Tema 12

Normas de cumplimiento: Protección de datos. Prevención de Blanqueo de Capitales. Compromiso ético y transparencia. Seguridad de la Información y Ciberseguridad

Contenido

12.1. Protección de datos

12.1.1. Introducción

Protección de datos como derecho fundamental

Según el Diccionario Lengua Española (DLE), los **derechos fundamentales** son derechos que, por ser inherentes a la dignidad humana y por resultar necesarios para el libre desarrollo de la personalidad, son normalmente recogidos por las constituciones modernas asignándoles un valor jurídico superior.

La protección de las personas físicas en relación con el tratamiento de los datos es un derecho fundamental protegido por el artículo 18.4 de la Constitución Española de 1978, denominado por la jurisprudencia constitucional como derecho fundamental a la protección de datos personales.

> Artículo 18 CE:
>
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
>
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La Sentencia de 292/2000 del Tribunal Constitucional considera el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente del derecho a la intimidad, que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos quiere proporcionar a un tercero (sea el Estado o un particular), qué datos puede ese tercero recoger, además, ese derecho permite conocer a la persona que tiene sus datos personales y para qué los tiene, pudiendo oponerse a esa posesión o uso.

Asimismo, la Carta de los Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000, reconoce en su artículo 8 como derecho fundamental el derecho a la protección de datos de carácter personal.

Normativa comunitaria: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas y a la libre circulación de estos datos (en adelante RGPD o Reglamento General de Protección de Datos o Reglamento Europeo)

A) ¿Por qué surge el RGPD?

La rápida evolución tecnología y la globalización han planteado nuevos retos para la protección de datos personales. La magnitud de la recogida e intercambio de los datos ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales a una escala sin precedentes a la hora de realizar sus actividades. Las personas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de datos personales.

B) ¿Cuál es el objeto de la norma? Directiva 95/46/CE versus RGPD

Con la anterior normativa europea de protección de datos, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos y a la libre circulación de estos datos, la protección de datos en el territorio de la Unión se aplicaba de manera fragmentada, existiendo una percepción generalizada entre la opinión pública de que existen riesgos importantes en la protección de las personas físicas, en particular en relación con las actividades en línea.

Para una mejor comprensión, consideramos oportuno aclarar que las directivas europeas son actos legislativos que establecen objetivos que todos los países de la UE deben cumplir, si bien corresponde a cada país elaborar sus propias leyes sobre cómo alcanzar esos objetivos. En cambio, los Reglamentos Europeos son actos legislativos vinculantes y deben aplicarse en su integridad en toda la Unión Europea. El Reglamento Europeo es una norma directamente aplicable a los países miembros de la Unión Europea, que no requiere de normas internas de transposición —como si lo requieren las directivas europeas— ni tampoco, en la mayoría de los casos, de normas de desarrollo o aplicación.

La aprobación del Reglamento General de Protección de Datos o RGPD pretende garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar diferencias que dificulten la libre circulación de datos personales dentro del mercado interior; para ello es necesario un reglamento que proporcione seguridad jurídica y transparencia de los operadores económicos —como las empresas— y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidad para los responsables y encargados del tratamiento, con el fin de garantizar una

supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros.

El Reglamento General de Protección de Datos ha procedido a reforzar la seguridad jurídica y transparencia.

Con la aprobación del Reglamento General de Protección de Datos en lugar de la Directiva, la Unión Europea ha querido asegurarse de que se ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidad para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes para todos ellos.

El Reglamento General de Protección de Datos establece las normas relativas a la protección de datos en lo que respecta al tratamiento de datos personales y las normas relativas a la circulación de tales datos.

Legislación española: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (en adelante LOPDGDD o legislación española)

A) ¿Por qué surge la LOPDGDD?

La LOPDGDD es la ley española en materia de protección de datos de carácter personal.

Si bien el Reglamento Europeo es una norma de aplicación general a toda la Unión Europea, esta ha permitido que sus normas sean especificadas o restringidas por el derecho de la Unión o el de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprendidas por sus destinatarios. Los reglamentos, pese a su característica de aplicabilidad directa en los países miembros de la Unión Europea, en la práctica, pueden exigir en algunos supuestos de otras normas internas complementarias para hacer plenamente efectiva su aplicación.

Entre los objetivos de la LOPDGDD está adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y completar sus disposiciones.

12.1.2. Pilares de la protección de datos

Definiciones

Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará **persona física identificable** a toda persona cuya identidad

pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Ejemplos de datos de carácter personal: nombre, apellidos de una persona, la matrícula de un coche, el número de teléfono, la dirección de correo electrónico, el número de su documento nacional de identidad (DNI), la dirección IP, etc.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Ejemplo: la mera visualización por el empleado de una oficina de Correos de los datos personales contenidos en el documento nacional de identidad de una persona es un tratamiento de datos de carácter personal.

Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

La elaboración de perfiles está formada por **tres elementos:**

(i) Debe ser una forma automatizada de tratamiento.
(ii) Debe llevarse a cabo con respecto a datos personales.
(iii) El objetivo debe ser evaluar aspectos personales sobre una persona física.

La elaboración de perfiles tiene muchas aplicaciones, entre ellas las comerciales; puede utilizarse para personalizar servicios y productos a fin de armonizarlos con las necesidades individuales. No obstante, ello puede plantear riesgos importantes para los derechos y libertades de las personas, lo que requiere de unas garantías adecuadas.

Seudonimización: es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Un dato seudonimizado sigue teniendo la consideración de dato de carácter personal, por lo que estos datos continúan estando bajo la protección de la normativa de protección de datos.

Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Este sería el caso de un archivador físico o de una base de datos electrónica que contenga contratos firmados por los clientes y ordenados mediante criterios alfabéticos, geográficos, etc.

Responsable del tratamiento (o **responsable**): la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el derecho de la Unión o el de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el derecho de la Unión o de los Estados miembros.

La Sociedad Estatal Correos y Telégrafos es responsable del tratamiento de los datos de los clientes (datos identificativos y datos de contacto del remitente y destinario del envío postal) que van a la oficina a enviar una carta certificada a un tercero.

Encargado del tratamiento (o **encargado**): la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

La empresa contratada por la Sociedad Estatal Correos y Telégrafos para la prestación de los servicios informáticos necesarios para el normal funcionamiento de los servicios de Correos sería una encargada del tratamiento, actuando dicha empresa en nombre y por cuenta de la Sociedad Estatal Correos y Telégrafos.

Corresponsable: cada uno de los responsables, dos o más, que determinan conjuntamente los objetivos y los medios de tratamiento.

Por ejemplo, en el ámbito de los sistemas comunes de información crediticia, el tratamiento de datos relativos a incumplimiento de obligaciones dinerarias, financieras o de crédito, la legislación española considera que las empresas que mantengan el sistema común de información y las acreedoras son corresponsables del tratamiento.

Tercero: es la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Destinatario: es la persona física o jurídica, autoridad, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Consentimiento del interesado: es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

El Reglamento General de Protección de Datos excluye lo que se conocía como **consentimiento tácito** o **presunto** —aquel que se presume con motivo del silencio del interesado o la inacción del titular de los datos de carácter personal—.

Ahora el consentimiento ha de darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica informada e inequívoca del interesado de aceptar el tratamiento de los datos de carácter personal que le conciernen. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Por ejemplo, el envío de un correo electrónico a varios clientes de la Sociedad Estatal Correos y Telégrafos sin incluir las direcciones electrónicas en copia oculta, o la entrega de un envío postal por error a una persona distinta del destinario constituyen, ambos, una brecha de seguridad.

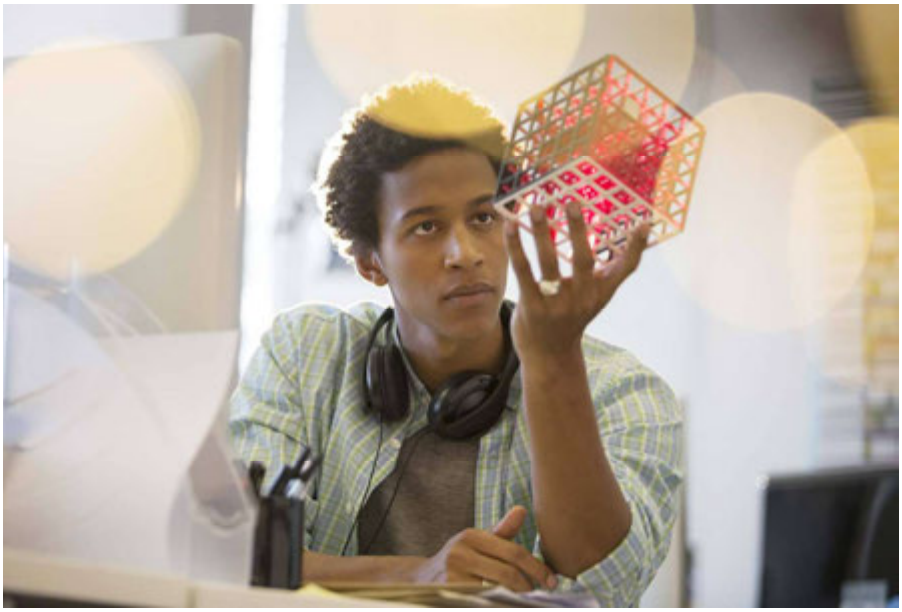
Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Autoridad de control: autoridad pública independiente encargada de supervisar la aplicación de la normativa de protección de datos con el fin de proteger los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos en la Unión.

En España, la autoridad pública de control de ámbito estatal en materia de protección de datos es la Agencia Española de Protección de Datos. Asimismo, existen autoridades autonómicas de protección de datos, que pueden ejercer las funciones y potestades recogidas en la normativa de protección de datos sobre los tratamientos de datos personales de los que sean responsables, entre otras, las entidades integrantes del sector público de las comunidades autónomas o de las entidades locales incluidas en su ámbito territorial.

Interesado: persona física titular de los datos que sean objeto de tratamiento.



Comité Europeo de Protección de Datos: órgano de la Unión Europea encargado de asesorar y garantizar la aplicación uniforme del Reglamento General de Protección de Datos. El Comité Europeo sustituye al anterior Grupo de Trabajo del artículo 29 que fue creado con la Directiva 95/46 ya derogada. No obstante, las directrices y recomendaciones emitidas por el Grupo de Trabajo del artículo 29, emitidas con anterioridad a la entrada en vigor del Reglamento General de Protección de Datos, siguen siendo válidas, teniendo un importante valor doctrinal.

Principios en protección de datos

Los principios en protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable.

El artículo 5 del RGPD establece los principios en materia de protección de datos siendo estos los siguientes:

I) Principio de licitud, lealtad y transparencia. Los datos han de ser tratados de manera lícita, leal y transparente. Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho.

Las bases legítimas del tratamiento de datos serán objeto de estudio en unidades posteriores.

