Política de Uso de Medios Tecnológicos

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Abril 2009	DSIGRT	Creación del Documento	Consejo de Administración
1.2	Abril 2019	DSIGRT	Revisión del Documento	Consejo de Administración
1.3	Julio 2025	DSIGRT	Revisión del Documento Inclusión de la regulación de la Inteligencia Artificia Unificación de formato con el resto del Marco Normativo	Consejo de Administración
1.4	Junio 2026	IS	Revisión del Documento	-

ÍNDICE

1. Ámbito de aplicación 4
2. Introducción 5
3. Objeto 6
4. Reglas generales de uso de los Medios Tecnológicos 9
5. Reglas específicas relativas a equipos/hardware 12
6. Reglas específicas relativas al software 12
7. Reglas específicas aplicables a los usuarios del correo electrónico 15
8. Reglas específicas de uso relativas a Internet 18
9. Reglas específicas relativas a medios audiovisuales y de geolocalización 20
10. Reglas específicas de uso relativas a las redes de datos 21
11. Reglas específicas de uso relativas a las redes sociales 23
12. Reglas específicas de uso relativas a los Sistemas de IA 25
13. Facultad de vigilancia del uso adecuado de los medios tecnológicos 27
14. Derecho a la desconexión digital 30
15. Garantías de información de los representantes legales y de las personas trabajadoras y de recepción de esta política 31
16. Suspensión o finalización de la relación con el usuario 32
17. Gestión y respuesta de alertas e incidentes de seguridad 33
18. Información básica de protección de datos 34

1. Ámbito de aplicación

La presente Normativa tiene el carácter de política corporativa y, por lo tanto, es de aplicación a todas las sociedades del Grupo FCC, con independencia de la actividad o lugar de realización de dicha actividad.

No obstante, lo anterior, y respecto de su aplicación en países distintos de España, se habrá de atender en todo caso a la normativa local y a la política interna que resulte de aplicación.

Fomento de Construcciones y Contratas, S.A., en su condición de sociedad cabecera del Grupo, es la responsable de establecer las bases, los instrumentos y los mecanismos necesarios para una adecuada y eficiente coordinación entre esta Sociedad y las demás sociedades que integran su Grupo. Todo ello sin perjuicio ni merma alguna del carácter de empleadora y de la capacidad de decisión autónoma que corresponde a cada una de dichas sociedades, de conformidad con el interés social propio de cada una de ellas y de los deberes que los miembros de sus órganos de administración mantienen hacia todos sus accionistas.

2. Introducción

Los sistemas informáticos, las aplicaciones de mensajería y correo electrónico, la utilización de Internet, redes sociales, redes de datos y de otros dispositivos se han convertido en herramientas necesarias e importantes para la operación de cada Organización.

Las Empresas del Grupo FCC, en adelante, Grupo FCC, FCC o la Empresa, proveen a su personal con distintos Medios Tecnológicos, cuyo propósito es realizar funciones relacionadas con su puesto de trabajo y garantizar que el personal tiene a su alcance las herramientas tecnológicas necesarias para poder desempeñar su trabajo.

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 Tecnológicos, salvaguardar la propiedad intelectual, prevenir supuestos de responsabilidad frente a terceros, y generar evidencias de las infracciones que se puedan cometer utilizando los Medios Tecnológicos.

Finalmente, es prioritario para estas políticas informar al personal y a sus representantes de las facultades empresariales de vigilancia que sobre tales Medios le reconoce la normativa al Grupo FCC, así como de su justificación y de los medios a utilizar al respecto.

3. Objeto

La presente política (en adelante, “la Política”) se enmarca dentro de la normativa interna del Grupo FCC, y desarrolla los principios recogidos en el Código Ético y de Conducta del Grupo.

Las finalidades de la Política son fundamentalmente las que se indican seguidamente:

- Su principal objetivo es garantizar que los usuarios de los medios tecnológicos hagan un uso adecuado, responsable y lícito de los mismos, protegiendo en todo caso la seguridad de la información.

  En el uso de dichos medios tecnológicos se incluye el uso conforme a las directrices establecidas en el Grupo FCC y a la legislación aplicable de los sistemas de Inteligencia Artificial que se desarrollen, implanten y utilicen en FCC y que se rigen por lo establecido en la “Política de Desarrollo y Uso aceptable de sistemas de Inteligencia Artificial en el Grupo FCC” y en el resto de normativa interna desarrollada.

A los efectos de la presente Política, debe significarse que:

- El término “usuario” o “usuarios” utilizado a lo largo del documento comprende al personal laboral o de otra naturaleza del Grupo FCC con contrato en vigor o en suspenso -o con obligaciones postcontractuales trascedentes para esta Política- y su contenido aplica a todas las Empresas del Grupo FCC sin excepción, y en tanto se mantenga la cesión y uso de medios tecnológicos. Cualquier referencia al contrato de trabajo, a personas trabajadoras o a la relación laboral, debe considerarse extensible a otros tipos de prestación de servicios de carácter civil o mercantil.
- Entre los medios tecnológicos (en adelante, “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, (c) servicios de Internet, Intranet, redes sociales, 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 por el Grupo FCC, (e) teléfonos fijos, teléfonos móviles, smartphones, GPS, etc., y (f) drones, robots, chatbots, vehículos inteligentes y sensores. Debe entenderse comprendido en lo anterior cualquier otro elemento o innovación tecnológica que pueda desarrollar, implantar, utilizar o adquirir el Grupo FCC en lo sucesivo, tales como sistemas que utilicen inteligencia artificial o cadena de bloques (*blockchain*, por su denominación en inglés).

