internet) personal a la red *wifi* de la empresa.

#### **4.5.2.- Uso de dispositivos móviles de la empresa**

Los teléfonos y otros dispositivos móviles asimilados a éstos -como ordenadores portátiles, tarjetas de memoria, tablets y demás equipamiento móvil- que DMANAN facilite a sus trabajadores y directivos para realizar su trabajo, atendiendo a las necesidades corporativas y de organización, gestión y realización propia de la actividad empresarial, se utilizarán con esta única finalidad.

Los trabajadores y directivos que cuenten con la posibilidad de utilizar un teléfono o un dispositivo móvil asimilado a éste deberán mantenerlo actualizado en todo momento, así como instalar en los mismos programas antivirus, y bloquear el acceso a los mismos mediante contraseña, patrón o identificador biométrico. Asimismo, los empleados no podrán descargar ni instalar en estos dispositivos aplicaciones ni software que no haya sido expresamente autorizado por el personal informático de DMANAN.

Los trabajadores y directivos que cuenten con la posibilidad de utilizar un teléfono o un dispositivo móvil asimilado a éste tienen la obligación de comunicar, de inmediato, a su superior jerárquico, así como al Comité de Compliance del Grupo, su pérdida, sustracción, así como cualquier vulneración de la seguridad del mismo imputable a un tercero.

DMANAN podrá instalar en estos teléfonos y dispositivos móviles asimilados, que pone a disposición de sus trabajadores y directivos, sistemas de seguridad, sistemas de seguimiento y bloquear el acceso a determinados sitios web, por razones de seguridad y de protección de la reputación del Grupo, así como de los datos personales de sus trabajadores, clientes y proveedores, contratistas y prestadores de servicios, y de las informaciones sensibles, de carácter confidencial, así como de las sometidas a protección por las normas reguladoras de la propiedad intelectual e industrial.

DMANAN llevará a cabo un registro interno de control de asignación de los recursos utilizados ( recogidos en el Anexo 7 de los portales existentes en la empresa subcontratada para tal fin en cada una de las entidades del grupo que sea de aplicación).

#### **4.5.3.-Utilización de equipamiento móvil fuera de las instalaciones**

Cuando se utilicen equipos pertenecientes a la organización (ordenadores portátiles, tablets, teléfonos móviles, etc.) fuera de las instalaciones de DMANAN deberán observarse las siguientes directrices:

- Se debe tener especial cuidado y diligencia con los equipos, extremando la precaución para evitar robos, sustracciones y acceso a información contenida en los mismos.
- No dejar nunca desatendido el dispositivo.
- Proteger el equipo de exposiciones a agentes externos dañinos (agua, polvo, campos electromagnéticos, etc.).
- No permitir la utilización del dispositivo por otra persona.

#### **Teletrabajo**

- Se considerará que el trabajador se encuentra prestando servicios en régimen de "teletrabajo" cuando el mismo utilice los equipos de información y comunicación fuera de la organización con ocasión de su trabajo.
- El Departamento de IT es el responsable de:
  - Procurar que los equipos sean utilizados de acuerdo con los procedimientos aplicables.
  - Evitar el acceso no autorizado de terceros.
  - Configurar adecuadamente la red local utilizada para conectarse a Internet.
  - En caso de finalización de la prestación de servicios de un trabajador, devolución de datos y equipamiento.
  - Existencia de un nivel mínimo de configuración de la instalación donde se realizarán las actividades de teletrabajo.
  - Determinar el listado de actividades permitidas y prohibidas, según el presente procedimiento.

#### **4.6.- USO DE REDES SOCIALES**

Se detalla a continuación de forma específica el uso de las redes sociales personales de cada trabajador: Los empleados no pueden hacer mención a ningún asunto relacionado con el trabajo desarrollado por los mismos con ocasión de su prestación de servicios a DMANAN en redes sociales, blogs o cualquier otra estructura social. En particular, con carácter descriptivo, pero no limitativo, se tendrán en cuenta las siguientes reglas:

- Está terminantemente prohibido publicar cualquier tipo de información relacionada con cualquier proyecto, cliente o proveedor de la organización a través de imágenes, comentarios, videos, etc., así como toda aquella información confidencial a la que el trabajador haya tenido acceso por razón de su puesto de trabajo.
- No está permitido crear grupos dentro de las redes sociales utilizando la marca, logotipo o nombre comercial de la organización.