El principio de lealtad está relacionado con el principio de transparencia y la finalidad. Los datos personales solo pueden utilizarse para la finalidad específica que ha sido

informada a los interesados, no pudiendo ser utilizado para otra finalidad distinta a la que ha sido informada.

Para las personas —los interesados— debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera sus datos personales, así como la medida en que dichos datos son o serán tratados.

El principio de transparencia exige que toda la información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender por los interesados y que se utilice un lenguaje sencillo y claro.

El elemento de fácil acceso se refiere a que el interesado no debe tener que buscar la información, sino que debe reconocer inmediatamente dónde y cómo acceder a esta información, por ejemplo, facilitándosela directamente al interesado, incluyendo un enlace a la información en materia de protección de datos, en una declaración o aviso de privacidad en línea estructurado en niveles, en la sección de preguntas frecuentes, mediante ventanas emergentes, etc.

Aunque se utilice un enfoque por niveles o capas de información —tal y como veremos más adelante— toda la información dirigida a los interesados debe estar a su disposición en un único lugar o documento completo único al que los usuarios puedan acceder con facilidad en caso de que deseen consultar toda la información que les incumbe.

¿En qué momento debe facilitarse la información en materia de protección de datos en cumplimiento del principio de transparencia? La información debe facilitarse en fase inicial del tratamiento, es decir, en el momento de la recogida de los datos de carácter personal de los interesados.

Por ejemplo, al rellenar un formulario en una página web o en una oficina de Correos, o al recoger los datos en un dispositivo electrónico.

Facilitar la información al interesado en materia de datos de carácter personal y hacerlo de manera oportuna es un aspecto fundamental de la obligación de transparencia y la obligación de tratamiento leal de los datos.

Cuando los datos de carácter personal sean facilitados por el interesado, la información que hay que facilitarle al interesado ha de ser en el momento en el que los datos personales se obtengan. Asimismo, el responsable del tratamiento debe observar los mismos principios cuando comunica el aviso de privacidad o política de protección de datos como cuando se produce cualquier cambio sustancial o importante que se introduzca posteriormente en esta política o aviso. Por ejemplo: habría de comunicarse un cambio en la forma en la que los interesados pueden ejercer sus derechos.

II) Principio de limitación de la finalidad. Los datos serán recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines, es decir, no pueden recogerse los datos para finalidades indeterminadas o genéricas, abstractas, implícitas o ilegítimas.

Asimismo, es importante indicar que los datos personales solo deben tratarse si la finalidad del tratamiento, es decir, el motivo por el que recogemos dichos datos, no pudiera lograse razonablemente por otros medios.

III) Principio de minimización de los datos. De acuerdo con este principio, los datos han de ser adecuados, pertinentes y limitados a lo necesario para los fines para los que son tratados, y en particular se debe garantizar que se limite a un mínimo estricto su plazo de conservación.

Los datos que se recaben han de ser los estrictamente necesarios para la finalidad para la cual van a ser tratados, no pudiendo ser recogidos datos de carácter personal, previendo que nos puedan ser útiles en un futuro o porque la aplicación a través de la cual se están recabando dichos datos tiene una configuración determinada.

Por ejemplo, si para contratar un servicio postal es necesario conocer el nombre, apellidos y dirección postal del remitente y destinatario del envío, y le preguntamos si tiene hijos, se estaría incumpliendo el principio de minimización de datos.

Por último, conviene indicar que el principio de minimización de datos está muy relacionado con la protección de datos desde el diseño y por defecto tal y como veremos más adelante.

IV) Principio de exactitud. Los datos han de ser exactos y, si fuera necesario, actualizados. Las organizaciones han de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación indebida los datos personales que sean inexactos con respecto a los fines para los que se tratan.

A estos efectos, de conformidad con el regulador español, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se suprima o rectifique sin dilación la inexactitud de los datos personales con respecto a los fines a los que se tratan siempre que, entre otros supuestos, los datos inexactos hubiesen sido obtenidos por el responsable directamente del afectado, o fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad tal y como veremos más adelante.

V) Principio de limitación del plazo de conservación. Los datos han de ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

Los datos de carácter personal no pueden conservarse de forma indefinida; el responsable del tratamiento ha de analizar el plazo para el cual es estrictamente necesario el tratamiento de los datos para el cumplimiento de las finalidades para las que fueron recabados, debiendo ser dichos datos bloqueados durante el plazo de prescripción de las acciones y posteriormente borrados o destruidos de forma definitiva de los sistemas informáticos o de los archivos en papel.

VI) Principio de integridad y confidencialidad. Los datos han de ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas, para impedir el acceso o uso no autorizado de dichos datos y del equipo utilizado para el tratamiento.

Los empleados de Correos juegan un papel fundamental en la aplicación de las medidas de seguridad técnicas y organizativas para evitar el tratamiento no autorizado o ilícito, pérdida o destrucción o daño accidental, durante el tratamiento o uso de los datos de carácter personal en el desempeño de sus funciones. Por ejemplo, custodiando las contraseñas de acceso a los sistemas de información de forma segura, no compartiendo con terceros las claves de acceso a los sistemas, no dejando a la vista de un tercero documentos en papel o una pantalla que pudieran contener datos de carácter personal.

Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase, como podrían ser empleados que tengan funciones de servicios de atención al cliente o carteros, estarán sujetos en todo momento al deber de confidencialidad.

La obligación de confidencialidad general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

Si un empleado hubiera accedido a datos personales en el ejercicio de sus funciones, únicamente habrá de tratarlos para el cumplimiento de sus funciones, prohibiéndose, en cualquier caso, su utilización para fines distintos o su comunicación, ni siquiera para su conservación a terceros.

Las obligaciones de confidencialidad anteriormente referidas se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento, es decir, se mantendrán de forma indefinida.

VII) Principio de responsabilidad proactiva. De acuerdo con este principio, el responsable del tratamiento será responsable del cumplimiento de los principios anteriormente señalados y deberá ser capaz de demostrar su cumplimiento.

El principio de responsabilidad proactiva constituye una de las mayores innovaciones del RGPD para los responsables del tratamiento y se proyecta sobre todas las obligaciones de las organizaciones.

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y

poder demostrar que el tratamiento de los datos es conforme con la normativa de protección de datos.

El responsable del tratamiento ha de poder demostrar ante los interesados y ante las autoridades de supervisión —la Agencia Española de Protección de Datos en el caso de España— que las medidas aplicadas son adecuadas al tratamiento de los datos y que se cumplen con los principios de protección de datos de carácter personal.

Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

Bases legítimas del tratamiento de datos

De conformidad con la normativa de protección de datos, tal y como hemos apuntado al hablar sobre el principio de licitud, **el tratamiento solo será lícito** si se cumple al menos una de las siguientes **condiciones:**

- el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- el tratamiento es necesario para el cumplimiento de una **misión realizada en interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Consentimiento

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de **voluntad libre, específica, informada e inequívoca** del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta

la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento.

Para poder tratar los datos, el titular debe prestar su **consentimiento,** que debe reunir unas **características** determinadas:

- **Libre.** La concesión de consentimiento no puede estar condicionada, por ejemplo, a la rebaja de un servicio.
  El consentimiento no se considerará libremente prestado cuando el interesado no goza de verdadera o libre elección, o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno. La noción de desequilibrio entre el responsable del tratamiento y el interesado también se tiene en cuenta en el RGPD. Asimismo, para que el consentimiento sea libre deberá permitirse autorizar por separado las distintas operaciones del tratamiento de datos personales.

- **Específico.** Con este requisito, el regulador quiere asegurarse de que, cuando el tratamiento tenga varias finalidades, se recabe el consentimiento para cada una de ellas. Asimismo, debe haber una clara separación entre la información relacionada con la obtención del consentimiento para las actividades del tratamiento y la información relativa a otras cuestiones.

- **Informado.** Tal y como hemos visto con anterioridad, el principio de transparencia es uno de los requisitos fundamentales, estrechamente vinculado con los principios de lealtad y licitud. Facilitar la información a los interesados antes de obtener su consentimiento es esencial para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando y, por ejemplo, ejercer su derecho a la retirada del consentimiento.
  El Comité Europeo de Protección de Datos opina que se requiere, al menos, la siguiente información para obtener un consentimiento válido:

  (i) Identidad el responsable del tratamiento.
  (ii) La finalidad para la que se quiere recabar el consentimiento.
  (iii) Qué tipo de datos van a recogerse y utilizarse.
  (iv) La existencia del derecho a retirar el consentimiento en cualquier momento.

- **Inequívoco.** El RGPD establece claramente que el consentimiento requiere una declaración del interesado o una clara acción afirmativa, lo que significa que siempre debe darse el consentimiento mediante una acción o declaración. Debe resultar evidente que el interesado dio su consentimiento a una operación concreta de tratamiento.

Asimismo, el Reglamento Europeo establece las siguientes **condiciones y requisitos para que el consentimiento sea válido:**

- Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

- Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
- No será vinculante ninguna parte de la declaración que constituya infracción del Reglamento Europeo al que nos referimos.
- El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello.
- Será tan fácil retirar el consentimiento como darlo.
- Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta, en la mayor medida posible, el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Interés legítimo

El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable.

Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable.

En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior.

El regulador considera que **puede estar amparado en el interés legítimo:**

- El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude.
- El tratamiento de datos personales con fines de mercadotecnia directa.
- Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados.

12.1.3. Derechos de los interesados en protección de datos

Derechos que pueden ejercer los interesados

A) Características

Son **derechos personalísimos:**

- Solo pueden ser ejercitados por el interesado o por su representante.
- Debe acreditarse la solicitud del interesado y, en su caso, de su representante, así como su capacidad de representación.

Plazo de respuesta:

- Deben tramitarse y darse respuesta en el plazo máximo de un mes desde la recepción de la solicitud.
- Se puede solicitar una prórroga de dos meses, siempre que sea necesario (por complejidad o número de solicitudes) y se comunique al interesado los motivos de la dilación en el plazo máximo de un mes desde su solicitud.

Ejercicio gratuito:

- Solo se puede pagar un canon razonable, en función de los costes administrativos afrontados, en caso de reiteraciones injustificadas de su solicitud.
- El responsable podrá, a su elección, negarse a actuar respecto a la solicitud.
- El responsable soportará la carga de demostrar el carácter manifiestamente excesivo o infundado de la solicitud.

Glosario

Derecho de acceso: Derecho que tiene toda persona a obtener información sobre qué datos se están tratando y las características del tratamiento de sus datos personales.

B) Los derechos que pueden ejercer los interesados son los siguientes

Derecho de acceso del interesado

El interesado tendrá derecho a obtener del responsable del tratamiento la confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y, entre otra, a la siguiente información:

- los fines del tratamiento;
- las categorías de datos personales de que se trate;
- los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales;
- de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales, la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

- el derecho a presentar una reclamación ante una autoridad de control;
- cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y
- cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia.

El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos.

El derecho a obtener la copia mencionada en el apartado anterior no afectará negativamente a los derechos y libertades de otros.