- Permitir que el Grupo FCC ejerza el debido control para tratar de prevenir que se utilicen los Medios Tecnológicos para incurrir, entre otras, en conductas prohibidas tales como las que se relacionan a continuación:
    - Acosar o discriminar a personas trabajadoras o a terceros.
    - Atentar contra la dignidad, la intimidad y otros derechos fundamentales de las personas trabajadoras o de terceros.
    - Difamar, calumniar, injuriar o cualquier otro atentado contra el buen honor, reputación e imagen de Empresas del Grupo FCC, de sus personas trabajadoras o de terceros.
    - Revelar información confidencial, durante o con posterioridad a la terminación del contrato de trabajo o de prestación de servicio.
    - 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.
    - Atentar contra la seguridad del Grupo FCC y sus activos tangibles e intangibles (propiedad de bienes, derechos de propiedad intelectual e industrial, fondo comercial, reputación, buena imagen, etc.).
    - Poner en riesgo la seguridad y la estabilidad de los equipos, los sistemas, o la información contenida en ellos.
    - Realizar actos de competencia desleal contra el Grupo FCC.
    - Incumplir los contratos o relaciones con terceros.
    - 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.
    - Borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles, de forma intencionada o con negligencia grave, datos o programas informáticos del Grupo FCC.
    - Desarrollar cualquier otra conducta que suponga un incumplimiento del Código Ético y de Conducta que rige en el Grupo FCC.

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

- En el supuesto de que se detecte un uso (o intento de uso) indebido de los Medios Tecnológicos o para comprobar el correcto cumplimiento por sus personas trabajadoras de sus obligaciones laborales el Grupo FCC pueda adoptar las medidas que resulten necesarias; entre ellas, poner fin a las conductas prohibidas, y adoptar las medidas disciplinarias correspondientes. Todo ello, respetando los derechos de las personas trabajadoras y los requisitos que se establecen en la normativa de aplicación.

El Grupo FCC se reserva el derecho de modificar esta Política en cualquier momento, adaptándola a los cambios y evolución tecnológica según sea conveniente y/o necesario, sin perjuicio de informar debidamente a los destinatarios de la misma.

4. Reglas generales de uso de los Medios Tecnológicos

a) Los Medios Tecnológicos son herramientas de trabajo de la Empresa por lo que el uso de los mismos debe estar destinado al cumplimiento de las prestaciones para las que fue contratado el usuario, debiendo utilizarse de forma adecuada a su naturaleza y a sus fines profesionales.

b) Los Medios Tecnológicos y la información contenida o gestionada a través de ellos, son titularidad de la Empresa, y en base a ese carácter de instrumentos de trabajo, ambos están sujetos en cualquier momento a la inspección, monitoreo y auditoría por parte de ésta. En consecuencia, la persona trabajadora no tiene expectativa de privacidad alguna en el uso de los Medios Tecnológicos.

c) No obstante lo anterior, se autoriza un uso privado de los mismos, siempre que sea moderado y puntual y sin perjudicar las responsabilidades laborales y de productividad. Dicho uso no generará expectativa de privacidad ni será impedimento para que la Empresa pueda acceder a la información profesional almacenada en los distintos dispositivos que emplee el usuario, por lo que éste ha de abstenerse de incluir aspectos relacionados con su privacidad que no desee su conocimiento por terceros. En especial, no está permitido titular emails o mensajes como personales con expectativa de intimidad o almacenar información personal en carpetas identificadas como tales en los Medios a los que se refiere esta política.

d) Los diferentes permisos de acceso a los Medios Tecnológicos, y a la información, ubicada en las instalaciones de FCC, o en entornos contratados por el Grupo FCC, 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.

   Las conexiones remotas a la red de FCC solamente se realizarán a través de los Medios destinados a tal fin, siendo éstos la única vía permitida de acceso, y siempre previa autorización de la División de Sistemas y Tecnologías de la Información.

   Todos los equipos de externos que pretendan conectarse a la red de la Empresa deberán tener implantados y correctamente actualizados los controles de detección, prevención y corrección de amenazas, tales como software malicioso o phishing. Asimismo, será necesario que tengan actualizado tanto el sistema operativo como el resto del software instalado o gestionado a través de sus equipos.

e) Cada usuario deberá mantener el debido cuidado de los Medios Tecnológicos que se le asignen, impidiendo el acceso (incluida la mera visualización) de otras personas a las herramientas de trabajo que se le han asignado para su uso.

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

Con carácter específico, deberá atenderse a la Norma de Seguridad de las Contraseñas que se encuentre vigente en cada momento. Todos los Medios Tecnológicos se configurarán de forma que después de 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.

f) Prevención ante software malicioso: los software maliciosos más conocidos son los virus y troyanos informáticos, pero este término es más amplio y hace referencia a cualquier programa que tenga como objetivo infiltrarse en los sistemas sin el conocimiento del usuario, con la finalidad de dañar la seguridad (o tomar el control) de esta máquina o de otros sistemas.