- No está permitido difundir información comercial de la organización a los contactos en la red social (spam).
- Si un empleado tiene un perfil abierto en una red social en la que se le pueda relacionar con DMANAN, debe incluir obligatoriamente la mención de que las opiniones publicadas son personales y en ningún caso representan las de la organización para la que trabaja.

#### **4.7.- REUTILIZACIÓN Y RETIRADA DE EQUIPOS**

Cuando un equipo perteneciente a la organización vaya a ser reutilizado o retirado, deberá ser entregado al Departamento de IT, que realizará las operaciones necesarias para la eliminación segura de la información que pudiera contener el equipo.

En el caso de utilizar los equipos pertenecientes a DMANAN fuera de las instalaciones de este, se debe tener en cuenta las siguientes reglas:

- No se dejará nunca desatendido ni se permitirá la utilización de este por terceros.
- En el caso de material informático propiedad de DMANAN que no esté asignado a un trabajador y que deba ser sacado fuera de sus instalaciones, deberá contarse con la preceptiva y previa autorización expresa del Responsable de Sistemas.

#### **4.8.- MANTENIMIENTO Y CAMBIOS**

- El mantenimiento de los distintos sistemas y recursos de tecnologías de la información será realizado por personal del Área de Mantenimiento de Sistemas de DMANAN, que deberá tener en cuenta las especificaciones del fabricante.
- Cuando sea necesaria la revisión y/o reparación de un equipo por parte de un proveedor especializado y dicho equipo salga de las instalaciones de DMANAN, el Departamento de IT tomará todas las medidas de seguridad necesarias para eliminar la información que los mismos contengan. Asimismo, se revisará el equipo una vez se haya realizado la revisión/reparación.
- Cuando el mantenimiento de los sistemas implique la realización de cambios significativos, se deberá realizar la correspondiente evaluación, que tendrá en cuenta los posibles impactos del cambio, debiendo prestar especial atención a las posibles implicaciones de seguridad.

Si los cambios afectan a sistemas vitales para el negocio de la organización, deberán estar aprobados por la Dirección Técnica.

Con anterioridad a efectuar los correspondientes cambios, , se efectuará la correspondiente comunicación a los usuarios y propietarios de los sistemas afectados.

#### **4.9.- SEGURIDAD EN SERVIDORES**

La operación de los servidores/máquinas virtuales/instancias, será realizada exclusivamente por personal del Departamento de IT, el cual es consciente de los riesgos existentes y conocedor de buenas prácticas de operación que aplica de forma sistemática.

#### **4.10.- CONTROL EMPRESARIAL**

Todas las herramientas informáticas son puestas por DMANAN a disposición de sus empleados, con fines exclusivamente laborales, por lo que las mismas deben ser utilizadas única y exclusivamente con esa finalidad, con las únicas excepciones previstas expresamente en la presente Política.

Por ello, la Dirección de DMANAN se reserva el derecho de comprobar, cuando lo estime conveniente, si la utilización que están haciendo sus empleados de las herramientas informáticas puestas a su disposición se ajusta a dicha finalidad y a lo previsto en la presente Política, mediante la realización de auditorías periódicas por profesionales dedicados al mantenimiento de estos dispositivos.

DMANAN únicamente podrá efectuar investigaciones sobre el uso que sus empleados realizan de los dispositivos electrónicos, correo electrónico e internet que ésta pone a su disposición cuando ello venga motivado por la denuncia de algún compañero o existan sospechas fundadas de su empleo con fines distintos para los cuales éstos son suministrados y que no obedezcan a lo establecido en el presente procedimiento. No obstante, y en referencia a esta posible investigación, se llevará acabo con el debido cumplimiento del artículo 20.3 del ET así como la normativa de protección de datos, especialmente el artículo 87 de la LOPDGDD, que contempla los requisitos legales a tener en cuenta en el control realizado por el empleador y derivado del uso de medios digitales facilitados a los trabajadores.

## **5. Anexos**

N/A

## **6. Referencias**

- Plan de dirección de ciberseguridad de DMANAN.
- Política de Compliance
- P01 Sistema interno de información y denuncia
- P07 Procedimiento de RRHH