Derecho de rectificación

Posibilidad de rectificar los datos personales que sean inexactos; y, teniendo en cuenta los fines del tratamiento, el interesado podrá completar los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Glosario

Derecho de rectificación: Derecho a través del cual las personas pueden solicitar la modificación de aquella información no veraz o inexacta sobre sí mismos.

Derecho de supresión

El responsable del tratamiento estará obligado a suprimir sin dilación indebida los datos personales cuando concurra, entre otras, alguna de las circunstancias siguientes:

- los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- el interesado retira el consentimiento en el que se basa el tratamiento de sus datos;
- el interesado se opone al tratamiento de sus datos, y no prevalecen otros motivos legítimos para el tratamiento;
- cuando el interesado se opone al tratamiento para fines de mercadotecnia directa, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia;
- los datos personales han sido tratados ilícitamente;
- los datos personales deben suprimirse para el cumplimiento de una obligación legal establecida en el derecho de la Unión o de los Estados miembros.

Glosario

Derecho de supresión: Derecho a obtener, del responsable del tratamiento, sin dilaciones indebidas, la eliminación de los datos personales que le conciernan, cuando ya no resulte necesario.

No obstante lo anterior, el Reglamento General de Protección de Datos recoge los supuestos en los que el derecho de supresión no se aplicará; entre dichos supuestos podemos destacar los siguientes:

- cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información;
- cuando el tratamiento sea necesario para el cumplimiento de una obligación legal;
- cuando sea necesario por razones de interés público en el ámbito de la salud pública;
- cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a la limitación del tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- El interesado se haya opuesto al tratamiento en virtud del interés legítimo mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando el tratamiento de datos personales se haya limitado por haber sucedido algunas de las condiciones mencionadas, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación:

- con el consentimiento del interesado,
- o para la formulación, el ejercicio o la defensa de reclamaciones,
- para proteger los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

Todo interesado que haya obtenido la limitación del tratamiento habrá de ser informado por el responsable antes del levantamiento de dicha limitación.

Derecho a la portabilidad de los datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se den las siguientes condiciones:

- el tratamiento esté basado en el consentimiento o en un contrato, y
- el tratamiento se efectúe por medios automatizados.

Consideramos oportuno aclarar que, para poder ejercer este derecho, **es necesario que se cumplan ambas condiciones.**

Al ejercer el derecho a la portabilidad de los datos, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable (esto es de una empresa a otro proveedor de servicios del mismo sector empresarial u otro) cuando sea técnicamente posible.

Es importante resaltar que, al igual que sucedía con el derecho de acceso, el derecho de portabilidad no podrá afectar negativamente a los derechos y libertades de otros.

Glosario

Derecho a la limitación del tratamiento: Permite al interesado, cuyos datos personales son objeto de tratamiento, solicitar al responsable del tratamiento el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en un futuro. Para ello el responsable habrá de aplicar medidas sobre esos datos para, entre otras cosas, evitar su modificación en su caso, su borrado, o supresión.

Glosario

Derecho de portabilidad de los datos: Se refiere al derecho del individuo para recibir una copia en un formato interoperable de los datos personales que se hayan facilitado a un responsable y a transmitirlos a otro responsable sin que el anterior lo pueda impedir.

Con el derecho de portabilidad el interesado también tiene derecho a recibir datos que haya facilitado al responsable del tratamiento y que incumban al interesado en cuestión y poder almacenar dichos datos para un uso personal posterior. Dicho almacenamiento podrá realizarse en un dispositivo privado o en una nube privada sin tener que transmitir necesariamente los datos a otro responsable del tratamiento. El derecho a la portabilidad ofrece al interesado una forma sencilla de gestionar sus datos y reutilizar por sí mismo sus datos personales.

Derecho de oposición

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en interés legítimo o en interés público, incluida la elaboración de perfiles.

El responsable del tratamiento dejará de tratar los datos personales, salvo en los siguientes supuestos:

- que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o
- para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

A más tardar, en el momento de la primera comunicación con el interesado, el derecho de oposición será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

Glosario

Derecho de oposición: Aquel que permite a los interesados oponerse al tratamiento de sus datos personales.

Derecho de información de los interesados cuando sus datos se obtienen del interesado o cuando los datos no se obtienen directamente del interesado

Asimismo, las organizaciones en su calidad de responsables del tratamiento deben tomar las medidas oportunas para facilitar al interesado toda la información indicada en los artículos 13 y 14 del Reglamento General de Protección de Datos. Estos artículos se refieren a la información que deberá facilitarse cuando se recogen los datos del interesado y a la información que habrá de ser facilitada cuando los datos no se recojan directamente del interesado.

Información que deberá facilitarse cuando los datos personales se obtengan del interesado

Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- la identidad y los datos de contacto del responsable;
- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos, y
- el derecho a presentar una reclamación ante una autoridad de control.

En algunos casos, dependiendo de la característica de responsable y del tratamiento a realizar, el responsable del tratamiento deberá de facilitar además la siguiente información:

- Los datos de contacto del delegado de protección de datos, en caso de que hubiese sido designado por la organización de forma obligatoria o voluntaria.
- Los datos de representante del responsable del tratamiento, en su caso.
- Cuando el tratamiento se base en el interés legítimo, los intereses legítimos del responsable o de un tercero.
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- La intención del responsable de transferir datos personales a un tercer país u organización internacional, y la existencia o ausencia de una decisión de adecuación de la Comisión.
- Cuando el tratamiento esté basado en el consentimiento, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles.
- Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos.

Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

El responsable habrá de facilitar al interesado, además de la información anteriormente indicada, la siguiente información:

- La categoría de los datos personales.
- El origen/fuente de la que proceden los datos.

Plazo para facilitar la información cuando los datos no se han obtenido del interesado:

- dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes;
- si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

- si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

Es decir, el derecho de información al interesado debería facilitarse en el plazo máximo de un mes, salvo que, antes de que se cumpla dicho plazo, el responsable necesitara utilizar los datos para comunicarse con el interesado o comunicar los datos a otro destinatario, en cuyo caso la información deberá facilitarse en el momento en el que se realice la comunicación.

Formato de la información facilitada

El responsable del tratamiento ha de adoptar medidas activas para suministrar la información al interesado o dirigir activamente al interesado a la ubicación de esta (por ejemplo, mediante un enlace directo o código QR). El interesado no tiene que buscar la información activamente entre información de otro tipo (como por ejemplo las condiciones de uso de un sitio web).

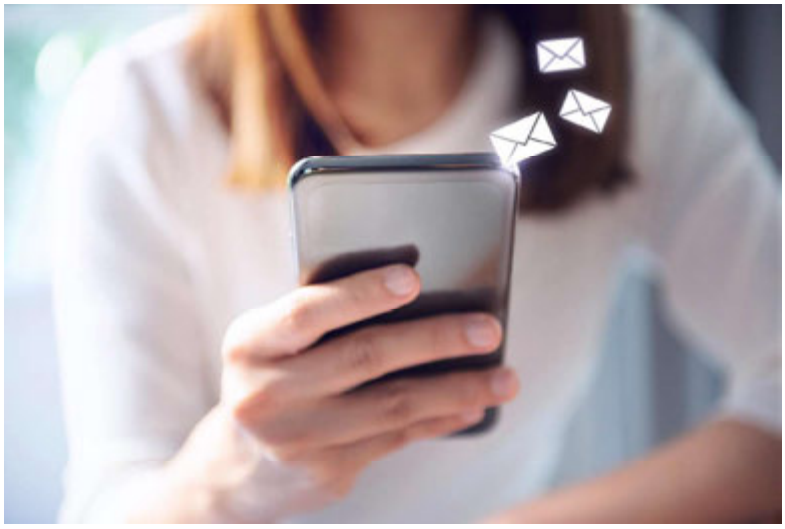
Enfoque por niveles

Con motivo de la cantidad de información que se debe facilitar al interesado, el Grupo de Trabajo del artículo 29 recomienda a los responsables del tratamiento seguir un enfoque por niveles para evitar la fatiga informativa. El diseño y la información del primer nivel será tal que el interesado obtenga una visión general y clara de la información disponible sobre el tratamiento de sus datos personales y sobre cómo puede encontrar la información detallada.

La información que ha de facilitarse en el primer nivel se refiere a los fines del tratamiento, quién es el responsable del tratamiento y una descripción de los derechos del interesado (por ejemplo, mostrándola a medida que un interesado rellena su formulario en línea), debiéndose remitir al interesado a la información adicional en un segundo nivel donde se presentarán detalladamente el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, su archivo.

En las interacciones con personas o por vía telefónica, el Grupo de Trabajo del artículo 29 recomienda que el primer nivel, es decir, la principal vía por la que el responsable interactúa por primera vez, transmita habitualmente la información más importante, esta es: cuál es la finalidad del tratamiento (para qué se van a utilizar sus datos personales), la identidad del responsable, la existencia de los derechos, junto con la información con mayor repercusión del tratamiento o el tratamiento que podría sorprender al interesado.

Por ejemplo, cuando el primer contacto con el interesado se realiza por teléfono, esta información se le podría facilitar durante la llamada con el interesado y este podría recibir el resto de información requerida por otro medio adicional distinto (por ejemplo, enviándole una copia de la política de privacidad por correo electrónico o un enlace a la declaración de privacidad en línea).



12.1.4. Obligaciones por parte de las empresas en materia de protección de datos

El delegado de protección de datos

De acuerdo con lo establecido en el Reglamento General de Protección de Datos, es obligatorio que algunos responsables y encargados del tratamiento designen a un delegado de protección de datos.

Así será en el caso de todas las autoridades y organismos públicos y de otras organizaciones cuya actividad fundamental consista en la observación sistemática a gran escala de personas o que traten categorías especiales de datos a gran escala.

Además, las organizaciones podrán designar de forma voluntaria un delegado de protección de datos.

Posición del delegado de protección de datos:

- Las organizaciones tienen que garantizar que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos.
- Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de los derechos reconocidos por la normativa de protección de datos, los cuales han sido objeto de estudio en unidades anteriores.
- Los delegados de protección de datos no son los responsables en caso de incumplimiento de la normativa. Son las organizaciones las que tienen la obligación de garantizar y demostrar que el tratamiento de los datos de carácter personal se realiza conforme a la normativa de protección de datos.

Entre las funciones del delegado de protección de datos consideramos oportuno destacar las siguientes:

- Informar y asesorar a las organizaciones y a los empleados que se ocupen del tratamiento de los datos de las obligaciones que les incumben en virtud de la normativa de protección de datos.
- Supervisar el cumplimiento de la normativa de protección de datos, incluyendo la asignación de responsabilidades, concienciación y formación del personal y las auditorías de protección de datos.
- Ofrecer asesoramiento que se le solicite acerca de las evaluaciones de impacto.
- Cooperar con la autoridad de control.

La Sociedad Estatal Correos y Telégrafos ha designado a un delegado de protección de datos.