Los controles de prevención, detección y corrección de los que disponen los sistemas de información pueden no ser suficientes para luchar contra el software malicioso. Para protegerse de estas amenazas, el usuario debe, entre otros:

- Mantener especial cuidado cuando utilice Internet o el correo electrónico, ya que estos medios suelen ser las vías más comunes de transporte y transmisión de software malicioso.
- No descargar ni utilizar software o archivos ejecutables de origen desconocido o no corporativo.
- Ponerse inmediatamente en contacto con Servicedesk y con el Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos (sdseguridad@fcc.es) cuando sospeche de la existencia de software malicioso y/o cualquier anomalía similar.

g) La vulneración por parte de un usuario de cualquier regla de la presente Política será considerada como un incumplimiento contractual que puede derivar en la adopción de las medidas disciplinarias que correspondan de conformidad con la normativa vigente.

h) A fin de asegurar evidencias digitales que de otra manera pudieran ser destruidas, el Grupo FCC podrá apartar al usuario de los Medios Tecnológicos que tenga asignados en cualquier momento y sin previo aviso, debiendo el usuario ponerlos inmediatamente a disposición del Grupo.

5. Reglas específicas relativas a equipos/hardware

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, faxes, impresoras, monitores, smartphones, dispositivos USB, discos duros externos, tarjetas de memoria, tabletas, teléfonos fijos, teléfonos móviles o dispositivos similares o equivalentes.

Son de aplicación las siguientes reglas:

- Instalación y mantenimiento de equipos: el usuario no podrá realizar ningún cambio, manipulación o modificación sin la autorización expresa y previa de la División de Sistemas y Tecnología de la información. La instalación de nuevos equipos deberá realizarse únicamente a través del departamento correspondiente, estando prohibida la instalación de cualquier elemento hardware adicional sin autorización por parte del Grupo FCC. Cualquier tipo de mantenimiento distinto deberá ser consultado y aprobado previamente por la misma.
- En caso de pérdida o robo de un dispositivo portátil que contenga información clasificada como sensible o que contenga datos personales se debe informar, de forma inmediata, al responsable de los datos perdidos y a la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos (sdseguridad@fcc.es) para permitir que se puedan tomar las medidas oportunas para minimizar los posibles impactos y poder cumplir con los requisitos exigidos por las normativas locales de aplicación.
- En las instalaciones de FCC se debe trabajar con Medios Tecnológicos de su titularidad. En caso de que fuera necesario introducir o utilizar Medios Tecnológicos ajenos, estos deberán cumplir, como mínimo, con los requisitos técnicos y de seguridad que se establezcan en este documento y/o los detallados por la Empresa en cada momento.
- La utilización en las instalaciones de FCC y durante el tiempo de trabajo de cualquier Medio Tecnológico propio de la persona trabajadora 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.
- Queda prohibida la conexión de los Medios Tecnológicos propios de la persona trabajadora a la red corporativa salvo que medie autorización expresa y previa de la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos.

6. Reglas específicas relativas al software

El software es el conjunto de elementos lógicos de un sistema de información, tales como aplicaciones, programas, sistema operativo, bases de datos, etc.

Son de aplicación las siguientes reglas:

- **Adquisición de software:** las aplicaciones y programas de los que FCC es dueño o titular del derecho de uso serán contratados según los procedimientos vigentes en el Grupo FCC y teniendo en cuenta los estándares establecidos por la División de Sistemas y Tecnologías de la Información.
- **Instalación de software**: cada equipo contendrá las aplicaciones y programas necesarios para facilitar el correcto desempeño de las funciones de los usuarios a los que se destina. El usuario debe justificar sus peticiones de instalación de nuevo software, que deberán ser aprobadas por la División de Sistemas y Tecnologías de la Información. Queda prohibido, además de las conductas prohibidas con carácter general en la presente Política:
    - Descargar e instalar, sin autorización de la División de Sistemas y Tecnologías de la Información, o el Departamento en el que ésta haya delegado, cualquier programa o aplicación informática a iniciativa propia del usuario.
    - Descargar, instalar, acceder y utilizar software no licenciado o “pirata” (conducta ilícita que puede conllevar graves responsabilidades de tipo penal y civil dependiendo de la regulación nacional de cada Estado, además de poner en riesgo evidente tanto los equipos informáticos como la información que contienen o gestionen).
    - Instalar en los equipos certificados digitales que puedan utilizarse para representar a cualquier Empresa del Grupo FCC, sin previa autorización del Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos.
    - Copiar, sin autorización, el software o aplicaciones instalados en los Medios Tecnológicos o tratar de descompilarlos, hacer ingeniería inversa, acceder a su código fuente o acceder por medios no autorizados a las mismas.
    - Utilizar software que permita inhabilitar, modificar o dejar sin efecto las medidas de seguridad y controles establecidos por la Empresa o realizar acciones destinadas a saltarse dichos controles.
    - Toda pretensión de instalación de software corporativo que pueda alterar las configuraciones de seguridad (p.ej. modificar reglas de *firewalling* del sistema operativo, etc.) o inhabilite las herramientas de seguridad de la información (p.ej. deshabilitar el EDR, etc.) deberá estar previamente alineado y autorizado por la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos del Grupo FCC.

- **Mantenimiento de software:** El mantenimiento del software comprende todo su ciclo de vida (instalación y configuración, mantenimiento, reparación, destrucción y pruebas). El usuario no podrá realizar ninguna acción de mantenimiento sobre las aplicaciones en ninguna de las fases de su ciclo de vida, salvo autorización expresa de la División de Sistemas y Tecnologías de la Información.

7. Reglas específicas aplicables a los usuarios del correo electrónico

El correo electrónico (en inglés: *electronic mail*, comúnmente abreviado e-mail o email) es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica. Su utilización ha de hacerse, fundamentalmente, con fines profesionales, y una utilización con fines personales ha de ser ocasional. En ambos casos, la persona trabajadora no debe incluir información que pueda afectar a temas privados o íntimos cuyo conocimiento por terceros no desee, dadas las facultades de control de la Empresa a las que ya se han hecho referencia en esta Política, sin que pueda existir ninguna expectativa de privacidad o intimidad al respecto.

Adicionalmente, son de aplicación las siguientes reglas:

a) Los correos electrónicos masivos entrañan problemas para la Empresa, dado que, entre otros daños, pueden colapsar la red y generar pérdidas muy costosas en tiempo de trabajo de todos los usuarios que reciben el mensaje. Por ello, con carácter general, 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 información, comunicación o difusión distintas del correo electrónico (como por ejemplo: circulares, noticias, anuncios, etc. colgados en Intranet), que, por una parte, no pongan en riesgo la red y que, por otra, no provoquen la interrupción de la actividad laboral de los destinatarios.

   En el caso de que un usuario necesite enviar por razones del negocio un correo masivo, deberá dirigirse a la División de Sistemas y Tecnologías de la Información para que inicie el procedimiento de envío de correos electrónicos masivos.

   La utilización de listas de distribución de correo electrónico se realizará restrictivamente para la organización del trabajo o la explotación del negocio.

b) Con el objeto de evitar la degradación del servicio de correo y la saturación involuntaria de los buzones de los usuarios, el volumen de los documentos, archivos, etc., que se adjunten a un correo electrónico no deberán superar en ningún caso el tamaño máximo autorizado por la División de Sistemas y Tecnologías de la Información.

   En el caso de que por razones de negocio sea necesario anexar un volumen superior al permitido, el usuario deberá solicitar autorización a la División de Sistemas y Tecnologías de la Información.

c) El uso correcto del servicio de correo electrónico, que en ningún caso debe perjudicar las responsabilidades laborales de la persona trabajadora o su productividad, supone que el

usuario no debe utilizarlo ni para las acciones prohibidas con carácter general en esta Política ni para las siguientes:

- Vulnerar lo establecido en las Políticas de Gestión de la Información, la de Ciberseguridad y Seguridad de la Información de Grupo FCC y, cualquier otra normativa interna.
- Acceder y/o utilizar la cuenta de correo de otro usuario sin autorización previa.
- Suplantar (o intentar suplantar) a otro usuario utilizando cualquier medio.
- Simular la pertenencia a una compañía ajena al Grupo FCC.
- Iniciar o participar en la propagación de cartas encadenadas o acciones análogas.
- Utilizar buzones privados de correo ofrecidos por cualquier proveedor de Internet para fines profesionales relacionados con el Grupo FCC.
- Utilizar el correo electrónico como herramienta de comunicación con fines de venta u otros de naturaleza comercial independiente a la Empresa.
- Enviar o solicitar mensajes, información, archivos o materiales con contenidos de carácter explícitamente sexual, de discriminación, que puedan llegar a ser ofensivos, difamatorios, amenazantes o insultantes para cualquier persona.
- Enviar o solicitar mensajes que incluyan contenidos audiovisuales, musicales, multimedia o de cualquier otra clase que, no estando relacionados con las funciones del usuario, puedan dificultar el tráfico de la red corporativa.
- Reenviar de forma dolosa correos electrónicos emitidos o recibidos (o sus archivos adjuntos) mediante su cuenta de correo electrónico corporativo a cuentas de correo electrónico externas. Asimismo, tampoco debe utilizar el sistema de copia oculta (COO) para remitir la información referida a cuentas externas.
- Enviar correos electrónicos de carácter profesional o relacionados con las Empresas del Grupo FCC desde direcciones de correo privadas del usuario (cuentas *Hotmail*, *Gmail* u otras) o desde dominios ajenos al Grupo FCC.
- Realizar o intentar realizar las acciones técnicas que impidan mantener online los correos de un buzón corporativo de los últimos seis meses, de forma que se obstaculice al Grupo FCC mantener dicha copia de seguridad de los mismos.

En este sentido, en relación con los correos electrónicos enviados o recibidos por medio del servidor de correo de la Empresa y otros canales susceptibles de contener información y,

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 con los clientes, proveedores, poderes públicos, administración y personas trabajadoras de la Empresa, como al control del cumplimiento por parte de los usuarios de las instrucciones establecidas en el presente documento.

Las reglas anteriores, con las adaptaciones necesarias, se aplican a cualquier otro sistema de comunicación digital, especialmente los servicios de mensajería o similares.

8. Reglas específicas de uso relativas a Internet

Internet es la red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

Las Empresas del Grupo FCC facilitan a los usuarios el acceso a Internet en función de las responsabilidades o tareas que se les hayan asignado. El usuario es responsable del material que visualice, acceda y/o descargue de Internet. Por tanto, debe realizar un uso responsable y lícito de la Web.

Como es el caso con los otros Medios del Grupo, el usuario sólo puede utilizar Internet facilitado por la Empresa con fines lícitos y profesionales y sin perjudicar sus responsabilidades laborales y de productividad. Un uso con fines personales sólo puede ser ocasional. En ambos casos, el usuario no debe revelar, con sus conexiones, información alguna que pueda afectar a temas privados o íntimos que no desee sea conocido por terceros, dadas las facultades de control de la Empresa a las que ya se han hecho referencia en esta Política y aplicables también a estas conexiones, sin que pueda existir ninguna expectativa de privacidad o intimidad al respecto.