Análisis de riesgos y evaluaciones de impacto

Análisis de riesgos

El responsable del tratamiento ha de realizar los análisis de riesgo de los tratamientos de datos de carácter personal que vaya a realizar, con el fin de que determinen y apliquen las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y deben poder demostrarlo (principio de responsabilidad proactiva).

Los riesgos a los que hace referencia el Reglamento General de Protección de Datos son los riesgos para los derechos y libertades de las personas, no se está refiriendo a los riesgos que pudieran derivar para las organizaciones. A estos efectos no hay que olvidar que el derecho a la protección de datos es un derecho fundamental, siendo el objeto de la normativa de protección de datos la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Las medidas técnicas y organizativas a las que se ha hecho referencia se establecerán teniendo en cuenta:

- el estado de la técnica,
- los costes de aplicación,
- la naturaleza, el alcance, el contexto y los fines del tratamiento, y
- los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo deberán, en su caso, incluir entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Asimismo, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Además, el responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona, que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, solo pueda tratar dichos datos siguiendo instrucciones del responsable del tratamiento.

Tal y como se ha indicado en unidades anteriores, el empleado tiene un papel fundamental en el cumplimiento de las medidas técnicas y organizativas de su organización, debiendo de adoptar las medidas que sean indicadas por esta.

Como ejemplos de medidas técnicas y organizativas que han de ser aplicadas por los empleados se enumeran las siguientes:

- El empleado deberá de tener siempre activado un salvapantallas con contraseña.
- Nunca se ha de comunicar la contraseña a nadie, ni se debe escribir en ningún sitio.
- No se deben enviar correos electrónicos con datos de carácter sensible.
- Antes de enviar un correo electrónico hay que comprobar el destinatario del mismo y si la información que se envía es la correcta.
- Los empleados no deberán dejar desatendidos los carritos que contengan cartas o paquetes de los clientes, ni los dispositivos electrónicos que utilicen en el desarrollo de sus funciones.
- Los empleados no deberán dejar información accesible a terceras personas que contenga datos de carácter personal, ni en su mesa de trabajo, ni en la impresora.
- La documentación en papel ha de ser guardada y almacenada de forma ordenada en armarios y cajones cerrados con llave.
- Los documentos con datos de carácter personal deben ser destruidos mediante las destructoras de papel que la compañía pone a disposición de los empleados.

Evaluaciones de impacto

El responsable del tratamiento habrá de realizar una evaluación de impacto en la protección de datos cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines entrañe un alto riesgo para los derechos y libertades de las personas físicas. La evaluación de impacto habrá de realizarse antes del tratamiento de datos.

La normativa establece **algunos supuestos** en los que ha de realizarse una evaluación de impacto:

- Evaluación sistemática y exhaustiva de aspectos personales de las personas, la cual se base en un tratamiento automatizado y sobre cuya base se tomen decisiones que produzcan efectos jurídicos.
- Tratamientos a gran escala de datos de categorías especiales (entre estos datos destacamos: los que revelen el origen étnico o racial, datos de salud, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, orientación o vida sexual, datos biométricos dirigidos a identificar de manera unívoca a una persona…) e infracciones penales.
- Observación sistemática a gran escala de una zona de acceso al público.

Asimismo, la autoridad de control ha publicado una lista (orientativa) de los tipos de operaciones que requieren una evaluación de impacto.

Protección de datos por diseño y por defecto

La protección de datos desde el diseño conlleva **incorporar los principios de protección de datos de carácter personal** desde las primeras etapas del diseño de un producto o servicio.

Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.

Las organizaciones en el momento en el que están diseñando un producto o servicio también deben definir las operaciones de tratamiento de los datos, los medios que serán utilizados para ello, teniendo en cuenta en su diseño el cumplimiento de los principios, los derechos y obligaciones de las organizaciones en materia de protección de datos.

En cuanto a **la privacidad** por defecto, tal y como indicamos está muy relacionada con el principio de minimización de datos de carácter personal. Los responsables deben adoptar las medidas necesarias que garanticen que solo se tratan los datos necesarios para cada uno de los fines específicos, en lo relativo a la cantidad de los datos tratados, la extensión del tratamiento de los datos, los periodos de conservación y la accesibilidad a los datos de carácter personal.

Violaciones de seguridad de los datos personales

En este apartado hay que recordar la definición de **violación de seguridad** que se recoge en el Reglamento General de Protección de Datos: «Toda violación que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos».

Cuando se produce una violación de seguridad de los datos personales (o brecha de seguridad) es muy importante determinar la dimensión de seguridad de los datos personales a los que ha afectado la brecha. Estas dimensiones son:

- La confidencialidad: cuando los datos personales han podido ser accedidos por terceros sin permiso.
  Como ejemplo, estaríamos en este supuesto en los siguientes casos: la pérdida de un dispositivo electrónico como una tableta, el envío por correo electrónico por error de un documento que contiene datos de carácter personal a una persona distinta a su destinatario, envío de un correo electrónico a múltiples destinatarios sin copia oculta o en una lista de distribución visible, el robo o la sustracción de una furgoneta con envíos, la pérdida de un envío postal.

- La disponibilidad: una brecha afecta a la disponibilidad cuando los datos han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos.
  Como ejemplo, estaríamos en este supuesto en los siguientes casos: la pérdida de un envío postal, robo o pérdida de un dispositivo electrónico (móvil o tableta, o un portátil), un ciberincidente de *ransomware* que afecta a los datos personales de los clientes.

- La integridad: una brecha afecta a la integridad cuando se han alterado los datos personales de forma ilegítima y el tratamiento de esos datos puede causar un daño a los afectados.
  Como ejemplo, estaríamos en este supuesto cuando un tercero ha modificado la base de datos de los clientes de la compañía.

Notificación a la autoridad de control

El responsable del tratamiento debe notificar a las autoridades de control, sin dilación indebida y a ser posible antes de las 72 horas después de que haya tenido constancia de la brecha de seguridad.

La notificación habrá de incluir como mínimo el siguiente contenido:

- Descripción de la naturaleza de la violación.
- Comunicación del nombre y los datos del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Categorías de los datos y número de los interesados afectados, así como las categorías y número aproximado de registro de datos personales afectados.
- Descripción de las posibles consecuencias de la violación de seguridad.
- Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de seguridad, incluyendo, si procede, las medidas adoptadas para mitigar los efectos negativos.

Los responsables del tratamiento deben documentar todas las violaciones de seguridad.

Comunicación a los interesados

Además, cuando sea probable que la violación de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable deberá comunicarlo al interesado sin dilación indebida.

Cualquier dilación en la comunicación a los afectados le resta efectividad, por lo que una comunicación a destiempo puede llegar a tener el mismo efecto que una comunicación no realizada.

En cumplimiento del **principio de transparencia,** la comunicación describirá en un lenguaje claro y sencillo, como mínimo, lo siguiente:

- La naturaleza de la violación.
- El nombre y los datos del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Describir las posibles consecuencias de la violación de seguridad.
  Los daños que se pueden causar a los afectados pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados (como consecuencia de su uso por quien ha accedido a los datos de forma no autorizada) hasta la usurpación de identidad, perjuicios económicos o exposición pública de datos confidenciales.
- Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de seguridad, incluyendo, si procede, las medidas adoptadas para mitigar los efectos negativos.

Registro de actividades

Las organizaciones han de tener un **registro de operaciones** de tratamiento en el que se contenga la información que establece el Reglamento General de Protección de Datos, entre las que **destacamos las siguientes:**

- Nombre y datos de contacto del responsable del tratamiento o corresponsable y del delegado de protección de datos.
- Fines del tratamiento.
- Descripción de las categorías de interesados y las categorías de los datos personales.

- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales.
- En su caso, las transferencias internacionales de datos.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, las descripciones de las medidas técnicas y organizativas de seguridad a las que nos hemos referido en el apartado relativo al análisis de riesgos y evaluaciones de impacto.

Además, cuando la organización actúe como encargada del tratamiento, también habrá de llevar un registro de actividades efectuadas por cuenta del responsable del tratamiento.

Estos registros de actividades estarán a disposición de la autoridad de control que lo solicite.

12.1.5. Régimen de sanciones

Las sanciones por incumplimiento de la normativa de protección de datos pueden llegar a ser muy elevadas.

La **Agencia Española de Protección de Datos (AEPD),** autoridad independiente encargada de supervisar la aplicación de la normativa de protección de datos, con el fin de proteger los derechos y libertades fundamentales de las personas físicas, en lo que respecta al tratamiento de los datos, es la autoridad que tiene la potestad de imponer una multa administrativa a los encargados y responsables del tratamiento que incumplan la normativa de protección de datos.

Glosario

AEPD: Agencia Española de Protección de Datos.

Según lo establecido en el **Reglamento General de Protección de Datos,** las **multas administrativas** pueden alcanzar los siguientes **importes:**

- **Multas administrativas de 20.000.000** de euros como máximo o, tratándose de una empresa, de una cuantía de equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero del anterior, optándose por el de mayor cuantía, en caso de infracción de, entre otras, las disposiciones siguientes:

  (i) Incumplimiento de los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento (principios que han sido objeto de estudio en el apartado 12.1.2. de este Tema).
  (ii) Infracción de los derechos de los interesados (derechos que han sido objeto de estudio en el apartado 12.1.3. de este Tema).
  (iii) Transferencias de datos personales a un destinatario en un tercer país o una organización internacional sin cumplir los requisitos recogidos en la normativa de protección de datos.

- **Multas administrativas de 10.000.000** de euros como máximo o, tratándose de una empresa, de una cuantía de equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero del anterior, optándose por el de mayor cuantía, en caso de infracción de, entre otras, las disposiciones siguientes:

  (iv) Obligaciones de responsables y encargados (algunas de las cuales han sido objeto de estudio en el apartado 12.1.4. de este libro).

12.2. Prevención de blanqueo de capitales

12.2.1. Conceptos

Prevención de blanqueo de capitales y financiación del terrorismo

Prevención de blanqueo de capitales (PBC)

El **blanqueo de capitales** o lavado de dinero es el proceso que usan los delincuentes en virtud del cual los bienes de origen delictivo se integran en el sistema económico legal con apariencia de haber sido obtenidos de forma lícita.

Siguiendo la doctrina establecida por el **Grupo de Acción Financiera (GAFI),** deben distinguirse **tres fases o etapas del blanqueo de capitales:**

Glosario

GAFI (Grupo de Acción Financiera): Institución intergubernamental creada en 1989 por el G8 con el propósito de desarrollar políticas que ayuden a combatir el blanqueo de capitales y la financiación del terrorismo.

- Colocación. Consiste en introducir el dinero en efectivo en el sistema financiero para desvincularlo del delito de origen.
- Encubrimiento. Se realizan muchas transacciones y conversiones para disipar los rastros.
- Integración. Vuelve a introducir los fondos en la economía con una procedencia aparentemente legítima.

Correos debe cumplir con la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y con el Real Decreto 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010. Correos está incluido entre los sujetos obligados por el artículo 2.1.j de la Ley 10/2010: «Los servicios postales respecto de las actividades de giro y transferencia».

Financiación del terrorismo (FT)

Según dispone la **Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales:** «se entenderá por financiación del terrorismo el suministro, el depósito, la distribución o la recogida de fondos o bienes, por cualquier medio, de forma directa o indirecta, con la intención de utilizarlos o con el conocimiento de que serán utilizados, íntegramente o en parte, para la comisión de cualquiera de los delitos de terrorismo tipificados en el Código Penal».

Así pues, la **financiación del terrorismo** es cualquier forma de acción económica, de ayuda o mediación que proporcione apoyo financiero a las actividades de elementos o grupos terroristas.

Algunas diferencias entre blanqueo de capitales y financiación del terrorismo:

	BLANQUEO DE CAPITALES	FINANCIACIÓN DEL TERRORISMO
Origen	Siempre ilícito	Lícito/Ilícito
Motivación	Ganancia	Ideológica
Conductos	Internamente, desde dentro de la organización	Internamente desde células autofinanciadas Externamente de benefactores y recaudadores de fondos
Foco de detención	Transacciones sospechosas	Relaciones sospechosas, como transferencias entre personas aparentemente no relacionadas
Importe de las transacciones	Grandes sumas, frecuentemente estructuradas para evitar su detección	Pequeñas sumas, en general por debajo de los límites de identificación establecidos
Actividad financiera	Compleja red de transacciones: empresas pantalla o fantasma y paraísos fiscales	No hay perfil financiero utilizable para los terroristas
Rastro del dinero	Circular. Generalmente vuelve a la persona que lo generó	Lineal. El dinero generado se usa para propagar el grupo y sus actividades terroristas

Cabe **destacar,** que:

- El principal coste (90%) de la financiación se destina al mantenimiento de células y comandos.
- La financiación es sumamente compleja y procede de diversas fuentes en continuo cambio.
- Al igual que con el blanqueo de capitales, la globalización facilita su actividad: estados no cooperantes, disparidad de controles, paraísos fiscales...
- Expolio de bienes culturales, peajes a otras actividades ilícitas (por ejemplo, tráfico de drogas, secuestros, donaciones, contrabando de petróleo...).

Las **medidas de control interno** constituyen el conjunto de normas, asesoramiento y capacitación interna que deben aplicar todos aquellos sujetos considerados como obligados por la ley.

- Los empleados de Correos deben obtener y registrar toda la información requerida por las políticas y procedimientos de identificación y mantenimiento de registros.
- Si surge la sospecha de que una transacción está relacionada con la financiación del terrorismo, el empleado debe hacer preguntas para conocer mejor a su cliente:
  - el origen del dinero,
  - el propósito de la transacción, y
  - la relación entre el remitente y el destinatario.

Si la transacción se ha completado o rechazado, y es dudosa, se envía un informe de actividad sospechosa con la información disponible.

Informe de autoevaluación del riesgo

Correos, **anualmente**, elabora el **informe de autoevaluación** del riesgo siguiendo las recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo emitidas por el SEPBLAC (que es la Unidad de Inteligencia Financiera española, y uno de los órganos de apoyo de la Comisión de Prevención del Blanqueo de Capitales).

El informe de autoevaluación analiza en profundidad las áreas de negocio, con el fin de identificar en qué puntos se ha detectado una mayor exposición al riesgo y a partir de este resultado poder definir las medidas de control interno recogidas en el Manual de Prevención.

Con la entrada en vigor del **Real Decreto 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril,** de prevención del blanqueo de capitales y de la financiación del terrorismo se procede a culminar el nuevo enfoque orientado al riesgo de la normativa preventiva en España; se incorporan las principales novedades de la normativa internacional surgidas a partir de la aprobación de las nuevas Recomendaciones de GAFI.

En este sentido, si bien el enfoque orientado al riesgo estaba ya incorporado en la Ley 10/2010, de 28 de abril, este Real Decreto procede al desarrollo y concreción de dicho concepto.

El **informe de autoevaluación es de carácter confidencial,** se presenta a la Comisión de Control y se encuentra a disposición de las Unidades de Control y del Servicio Ejecutivo.

Diligencia debida

Glosario

Diligencia debida: Conjunto de precauciones que la ley o el buen sentido aconsejan adoptar en el desarrollo de una actividad para evitar daños previsibles.

Las obligaciones en materia de **diligencia debida** tienen por objeto la identificación y conocimiento de aquellas personas físicas o jurídicas que pretendan establecer relaciones de negocio con los sujetos obligados. La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y su Reglamento, aprobado por Real Decreto 304/2014, de 5 de mayo prevén, en función del riesgo, distintos **niveles de aplicación de las medidas de diligencia debida (SEPBLAC):**

- **Identificación de clientes. Personas físicas y personas jurídicas**

  – **Identificación formal**
  Los empleados de Correos identificarán y comprobarán, mediante documentos fehacientes, la identidad del cliente con carácter previo a la realización de operaciones: admisión o pago de giro nacional o internacional, en cualquiera de sus modalidades y con independencia del importe de estas.

- **Documentos fehacientes**

  – **Personas físicas**
  Cuando el cliente sea persona física, deberá presentar cualquiera de los **documentos originales y en vigor** que se relacionan a continuación:

  - De **nacionalidad española:**

    › Documento Nacional de Identidad.

  - De **nacionalidad extranjera:**

    › Tarjeta de Identidad de Extranjero o Tarjeta de Residencia.
    › Pasaporte válido en el país de procedencia que incorpore fotografía de su titular.
    › En el caso de ciudadanos de la Unión Europea o del Espacio Económico Europeo y de la Confederación Suiza, el documento, carta o tarjeta oficial de identidad personal expedido por las autoridades de origen o el pasaporte (documento de identidad europeo).
    › Será asimismo documento válido para la identificación de extranjeros el documento de identidad expedido por el Ministerio de Asuntos Exteriores y de Cooperación para el personal de las representaciones diplomáticas y consulares de terceros países en España.
    › Tarjeta de Asilo Político.

Excepcionalmente, se podrán aceptar otros documentos de identidad personal expedidos por una autoridad gubernamental siempre que gocen de las adecuadas garantías de autenticidad e incorporen fotografía del titular. Para la aceptación de estos documentos es necesaria la solicitud de autorización al Área de Prevención de Blanqueo de Capitales; una vez verificados los documentos, el Área comunicará a la Oficina el resultado. Posteriormente, la Comisión de Control será informada por el Área de PBC de estas excepcionalidades.

Los documentos de identificación de los clientes deben ser fehacientes y encontrarse en vigor.

– **Personas jurídicas**
  Cuando el titular de la operación sea una persona jurídica, serán válidos los documentos públicos que acrediten su existencia y contengan su denominación social, forma jurídica, domicilio, la identidad de sus administradores, estatutos y número de identificación fiscal.
  En el caso de personas jurídicas de nacionalidad española, preferentemente, será admisible, a efectos de identificación formal, la certificación del Registro Mercantil provincial, aportada por el cliente u obtenida mediante consulta telemática.
  De esta forma, **deberá obtenerse la siguiente documentación:**

  - La persona física que realiza la operación deberá identificarse, como los clientes que actúan por cuenta propia, presentado su documento de identidad válido y en vigor y además presentará:

    › **Poder o autorización** para actuar en nombre de la persona jurídica.
    › **Documentos identificativos de las personas físicas** que actúen en nombre de la persona jurídica.

  - De la persona jurídica, deberá presentar una de las dos opciones descritas a continuación:

    › **Certificación del Registro Mercantil provincial**, preferentemente, en caso de ser una persona jurídica española, aportada por el cliente u obtenida mediante consulta telemática (no es válida la nota simple).
    El motivo por el cual es más conveniente recabar el certificado del Registro Mercantil actualizado es el siguiente:
    La escritura de constitución de una empresa es un documento jurídico mediante el cual el socio o los socios (dependiendo de si la empresa depende de una persona o de más de una persona) hacen constar legalmente su voluntad de constituir una sociedad para desarrollar una actividad económica determinada, el tipo de sociedad que quieren formar, los estatutos sociales de la empresa y la relación de los socios de la empresa entre ellos así como con la empresa, y como tal refleja la situación básica inicial de la misma. Este documento, por tanto, no recogerá cambios posteriores tales como modificaciones en el objeto o denominación social, compraventa de participaciones, fusiones, cambios en los administradores o socios o en la titularidad real.

Sin embargo, el certificado del Registro Mercantil actualizado permite conocer la situación de una determinada sociedad y qué información consta de ella en el Registro Mercantil, y permite dar cuenta de que la sociedad está vigente, de qué personas ostentan los cargos sociales (administrador, apoderado, consejeros, director, secretario, etc.), es decir, constituye la «fotografía» actual de la sociedad.

- O bien la **escritura de constitución, estatutos** (si no estuvieran incorporados en la escritura de constitución) **y tarjeta CIF/NIF**. Hay que tener en cuenta que el documento aportado debe acreditar fehacientemente su denominación, forma jurídica, domicilio, identidad de los administradores, estatutos, número de identificación fiscal y titulares reales.
- Cumplimentar la **DAE (Declaración de Actividad Económica)** de persona jurídica, en la cual, de forma obligatoria, es necesario consignar en los apartados correspondientes tanto la estructura de control como los titulares reales.

En el caso de que se obtengan las escrituras de constitución, se deberían obtener según el tipo de persona jurídica de que se trate:

- **Sociedades mercantiles (SL y SA):** escritura de constitución.
- **Comunidades de bienes (CB) y sociedades civiles (SC):** escritura pública o contrato privado de constitución en el que figure la identificación de todos los socios o comuneros, su cuota de participación y el objeto de la comunidad, firmado por todos los comuneros. Si en la constitución se aportaron bienes inmuebles o derechos reales, habrán de aportar la escritura de constitución.
- **Sociedades Cooperativas (S. Coop.):** escritura pública inscrita en el Registro de Sociedades Cooperativas.
- **Fundaciones:** escritura pública de constitución inscrita en el Registro de Fundaciones.
- **Asociaciones:** acta fundacional, en documento privado o escritura pública, inscrita en el Registro de Asociaciones.

En el caso de entidades sin personalidad jurídica se identificará y comprobará mediante documentos fehacientes la identidad de todos los partícipes. No obstante, en el supuesto de entidades sin personalidad jurídica que no ejerzan actividades económicas bastará, con carácter general, con la identificación y comprobación mediante documentos fehacientes de la identidad de la persona que actúe por cuenta de la entidad. En los casos de representación legal o voluntaria, la identidad del representante y de la persona o entidad representada será comprobada documentalmente. A estos efectos, deberá escanearse el documento fehaciente a que se refiere el apartado precedente correspondiente tanto al representante como a la persona o entidad representada, así como el documento público acreditativo de los poderes conferidos.
Es imprescindible la cumplimentación y firma de la DAE, la cual debe incluir de forma inexcusable los datos correspondientes a aquellas personas que ostentan la titularidad real, firmada por el representante de la persona jurídica o por aquella persona con poder bastante y suficiente, manifestando que los datos consignados en la documen-

tación aportada son verídicos y se encuentran en vigor y firmada por el empleado, así como visada por el responsable de la oficina.