Queda terminantemente prohibido el uso de Internet para las conductas prohibidas recogidas en esta Política y además para:

- Descargar y/o instalar en los equipos software, ficheros ejecutables o bases de datos desde Internet. Si lo necesitara el usuario para el desempeño de las funciones, deberá solicitar autorización a la División de Sistemas y Tecnologías de la Información.
- Utilizar software de descarga o intercambio de archivos o ficheros extremo a extremo (*peer to peer*), así como cualquier otro software de descarga de música, películas, vídeos y/o juegos o servicios de reproducción multimedia con fines de ocio, o el visionado de cualquier vídeo y/o producto multimedia en modalidad de *streaming* o similar.
- Acceder a sitios web expresamente prohibidos por las políticas internas del Grupo o que contengan contenidos inapropiados o que alberguen dudas sobre su licitud, evitando asimismo aquellos sitios Web que automáticamente redireccionen a otros en los que no sea posible establecer control o supervisión alguna. Igualmente estará prohibido tratar de modificar los parámetros de seguridad implementados en la Red y Sistemas de Internet Corporativo para tratar de acceder a dichos sitios web.
- Utilizar la conexión facilitada por FCC para el acceso a Internet con cualquier dispositivo particular o ajeno al Grupo, salvo autorización previa por parte de la División de Sistemas y Tecnologías de la Información.
- Incluir o cargar datos de carácter personal, información restringida (confidencial, secreta e interna), sensible o estratégica para FCC en las páginas Web/URL que dispongan de

inteligencia artificial, siempre que no se encuentren previamente autorizadas por la División de Sistemas y Tecnologías de la Información.

- Utilizar sistemas, interconectar con las aplicaciones corporativas y/o utilizar páginas Web/URL que dispongan de inteligencia artificial, salvo previa autorización expresa por la División de Sistemas y Tecnologías de la Información.

Cuando se acceda a Internet o a cualquier otra red de ordenadores, se deberán cumplir los requisitos técnicos y de seguridad especificados por el Grupo FCC en la correspondiente normativa interna.

9. Reglas específicas relativas a medios audiovisuales y de geolocalización

Por razones de supervisión y control de la prestación del trabajo y de seguridad de personas y bienes o de evitación de riesgos laborales, la Empresa podrá instalar medios de captación de imágenes o movimientos (cámaras, sensores, etc.) en las instalaciones u otros medios técnicos de su propiedad. De dicha instalación se informará inicial y regularmente tanto a los representantes legales como a las personas trabajadoras y la misma se realizará con la mínima limitación de los derechos de intimidad y a la propia imagen de los afectados, y con exclusión de lugares tales como vestuarios o servicios.

Los medios de registro de sonidos sólo podrán ser utilizados cuando sean estrictamente necesarios por aquellas razones de supervisión o de seguridad o prevención de riesgos, con la mínima afectación de los derechos de los afectados e informando adecuadamente a éstos y a sus representantes.

Igualmente, por razones de supervisión y control de la prestación de trabajo o de seguridad de las personas y bienes o de evitación de riesgos laborales, la Empresa podrá instalar en sus vehículos y otros medios de su propiedad sistemas de geolocalización adecuados a tales efectos. De dicha instalación se informará inicial y regularmente tanto a los representantes legales como a las personas trabajadoras y la misma se realizará con la mínima limitación de su derecho de intimidad.

Dichos sistemas deberán ser desconectados exclusivamente cuando los medios portadores de tales sistemas estén en posesión de las personas trabajadoras en periodos temporales que no tengan la consideración de tiempo de trabajo, de acuerdo con las reglas que se determinen al respecto.

A los datos que puedan obtenerse por los medios y sistemas contemplados en este apartado les será de aplicación la normativa de protección de datos personales prevista al efecto.

10. Reglas específicas de uso relativas a las redes de datos

Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos.

La utilización de las redes de datos de las empresas del Grupo FCC debe regirse por el uso correcto de los recursos que las componen, quedando expresamente prohibidas las siguientes actividades además de las prohibidas con carácter general en la Política:

- Intentar acceder, leer, descargar, borrar, copiar o modificar los archivos de otros usuarios sin el conocimiento y consentimiento de su autor, o en su caso, de la Empresa.
- Intentar acceder a áreas restringidas de los sistemas informáticos de FCC, de sus otros usuarios o de terceros.
- Destruir, alterar, inutilizar, eliminar o dañar los datos, información, programas o documentos electrónicos de FCC, de sus otros usuarios, o de terceros.
- Intentar aumentar y/o modificar (sin autorización) el nivel de privilegios de un usuario en el sistema.
- Intentar descifrar las claves, sistemas, algoritmos de cifrado o cualquier otro elemento de seguridad que intervenga en los procesos técnicos y telemáticos del Grupo FCC.
- Obstaculizar voluntariamente el acceso de otros usuarios a los equipos y sistemas de FCC, por el consumo masivo de los recursos informáticos y telemáticos, así como realizar acciones que dañen, interrumpan o generen errores en dichos equipos y sistemas.
- Introducir programas maliciosos, virus, troyanos, macros, scripts, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los recursos informáticos y/o en la información en ellos gestionada.
- Introducir, descargar, reproducir o distribuir programas informáticos no autorizados expresamente por FCC, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros.
- Poner a disposición de terceros no autorizados la información, los equipos y el software suministrados por la Empresa.
- Compartir recursos e información (ficheros, directorios, etc.) sin los mecanismos de seguridad necesarios (en función de su riesgo y de la tipología de la información) y disponibles en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.