- **Documentos no válidos**
  No serán documentos válidos de identificación:

  a) Permiso de conducir.
  b) Pasaporte español: el RD 304/2014 de 5 de mayo, solo reconoce como documento identificativo para las personas de nacionalidad española el DNI.
  c) Cédulas de identificación (documentos de identidad) de países no pertenecientes a la Unión Europea o al Espacio Económico Europeo (EEE).
  d) Certificado de registro de ciudadanos de la Unión (carta verde): este no es un documento válido para la acreditación de la identidad ni de la nacionalidad del portador, por lo que deberá presentar un documento identificativo válido y en vigor. Además, consta expresamente en el propio certificado que no es válido a efectos de identificación.
  e) *Seaman's book* o Libreta Marítima: es un documento no oficial, que da constancia simplemente del embarque de personas bajo el pabellón de un buque proveniente de un país extranjero, por lo cual no es un documento de identificación válido, si bien es admisible para acreditar la estancia en nuestro país. Excepcionalmente son válidos los documentos emitidos por la Marina Mercante de los países descritos en el Anexo 6, bajo la Convención «Seafarers Identity Documents» de la ONU, pueden admitirse dentro de los documentos excepcionales expedidos por una autoridad gubernamental.

  f) Carnet consular: el carnet consular es un documento que acredita la inscripción de una determinada persona en el consulado del país en el que temporalmente vaya a permanecer o residir. No es un documento de identificación válido en caso de que haya sido expedido en un tercer país.
  El RD 304/2014 admite como válidos los carnets consulares expedidos por el Ministerio de Asuntos Exteriores para diplomáticos residentes en España.

- **Identificación del titular real**
  Se identificará a los titulares reales y se adoptarán medidas adecuadas a fin de comprobar su identidad con carácter previo al establecimiento de relaciones de negocio o a la ejecución de cualesquiera operaciones.
  Se entiende por titular real (art. 4 Ley 10/2010):

  a. «La persona o personas físicas por cuya cuenta se pretenda establecer una relación de negocios o intervenir en cualesquiera operaciones».

  b. «La persona o personas físicas que en último término posean o controlen, directa o indirectamente, un porcentaje superior al 25 por ciento del capital o de los derechos de voto de una persona jurídica, o que por otros medios ejerzan el control, directo o indirecto, de una persona jurídica. A efectos de la determinación del control serán de aplicación, entre otros, los criterios establecidos en el artículo 42 del Código de Comercio».

b. bis) «Cuando no exista una persona física que posea o controle, directa o indirectamente, un porcentaje superior al 25 por ciento del capital o de los derechos de voto de la persona jurídica, o que por otros medios ejerza el control, directo o indirecto, de la persona jurídica, se considerará que ejerce dicho control el administrador o administradores. Cuando el administrador designado fuera una persona jurídica, se entenderá que el control es ejercido por la persona física nombrada por el administrador persona jurídica. Los sujetos obligados verificarán su identidad y consignarán las medidas tomadas y las dificultades encontradas durante el proceso de verificación».

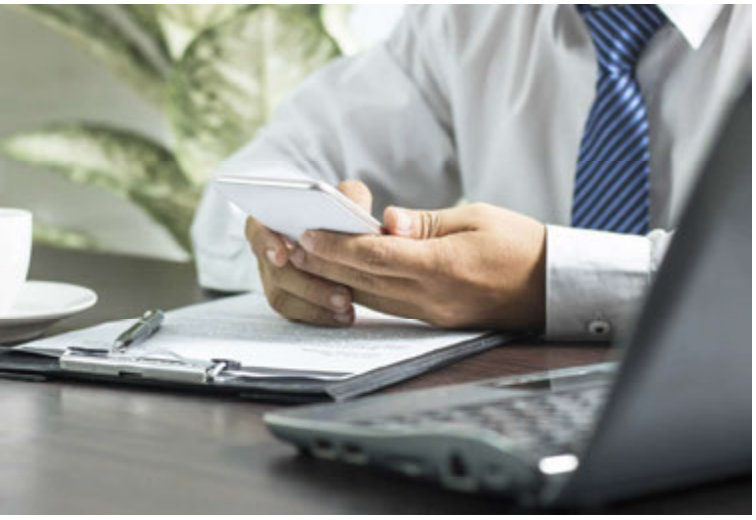
La identificación del titular real deberá abarcar los datos de identidad, su número de documento, nacionalidad, país de residencia y fecha de nacimiento, así como la naturaleza del interés o participación que determinen su consideración como titular real.
Finalmente, en aquellos casos en los que el cliente, el titular real o la operación presenten riesgos superiores al promedio, se deberá obtener documentación adicional o información de fuentes fiables e independientes cuando existan indicios de que la identidad de la titular real declarada por el cliente no es exacta o veraz, o bien cuando concurran circunstancias que determinen el examen especial de operaciones.

A) Medidas simplificadas

«Los sujetos obligados podrán aplicar, en los supuestos y con las condiciones que se determinen reglamentariamente, medidas simplificadas de diligencia debida respecto de aquellos clientes, productos u operaciones que comporten un riesgo reducido de blanqueo de capitales o de financiación del terrorismo» (artículo 9 de la Ley 10/2010).

Se aplicarán **medidas simplificadas** a:

- Las administraciones o empresas públicas, previamente clasificadas mediante su CIF por Correos, así como de sus organismos dependientes cuando estos sean los ordenantes o receptores de los giros.



- Las entidades de derecho público de los Estados miembros de la Unión Europea o de países terceros equivalentes.
- Las sociedades u otras personas jurídicas controladas o participadas mayoritariamente por entidades de derecho público de los Estados miembros de la Unión Europea o de países terceros equivalentes.
- Las entidades financieras, exceptuadas las entidades de pago, domiciliadas en la Unión Europea o en países terceros equivalentes que sean objeto de supervisión para garantizar el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo.

- Las sucursales o filiales de entidades financieras, exceptuadas las entidades de pago, domiciliadas en la Unión Europea o en países terceros equivalentes, cuando estén sometidas por la matriz a procedimientos de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Las sociedades cotizadas cuyos valores se admitan a negociación en un mercado regulado de la Unión Europea o de países terceros equivalentes, así como sus sucursales y filiales participadas mayoritariamente.
- Los giros para pago del propio Servicio Postal con origen y destino en el propio servicio de Correos.
- No se aplicarán medidas o se cesará la aplicación de las simplificadas cuando concurran o surjan indicios o certeza de blanqueo de capitales o de financiación del terrorismo o riesgos superiores al promedio.

B) Medidas normales

Por ser considerada la operativa de «envío de dinero» de riesgo alto, a todos los clientes se les aplican, como mínimo, medidas normales. **Además** de la identificación formal del cliente y la comprobación de su identidad, las medidas normales **consisten en:**

1. **Conocimiento de la actividad** profesional o empresarial del cliente.
   «En particular, los sujetos obligados recabarán de sus clientes información a fin de conocer la naturaleza de su actividad profesional o empresarial y adoptarán medidas dirigidas a comprobar razonablemente la veracidad de dicha información» (artículo 5 de la Ley 10/2010).
   La información sobre la actividad profesional o empresarial del cliente y el fin que justifica la operación son recogidos en la aplicación informática. Tras reseñar el empleado el tipo y número de documento del cliente, el sistema realiza la llamada a la base de datos de PBC para consultar o para que sea cumplimentado el formulario de aceptación de clientes, siendo la actividad económica uno de los datos obligatorios a cumplimentar en la ficha de cliente. La actividad recogida deberá ser modificada en caso de que el cliente manifieste su variación.

2. **Conocimiento del propósito y la índole** que motiva la operación.
   En aplicación de medidas de diligencia debida en la admisión/pago de giros es necesario solicitar al cliente el «motivo del envío». Este campo es obligatorio, siendo necesario informar de forma sucinta los motivos del envío. Con el fin de facilitar la información declarada por el cliente, se ha estandarizado la respuesta debiéndose marcar la más acorde. Debe existir relación entre la actividad profesional o empresarial informada y el motivo declarado.

3. **Seguimiento continuo** de la relación de negocio.
   Se realizan periódicamente procesos de revisión con objeto de asegurar que los documentos, datos e informaciones obtenidos como consecuencia de la aplicación de las medidas de debida diligencia se mantengan actualizados y se encuentren vigentes. La

actualización será, en todo caso, preceptiva cuando se verifique un cambio relevante en la actividad del cliente que pudiera influir en su perfil de riesgo.

Correos realiza el seguimiento continuo a la relación de negocios, incluido el escrutinio de las operaciones efectuadas a lo largo de dicha relación, a fin de garantizar que las operaciones coincidan con el conocimiento que se tenga del cliente y de su perfil empresarial y de riesgo. También efectúa el análisis del origen de los fondos para, de este modo, garantizar que los documentos, datos e información de que se disponga están actualizados. Este seguimiento se realiza automáticamente mediante la aplicación informática ARED, la cual cuenta con patrones de comportamiento asignados al estudio de perfil de los clientes.

Se aplicarán **medidas normales a:**

- Los clientes de **giro nacional e internacional,** que actúen en su propio nombre, remitentes o destinatarios en oficina que no superen los 3.000€, individuales o acumulados, en un trimestre.
- Los clientes de **giro internacional** que envíen o reciban fondos con países designados por el ordenamiento jurídico y realicen operaciones que, acumuladas con las del último mes natural, no superen los 1.500€ (enviados o recibidos).

C) Medidas reforzadas

Además de las medidas normales de diligencia debida, los sujetos obligados deben aplicar medidas reforzadas en los supuestos previstos en la Sección 3.ª del Capítulo II de la Ley 10/2010, de 28 de abril, y en aquellos otros determinados en su Reglamento.

Se aplicarán **medidas reforzadas** en aquellas situaciones que, por su naturaleza, presenten un **riesgo más elevado de blanqueo de capitales y de la financiación del terrorismo** y, concretamente, se aplicarán a los clientes que cumplan con los requisitos recogidos a continuación.

Adicionalmente, **la Comisión podrá valorar la aplicación de medidas reforzadas** en los casos específicos de otros clientes que, aunque no cumplan con los requisitos exigidos, sean objeto de análisis y seguimiento. En este sentido, se aplicarán medidas reforzadas cuando las operaciones del cliente no se correspondan con su actividad declarada o con sus antecedentes operativos y en caso de que proceda el examen especial de operaciones o la comunicación por indicio al SEPBLAC.

Asimismo, se aplicarán **medidas reforzadas de diligencia** debida a las operaciones realizadas por personas con responsabilidad pública.

Las operaciones en las que intervengan clientes sujetos a medidas reforzadas NO se realizarán hasta que el cliente acredite su actividad económica y el origen lícito de sus fondos, mediante la presentación de documentos fehacientes.

De forma complementaria a esta documentación, se admitirá la aportación de documentos que justifiquen los vínculos familiares entre los intervinientes, así como el propósito y la índole de la operación en determinadas operaciones.

Se analizará, por el Área de Prevención, la documentación de las operaciones que han requerido medidas reforzadas y, en los supuestos de mayor riesgo, se realizarán controles específicos. El Área de PBC recibe *online* mediante correo electrónico información sobre operaciones con medidas reforzadas de clientes. Se revisará la documentación justificativa aportada por el cliente y, en caso de ser incompleta, se marca al cliente como riesgo alto o pendiente de documentación.

Con el fin de evitar solicitar constantemente la documentación a determinados clientes habituales, que tenemos la certeza de tener conocimiento de su actividad y además está archivada la documentación necesaria de aplicación en medidas reforzadas, la periodicidad de revisión documental será acorde al modelo o tipo de documentación aportada siendo el plazo máximo de validez de un año, en caso de que, tras efectuar el seguimiento continuo de sus operaciones, se compruebe que estas son coherentes con la documentación presentada.

Por el contrario, si las sucesivas operaciones realizadas por estos clientes habituales no son coherentes con la documentación de conocimiento aportada, tanto por su importe y número de giros, como por cualquier otra característica de la operativa, se procederá a recabar nueva documentación adicional que justifique el origen de los fondos, aunque haya transcurrido un periodo de tiempo inferior a un año.

Todos los clientes a los que se apliquen estas medidas, además de las medidas normales, deberán presentar:

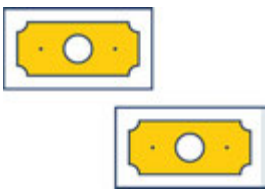
Justificación documental

La política de prevención de blanqueo de capitales se ha concebido para limitar el riesgo en Correos. Por lo tanto, con el fin de evitar riesgos, es necesario que en aplicación de medidas reforzadas de diligencia debida se deban documentar las transacciones, así como identificar y evitar las que pudieran estar asociadas al blanqueo de capitales u otras actividades ilegales.

Es importante distinguir la justificación documental a presentar, que será diferente para operaciones de envíos y operaciones de pagos.

Los clientes deberán presentar obligatoriamente:

- Para **operaciones de envíos** (justificar el origen lícito de los fondos):
  - Documentación que justifique el origen lícito de los fondos con los que se va a llevar a cabo la operación, o
  - documentación acreditativa de su actividad económica.



- Para **operaciones de pagos** (propósito e índole de la operación):
  - Justificar el vínculo familiar existente entre los intervinientes y avalar el propósito e índole de la operación.
  - Opcionalmente, documentación que acredite el origen de los fondos del remitente del giro.

De modo exclusivamente orientativo, se exponen los siguientes **documentos admitidos:**

- **En envíos.** Para acreditar la actividad económica y el origen de los fondos de los clientes, según su tipología:

  1. Personas jurídicas residentes:
     - IVA anual (Modelo 390) o trimestral (Modelo 303) o mensual (Modelo 322).
     - Impuesto sobre Sociedades (Modelo 200).
     - Pagos fraccionados del último trimestre (Modelo 202).
  2. Personas jurídicas no residentes (en su caso, con la debida traducción jurada al castellano):
     - Balance económico del ejercicio anterior.
     - Presupuestos del año actual.
     - Memoria de actividades.
     - Cualquier otro documento que acredite fehacientemente la actividad (documentos equivalentes a los relacionados para las residentes en España).
  3. Personas físicas profesionales liberales o autónomos:
     - Declaración del IVA mensual, trimestral o anual reciente.
     - Pagos fraccionados recientes.
     - Última declaración del IRPF.
  4. Personas físicas asalariadas, pensionistas o personas sin ingresos:
     - Nómina o pensión.
     - Última declaración del IRPF.
     - Otro documento que acredite fehacientemente el origen de sus ingresos.
  5. Asociaciones, fundaciones, colegios profesionales:
     - Cuentas del ejercicio anterior.
     - IVA anual o trimestral.
     - Impuesto sobre Sociedades.
     - Presentación de cuentas en el Registro.

- **En pagos.** Para avalar el propósito y la índole de la operación:
  - Factura normal o proforma.
  - Contrato de alquiler, pago de recibos.

- Presupuesto.
- Contrato de servicios.
- Libro de familia (vínculo familiar).
- Si no se puede justificar con lo anterior, es necesaria la justificación del origen lícito de los fondos por parte del remitente.

En caso de que la procedencia de los fondos con los que se pretende llevar a cabo la operación no esté directamente vinculada con la actividad económica del cliente, se deberá aportar justificación documental del origen lícito de dichos fondos (por ejemplo, escrituras de una compraventa, herencias, premios de lotería, facturas, etc.).

La operación no podrá ser realizada hasta que la documentación presentada por el cliente haya sido analizada por el Director, que valorará si justifica adecuadamente la operación, teniendo en cuenta su importe y su destino declarado y decidirá si el giro puede ser ejecutado o debe ser anulado definitivamente.

De esta forma, se garantizará que la documentación aportada sea coherente con las características de la operación que se pretende ejecutar y justifique su importe.

Por ejemplo, el importe de los giros enviados no debe ser superior al 75% del importe de la nómina presentada por el cliente. Asimismo, si de forma complementaria el cliente presenta un extracto de su cuenta bancaria, el saldo medio de los últimos tres meses debe ser superior al importe enviado en dicho periodo, y los movimientos de la misma deben acreditar el ahorro efectuado.

En caso de que la documentación presentada sea insuficiente, no se permitirá la ejecución de la operación hasta que se presente documentación adicional que justifique el origen lícito de los fondos y esta sea aprobada.

Las acciones adicionales de comprobación de la actividad y el origen de los fondos de los clientes pueden completarse mediante la obtención de información de fuentes externas fiables independientes.

A tenor de la información y documentación recabada, el Área de Prevención también podrá limitar la naturaleza o cuantía de las operaciones de estos clientes de mayor riesgo.

Declaración de Actividad Económica (DAE)

La Declaración de Actividad Económica (DAE) es el **documento** que debe ser cumplimentado y firmado por el cliente donde se recogen sus manifestaciones relativas a su actividad económica.

Debemos tener en cuenta que **según el tipo de persona:**

- **DAE de personas físicas,** en el caso de que sea necesaria, la DAE se cumplimentará automáticamente con la información facilitada por el cliente.
  En operaciones, los supuestos de riesgo elevado o clientes que realicen operaciones que se consideren fuera de lo normal, inusuales o que presenten indicios de sospecha

en relación con la prevención de blanqueo de capitales, el empleado podrá solicitar al cliente la cumplimentación de la DAE que se obtendrá de Conecta. En este caso, una vez cumplimentada la DAE por el cliente, el empleado comprobará que es legible, con datos que ofrezcan información y no adoptar fórmulas genéricas. Se deberá solicitar aclaración o ampliación de aquellos apartados que no estén cumplimentados o cuya descripción sea genérica, susceptible de duda o que no ofrezcan información concreta.
La negativa del cliente a cumplimentar la DAE cuando sea requerido a hacerlo conlleva la NO ACEPTACIÓN de la operación. Tampoco se aceptará la operación cuando el cliente rehúse proporcionar cualquier otra información que le sea requerida en relación con la normativa de prevención de blanqueo de capitales o cuando el cliente facilite datos falsos. En cualquiera de estos casos se comunicará al Área de Prevención de Blanqueo de Capitales como operación sospechosa.

- **DAE de personas jurídicas:** el cliente entregará cumplimentada la DAE en la oficina; el documento recogerá cuanta información considere oportuna para un conocimiento más amplio de las actividades a las que se dedica la empresa o entidad, así como la información relativa a su titular real y estructura de propiedad o de control. La información de la estructura de propiedad o de control de la entidad, aportada a la DAE, deberá contener el país de residencia y el porcentaje de participación.

En el caso de giro internacional, al que se le aplican medidas reforzadas, si en el documento de identificación presentado por el cliente no figura domicilio o el que figura es en el extranjero, este deberá aportar cualquier documento que acredite su estancia, permanente o temporal, en España. El documento presentado deberá ser original y recogerá el nombre completo del cliente y una dirección.

A título descriptivo, son **documentos acreditativos** válidos para justificar la estancia:

- Certificado de empadronamiento,
- contrato de alquiler de vivienda,
- escrituras de vivienda,
- *seaman's book* o libreta marítima, etc.

No se aceptará Lista de Correos como domicilio.

La DAE debe recoger la firma del declarante y del empleado.

- Se aplicarán **medidas reforzadas a:**

  – Los clientes de giro internacional de países, territorios o jurisdicciones de riesgo o que envíen o reciban fondos de o hacia los mismos, cuyo importe acumulado de sus operaciones en el mes natural sea superior a 1.500 €.
  Se incluirá entre estos países, territorios y jurisdicciones a los designados como tales por el ordenamiento jurídico y aquellos para los que el Grupo de Acción Financiera (GAFI) exija la aplicación de medidas de diligencia reforzada, todo ello de acuerdo con lo dispuesto en el artículo 22 del Real Decreto 304/2014 de 5 de mayo.

– Los clientes de giro nacional o internacional remitentes o destinatarios que superen 3.000€, individuales o acumulados en un periodo de 90 días.
– Los clientes relacionados con peticiones de Juzgados o Policía.
– Los clientes que realicen operaciones que se consideren fuera de lo normal, inusuales o que presenten indicios de sospecha en relación con la prevención de blanqueo de capitales.
– Las operaciones con origen o destino a países que supongan un riesgo superior al normal y que, una vez informada la Comisión de Control, tome razón de esta decisión.

– Los menores de edad.
  Es preciso tener en cuenta que, según los estándares nacionales e internacionales, los menores presentan un riesgo más elevado en materia de prevención de blanqueo de capitales. En este sentido, se recomienda la aplicación de medidas reforzadas a este tipo de clientes, cuya aplicación habrá de graduarse en función del riesgo que representen.

  - La minoría de edad constituye un estado civil diferente de la mayoría y de la emancipación. El menor se encuentra sometido a la patria potestad o a la tutela. Los menores de edad, aunque tienen capacidad jurídica, no tienen capacidad de obrar, por lo que no pueden contratar por sí mismos, sino debidamente representados, normalmente por sus padres o, en su defecto, por su representante legal.
  - Para la admisión y pago de giros a menores, estos deberán actuar necesariamente representados por sus padres, tutores o representantes legales.
  - Al ser necesaria la presentación del DNI con carácter previo a la realización de la operación, únicamente pueden admitirse y pagarse giros a los mayores de catorce años, que habrán de actuar siempre representados por sus padres, tutores o representantes legales.
  - Por tanto, en los sistemas de envío/pago de dinero, el menor que realiza la operación, acompañado de uno de los padres, el tutor o el representante legal, deberá identificarse, presentado su documento de identidad válido y en vigor, y, además, se verificará la identidad del representante que será comprobada documentalmente. A estos efectos, deberán escanearse los documentos identificativos de ambos y el documento que acredite la relación de parentesco o la representación legal del menor.
  - En caso de menores emancipados, deberán presentar la escritura de emancipación no siendo necesaria la figura del tutor legal.