- Conectarse mediante los medios tecnológicos del Grupo FCC a través de servicios de VPN, proxies anónimos o cualquier otro servicio de anonimización no autorizado por el Grupo FCC.
- Acceder a los medios tecnológicos del Grupo FCC a través de cualquier navegador que permita conectividad desde/hasta la Dark Web o Deep Web (como p.ej. navegador Tor).

11. Reglas específicas de uso relativas a las redes sociales

La presente Política, que desarrolla lo dispuesto al respecto en el Código Ético y de Conducta, se aplica al uso de las redes sociales tanto para el uso corporativo como personal, esto último exclusivamente en los casos en que ese uso personal pueda tener consecuencias o trascendencias significativas para la Empresa. También se aplica para su uso ya sea durante la jornada de trabajo o fuera de la misma, y se aplica independientemente de si se ha accedido a las redes sociales mediante equipos de la Empresa o equipos personales de la persona trabajadora.

En este sentido, la imagen del Grupo constituye uno de sus activos más valiosos que, como tal, debe ser protegido, y ello con el fin de preservar la confianza de los accionistas, clientes, socios, personas trabajadoras, proveedores, autoridades y de la sociedad en general.

La Empresa utiliza sus redes corporativas de acuerdo con los principios, valores y reglas reflejados en sus políticas internas, y muy en especial en su Código Ético y de Conducta, así como con la legislación vigente. Todo usuario que acceda a tales redes debe hacerlo en consonancia con esa regulación.

Por lo tanto, si las funciones de una persona trabajadora requieren que haga uso de la red corporativa, el mismo debe hacerse de forma responsable y debe tener la adecuada autorización al respecto. Cualquier información publicada en los canales internos de la Empresa no puede ser publicada en medios externos sin la autorización de la Dirección de Comunicación, Marketing Corporativo y Marca.

En todo caso, el usuario nunca debe utilizar los canales corporativos para sus propias comunicaciones personales. El usuario tampoco debe crear o registrar una cuenta o canal en las redes sociales en nombre de la Empresa, ni de algún miembro de la misma o propio, sin la autorización previa del responsable de la Empresa. Sólo la Dirección de Comunicación, Marketing Corporativo y Marca está autorizada a abrir canales digitales (redes sociales, webs, blogs etc.) en nombre de la Empresa. En caso de la detección de perfiles no autorizados por el Grupo FCC por los que se haga un uso no autorizado de las marcas/logos o se suplante la identidad de éste (o de cualquiera de las empresas que lo componen) podrá llevar la inmediata solicitud de eliminación del perfil no autorizado a la red o sitio Web que corresponda.

La utilización en las instalaciones de FCC y durante el tiempo de trabajo de redes sociales personales de la persona trabajadora 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.

El uso personal de las redes sociales no puede realizarse incumpliendo el Código Ético y de Conducta, en particular, en lo referente a la discriminación, el acoso o la intimidación de otros

miembros de la Empresa o de terceros relacionados con la misma. Asimismo, no pueden publicarse comentarios sobre aspectos empresariales confidenciales o reservados de la Empresa, u otros que puedan perjudicar la reputación de la misma.

12. Reglas específicas de uso relativas a los Sistemas de IA

En un entorno laboral, los sistemas de IA (modelos o sistemas de Inteligencia Artificial, en adelante "**Sistema de IA**") pueden mejorar la eficiencia, optimizar procesos y aumentar la productividad al automatizar tareas, analizar grandes volúmenes de datos o apoyar en la toma de decisiones. Sin embargo, su uso debe ser responsable, ético y alineado con los principios de transparencia, seguridad y equidad.

El uso de Sistemas de IA por las personas trabajadoras que trabajen para las empresas del Grupo FCC debe realizarse siguiendo las siguientes directrices:

- Ciberseguridad: se debe utilizar exclusivamente Sistemas de IA aprobados por el Grupo FCC, por lo que queda prohibido el uso de plataformas o servicios no autorizados.
- Revisión de instrucciones y Términos y Condiciones: los Sistemas de IA tienen Términos y Condiciones y, en muchas ocasiones, manuales de instrucciones. Sin perjuicio de la formación sobre Sistemas de IA que se imparta por el Grupo FCC, el/la usuario/a debe leer dichos textos antes del uso de los Sistemas de IA, en caso de necesitar mayor detalle para conocer su finalidad, características, carencias, etc.
- Supervisión humana: no se debe asumir que los resultados generados por Sistemas de IA son siempre correctos o exentos de errores o sesgos, por tanto, éstos deben ser revisados y validados antes de su uso o aplicación, en particular y de forma obligatoria cuando se trate de Sistemas de alto riesgo. Esta revisión consiste en una validación sencilla de la veracidad y exactitud del resultado.
- Calidad de los datos de entrada: al introducir datos en Sistemas de IA, es fundamental asegurarse de que sean representativos y precisos para evitar sesgos o resultados inexactos.
- Transparencia y notificación: la información y la transparencia serán especialmente relevantes en las prácticas de aquellos Departamentos del Grupo FCC vinculados, en su caso, a Sistemas de IA de alto riesgo, tal y como se definen en el artículo 6.2 y el Anexo III del Reglamento IA, Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.
- Propiedad intelectual: el contenido generado por Sistemas de IA como audios, imágenes, videos, etc. puede estar protegido por derechos de propiedad intelectual o industrial (por ejemplo, si incluye una marca o una obra de arte). Por tanto, el uso de dicho contenido debe

estar debidamente alineado con la legislación aplicable y las políticas y prácticas del Grupo FCC.

13. Facultad de vigilancia del uso adecuado de los medios tecnológicos

Búsqueda automática o manual

De acuerdo con las reglas establecidas con anterioridad, y especialmente respecto a las garantías de información regular a los usuarios y sus representantes sobre los derechos de supervisión y control de la Empresa y la ausencia de expectativa de intimidad o privacidad que aquéllos tienen en el uso de los Medios Tecnológicos, dicha facultad de vigilancia tendrá como principales reglas generales las siguientes:

- Como regla general, existirán dos tipos de controles sobre los Medios Tecnológicos. Uno de carácter regular, preventivo y aleatorio, tendente a identificar cualquier utilización de aquellos medios contraria 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 la Empresa o de su personal. Otro, de carácter investigador y específico, cuando la Empresa tenga indicio de que un usuario o grupo de usuarios están realizando conductas o actos o contrarias a la Política .
- En equipos, el acceso realizado por el Grupo FCC consistirá en detectar mediante búsqueda automática o manual si en los equipos se almacena software ilegal que vulnere (o pueda vulnerar) los derechos de propiedad intelectual o industrial de terceros, o no autorizado por la Empresa. Igualmente consistirá también en buscar mediante búsquedas automáticas o manuales términos libres que pudieran revelar conductas indebidas, como acoso, discriminación, competencia desleal, revelación de secretos, etc. Asimismo, consistirá también en identificar las llamadas realizadas desde o recibidas en un Medio Tecnológico.
- Respecto a los buzones de correo electrónico y a la información contenida en los correos electrónicos consistirá en detectar mediante búsquedas automáticas o manuales términos libres que pudieran revelar conductas indebidas como acoso, discriminación, competencia desleal, revelación de secretos, etc.

  Se almacenará una copia de seguridad completa de todos los elementos del correo electrónico enviados o recibidos por medio del servidor de correo de FCC y otros canales susceptibles de contener información.

  La facultad de monitorización y control sobre las cuentas de correo electrónico corporativas no se limita al contenido de los mensajes emitidos y recibidos por medio de las mismas, sino también a las cabeceras, a los datos de tráfico y a cualquier otra información relativa a los correos electrónicos.

- Respecto al uso de Internet y de la Intranet por el usuario, se accederá automáticamente al registro de los sitios web accedidos por el usuario para detectar contenidos ajenos a la actividad del Grupo FCC (por ejemplo, hora y fecha de inicio de sesión, dirección IP que permite identificar el equipo desde el que se accede, usuario, página web o url accedida, fecha y hora de acceso). Igualmente, se buscarán términos libres que pudieran revelar conductas indebidas como acoso, discriminación, competencia desleal, revelación de secretos, etc.
- La Empresa podrá igualmente bloquear la posibilidad de realizar determinadas acciones (por ejemplo, compartir determinada información por cualquier medio electrónico), y crear una alerta en caso de que un usuario las intente realizar.
- Los criterios y reglas expuestos se aplicarán de manera análoga a los otros Medios puestos a disposición de los usuarios.

Extracción de información

En el supuesto de que se detecte o existan sospechas fundadas de cualquier incumplimiento de la presente Política, el Grupo FCC evaluará la posibilidad de extraer información de los activos corporativos implicados con el fin de comprobar si se ha incurrido o no en la conducta indebida, en aras de adoptar las medidas pertinentes dentro del poder de dirección y control que le compete.

Toda solicitud realizada por un área, departamento o función interna del Grupo FCC, con independencia de su dependencia funcional o jerárquica, para la obtención de información relacionada con el uso de Medios Tecnológicos debe seguir el proceso correspondiente normado en el Grupo, y cumplir con los siguientes requisitos de idoneidad, necesidad, razonabilidad y proporcionalidad ya incluidos en las facultades de vigilancia y control previstas en esta Política:

Ser idónea y necesaria	Se considera que no existe otra medida menos intrusiva para los derechos de la persona trabajadora que permita la obtención de la información necesaria para el asunto objeto de análisis o investigación, o que, de existir, no es suficiente o viable.
Ser razonable	Se debe a motivaciones objetivas, justificadas y no arbitrarias, no incurriendo en abuso de los derechos que la ley reconoce al empleador.

Ser proporcional	Es respetuosa con el derecho a la intimidad, procurando su mínima injerencia, y se limita únicamente al asunto o asuntos objeto de investigación o análisis y a la persona o personas relacionadas, en un periodo de tiempo concreto. En todos los casos se identificarán de términos clave pertinentes y adecuados a la finalidad que se quiere conseguir, no utilizando términos genéricos que no permitan acotar suficientemente los contenidos que incluyan información de relevancia. Podrán ser palabras o cadenas de palabras y/o caracteres, así como direcciones de correo electrónico o nombres propios.
Ser debidamente aprobada	Debe recibir el visto bueno por parte de los responsables oportunos en cada caso.

14. Derecho a la desconexión digital

Los usuarios de los Medios Tecnológicos de la Empresa que impliquen información y comunicación 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 inaplazables propias de su puesto de trabajo.

Todas las Empresas del Grupo FCC están comprometidas con el bienestar de sus personas trabajadoras 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.

A fin de promover y garantizar el derecho a la desconexión digital la Empresa elaborará acciones de formación, sensibilización del personal sobre un uso razonable de las herramientas tecnológicas.

Cuando el usuario deba desarrollar de forma regular y convenientemente autorizada su trabajo a distancia, incluyendo el realizado en su propio domicilio, o esté sometido a una distribución del tiempo de trabajo especialmente flexible, también estará sometido a la anterior regulación respecto a la desconexión digital, con las especialidades que puedan contemplarse.

15. Garantías de información de los representantes legales y de las personas trabajadoras y de recepción de esta política

La Empresa informará inicialmente tanto a los representantes legales de las personas trabajadoras como a estas últimas de la implantación, desarrollo y condiciones de establecimiento, uso y finalidad de los Medios Tecnológicos y sistemas contemplados en esta Política, así como de sus actualizaciones. Dicha información podrá realizarse tanto de forma individualizada como colectiva, y se desarrollará por cualquier medio, digital o físico, que garantice su recepción y conocimiento efectivos. Tanto los representantes como las personas trabajadoras deberán acusar recibo de tal información y conocimiento.

16. Suspensión o finalización de la relación con el usuario

La cesión del uso de los Medios a los usuarios para la realización de su prestación profesional sólo se mantiene mientras dure la relación con la Empresa.

A partir del momento en el que se produzca la terminación de la relación por cualquier causa, se denegará el acceso a dichos Medios. La previsión anterior podrá aplicarse en el caso de apertura de expediente contradictorio por comisión de falta muy grave por parte de un usuario.

No obstante lo anterior, de forma coetánea o inmediatamente previa a la terminación de la relación, se permitirá el acceso al usuario, bajo la supervisión de la División de Sistemas y Tecnología de Información o de la persona en la que delegue este Departamento, con la finalidad de que éste pueda borrar y/o extraer la información personal.

Tras la extinción de la relación laboral la Empresa accederá al Medio y a la información en él contenida sin limitación alguna, borrando en el caso de que no lo hubiera llevado a cabo la persona trabajadora la información personal.

En el supuesto de finalización de la relación con la Empresa, el usuario que tenga en su poder cualesquiera Medios tendrá que devolverlos en la fecha de extinción del contrato cumpliendo el proceso de devolución previsto.

A su vez, el responsable de un usuario que finalice su relación con la Empresa tendrá la obligación de solicitarle la devolución de los Medios.

Las reglas anteriores, con las adaptaciones que se consideren necesarias, podrán aplicarse también a las situaciones de suspensión de la relación laboral, especialmente aquellas de larga duración.

17. Gestión y respuesta de alertas e incidentes de seguridad

El Grupo FCC cuenta en su División de Sistemas y Tecnología de Información con un equipo de profesionales encargados de ofrecer soporte en todo lo relativo a las aplicaciones y herramientas de los sistemas de información.

Por su parte, la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos del Grupo FCC dispone de servicios de monitorización en materia de Ciberseguridad (por los que se revisa todo lo que ocurre en el entorno tecnológico, en todo momento, para detectar si existe cualquier tipo de amenaza para el Grupo FCC con la intención de aplicar cualquier tipo de medida técnica que ayude a reducir o mitigar los riesgos de seguridad detectados). Entre otros, destacan el centro de operaciones de seguridad (denominado SOC, por sus siglas en inglés), y servicios similares como Cyberthreats y Threat Hunting.

1. Cualquier usuario que sufra un incidente relativo a los sistemas de información deberá informar sobre éste de forma inmediata a la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos del Grupo FCC, sin realizar por su cuenta ninguna acción sobre el recurso que haya sufrido el incidente ni tampoco apagarlo, reiniciarlo o resetearlo. La Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos del Grupo FCC evaluará y clasificará lo antes posible la incidencia y dará una respuesta al usuario que haya sufrido el incidente.
2. Todo usuario deberá cumplir con el contenido de las alertas de seguridad de la información remitidas por la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos del Grupo FCC, así como responder a los requerimientos de información que puedan recibir por ésta con la finalidad de clarificar un determinado hecho o sospecha.

   En el supuesto de no obtener respuesta, en tiempo y forma, por parte del usuario, la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos del Grupo FCC podrá aplicar medidas técnicas y/o organizativas adecuadas para reducir o mitigar la posible amenaza para los Medios Tecnológicos (como el bloqueo de aplicaciones, aislamiento de equipo o servidor, desactivación del usuario, rotado de credenciales, revocación de sesiones activas, etc.).

18. Información básica de protección de datos

Información adicional sobre tratamiento de Datos Personales	
Responsable	Fomento de Construcciones y Contratas, S.A., con CIF A28037224, Dirección de Seguridad de la Información y Riesgos Tecnológicos. Federico Salmón, 13. 28016 Madrid. Web www.fcc.es y contacto en protecciondedatos@fcc.es
Finalidad	Evitar las fugas de información de las entidades del Grupo FCC, realizar un control de la actividad profesional, verificar que no se producen incumplimientos y/o usos indebidos y/o ilícitos de los Medios Tecnológicos, así como recopilar y tratar la seguridad de la información en los sistemas de la misma.
Legitimación	Finalidades basadas en el tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable (Entidad) y para la ejecución de un contrato, en su caso.
Derechos de interesados	Acceso, rectificación, supresión, portabilidad, limitación u oposición (cuando apliquen) mediante correo a protecciondedatos@fcc.es. Si consideras que no se han tratado tus datos según la normativa de protección de datos, puedes contactar directamente con la Delegada de Protección de Datos (protecciondedatos@fcc.es). En todo caso, podrás presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).
Información adicional	El Usuario podrá disponer de la información adicional y completa a través del apartado “Protección de Datos” ubicado en la Intranet de FCC (https://fccone.fcc.es/) o mediante petición a protecciondedatos@fcc.es o mediante la solicitud de la misma en formato papel al Dpto. de Recursos Humanos.