Personas de responsabilidad pública (PRP):

Se considerarán personas con responsabilidad pública las siguientes:

- Se considerarán personas con responsabilidad pública aquellas que desempeñen o hayan desempeñado funciones públicas importantes, tales como los jefes de Estado, jefes de Gobierno, ministros u otros miembros de Gobierno, secretarios de Estado o subsecretarios; los parlamentarios; los magistrados de tribunales supremos, tribunales constituciona-

les u otras altas instancias judiciales cuyas decisiones no admitan normalmente recurso, salvo en circunstancias excepcionales, con inclusión de los miembros equivalentes del Ministerio Fiscal; los miembros de tribunales de cuentas o de consejos de bancos centrales; los embajadores y encargados de negocios; el alto personal militar de las Fuerzas Armadas; los miembros de los órganos de administración, de gestión o de supervisión de empresas de titularidad pública; los directores, directores adjuntos y miembros del consejo de administración, o función equivalente, de una organización internacional; y los cargos de alta dirección de partidos políticos con representación parlamentaria.

- Asimismo, tendrán la consideración de personas con responsabilidad pública:

  a) Las personas, distintas de las enumeradas en el apartado anterior, que tengan la consideración de alto cargo de conformidad con lo previsto en el artículo 1 de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio de altos cargos de la Administración General del Estado.
  b) Las personas que desempeñen o hayan desempeñado funciones públicas importantes en el ámbito autonómico español, como los presidentes y los consejeros y demás miembros de los Consejos de Gobierno, así como las personas que desempeñen cargos equivalentes a las relacionadas en la letra a) y los diputados autonómicos y los cargos de alta dirección de partidos políticos con representación autonómica.
  c) En el ámbito local español, los alcaldes, concejales y las personas que desempeñen cargos equivalentes a las relacionadas en la letra a) de los municipios capitales de provincia, o de Comunidad Autónoma y de las Entidades Locales de más de 50.000 habitantes, así como los cargos de alta dirección de partidos políticos con representación en dichas circunscripciones.
  d) Los cargos de alta dirección en organizaciones sindicales o empresariales españolas.
  e) Las personas que desempeñen funciones públicas importantes en las organizaciones internacionales acreditadas en España. Estas organizaciones deberán elaborar y mantener actualizada una lista de esas funciones públicas de conformidad con lo señalado en el primer apartado.

  La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias elaborará y publicará una lista en la que se detallará qué tipo de funciones y puestos determinan la consideración de persona con responsabilidad pública española.

- Ninguna de las categorías previstas en los apartados anteriores incluirá empleados públicos de niveles intermedios o inferiores.

- Se aplicarán estas medidas a los familiares y allegados de las personas con responsabilidad pública.
  A estos efectos, tendrá la consideración de familiar el cónyuge o la persona ligada de forma estable por análoga relación de afectividad, así como los padres e hijos, y los cónyuges o personas ligadas a los hijos de forma estable por análoga relación de afectividad. Se considerará allegado toda persona física de la que sea notorio que ostente la

titularidad o el control de un instrumento o persona jurídicos juntamente con una persona con responsabilidad pública, o que mantenga otro tipo de relaciones empresariales estrechas con la misma, o que ostente la titularidad o el control de un instrumento o persona jurídicos que notoriamente se haya constituido en beneficio de la misma.

Aunque la persona contemplada en los apartados anteriores haya dejado de desempeñar sus funciones, se continuarán aplicando las medidas reforzadas por un periodo de dos años. Transcurrido ese plazo, se aplicarán medidas de diligencia debida adecuadas en función del riesgo que siga presentado el cliente y mientras se determine que ya no representa un riesgo específico derivado de su antigua condición de persona con responsabilidad pública.

Se aplicarán medidas reforzadas de diligencia a estas personas con el fin de determinar el origen del patrimonio y de los fondos con los que se pretende llevar a cabo la operación.

La admisión de las personas con responsabilidad pública como clientes deberá ser autorizada directamente por el responsable de Oficina/Unidad de Reparto, que trasladará su decisión al Área de Prevención.

Finalmente, las operaciones y relaciones de negocio establecidas con las personas con responsabilidad pública serán objeto de un seguimiento reforzado y permanente.

El Área de Prevención informará en las reuniones de la Comisión de Control de las comunicaciones afirmativas de oficinas para que tome razón de esta decisión.

Durante el periodo en el que el cliente tenga la consideración de PRP, deberá justificar documentalmente su actividad económica y el origen de los fondos, respetando el plazo de validez de la documentación aportada, sin tener en cuenta el importe de la operación realizada.

12.2.2. Marco legal de la PBC

Disposiciones legales nacionales

En materia de PBC/FT se establecen en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y en el Real Decreto 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010.

- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo (BOE 29/04/10).
- Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Real Decreto-Ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención del blanqueo de capitales, entidades

de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

- Real Decreto-ley 11/2018, de 31 de agosto, de transposición de directivas de la Unión Europea en materia de protección de los compromisos por pensiones con los trabajadores, prevención del blanqueo de capitales y requisitos de entrada y residencia de nacionales de países terceros.
- Ley 12/2003, de 21 de mayo de bloqueo de la financiación del terrorismo.
- Orden EHA/2619/2006, de 28 de julio, por la que se desarrollan determinadas obligaciones de prevención del blanqueo de capitales de los sujetos obligados que realicen actividad de cambio de moneda o gestión de transferencias con el exterior.
- Real Decreto 1080/1991, de 5 de julio, por el que se determinan los países o territorios a que se refieren los artículos 2.º, apartado 3, número 4, de la Ley 17/1991 de 27 de mayo de Medidas Fiscales Urgentes, y 62 de la Ley 31/1990, de 27 de diciembre, de Presupuestos Generales del Estado para 1991.
- Orden EHA/2444/2007, de 31 de julio, por la que se desarrolla el Reglamento de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, aprobado por Real Decreto 925/1995, de 9 de junio, en relación con el informe de experto externo sobre los procedimientos y órganos de control interno y comunicación establecidos para prevenir el blanqueo de capitales.
- Orden EHA 1439/2006, de 3 de mayo reguladora de la declaración de movimientos de medios de pago en el ámbito de la prevención del blanqueo de capitales.
- Orden ECO/2652/2002, de 24 de octubre, por la que se desarrollan las obligaciones de comunicación de operaciones en relación con determinados países al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.
- Resolución de 10 de agosto de 2012, de la Secretaría General del Tesoro y Política Financiera, por la que se publica el Acuerdo de 17 de julio de 2012, de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, por el que se determinan las jurisdicciones que establecen requisitos equivalentes a los de la legislación española de prevención del blanqueo de capitales y de la financiación del terrorismo.

Disposiciones legales internacionales

Las disposiciones que se han utilizado como referencia para la elaboración de las leyes en la mayor parte de los países se recogen en el listado siguiente:

- Las cuarenta recomendaciones del GAFI (febrero 2012).
- Nueve recomendaciones especiales contra la financiación del terrorismo del GAFI (octubre 2004).

- Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo de 20/05/2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo.
- Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30/05/2018.
- Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15/03/2017.
- Reglamento Delegado (UE) 2019/758 de la Comisión, de 31/01/2019.
- Reglamento Delegado (UE) 2018/1108 de la Comisión, de 7/05/2018.
- Reglamento Delegado (UE) 2018/212 de la Comisión, de 13/12/2017.
- Reglamento Delegado (UE) 2018/105 de la Comisión, de 27/10/2017.
- Reglamento Delegado (UE) 2016/1675 de la Comisión, de 14/07/2016.
- Reglamento (UE) 2015/847 del Parlamento Europeo y del Consejo de 20/05/2015.

12.2.3. La estructura de la prevención en Correos

A) Normativa interna

Correos debe cumplir con:

- La Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y con el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010. Al estar incluida entre los sujetos obligados por el artículo 2.1.j) de la Ley 10/2010: «Los servicios postales respecto de las actividades de giro y transferencia».

- El artículo 2.c) de los estatutos sociales de Correos dispone que, entre otros, el objeto de la sociedad es «La prestación de los servicios financieros relacionados con los servicios postales, los servicios de giro y de transferencias monetarias».

La Entidad lleva a cabo la actividad de gestión de envío y pago de dinero mediante la prestación de los servicios de Giro Nacional y Giro Internacional y actúa como agente de Western Union Payment Services Ireland Limited para ordenar y pagar transferencias de dinero urgente en más de ciento noventa países, bajo la marca Western Union.

La **normativa interna** que se aplica en Correos se define a continuación:

- **Procesos operativos vigentes**

  – **Envío y recepción de dinero**

  El **giro postal** es un sistema de pago implementado por muchas empresas de correos de todo el mundo. Consiste en el envío mediante el servicio postal de una cantidad de dinero que se hará efectiva a una persona, bien en una oficina de correos o bien en la dirección indicada.

  Correos ha adecuado los sistemas informáticos en la operativa de admisión y pago de giros, creando un módulo o sistema para las diferentes aplicaciones de envío de dinero, con un ámbito exclusivo para la prevención del blanqueo de capitales, denominado SEDI/PBC.

  Actualmente, los sistemas informáticos afectados por estas modificaciones son IRIS (admisión y pago de giros), SGIE (pago de giros a domicilio) y HERA (admisión y pago de giros rurales).

  Mediante este nuevo sistema, es necesario efectuar un registro inicial de todos los clientes en el momento de realizar su primera operación, creando una «Ficha del Cliente» con una serie de datos personales obligatorios, entre los que se encuentra el de su actividad profesional o empresarial y el motivo del giro.

  La legislación postal establece, así como por la propia naturaleza del servicio, que es requisito indispensable la identificación del cliente con carácter previo a la realización de operaciones de admisión o pago de giro, mediante documento identificativo válido del remitente o beneficiario, cuyos datos sobre nombre, apellidos, domicilio y número y tipo de documento de identidad quedan registrados en los sistemas informáticos de la entidad.

  Los procesos de Envío y Recepción de Dinero describen detalladamente las normas operativas que regulan estos servicios.

  – **Archivo y control de documentos**

  La documentación de operaciones y clientes relacionados con operaciones de giro se conservará digitalmente en el sistema SEDI/PBC y la generada por comunicación de operativa sospechosa se archivará siguiendo las normas recogidas en el proceso Archivo-Control de Documentos.

El periodo de conservación de los documentos y registros justificativos de las operaciones y las relaciones de negocios, así como los exigidos para la aplicación de medidas de diligencia debida a los clientes, es de 10 años. Este periodo se contará desde el día en que se ejecute la operación o desde la fecha de terminación de la relación de negocios.

Transcurrido el periodo de 10 años establecido, la documentación se eliminará según el formato de esta, bien sea en papel o digitalizada.

Asimismo, llegado un periodo de 5 años desde la terminación de la relación de negocios o la ejecución de la operación ocasional, la documentación conservada únicamente será accesible por los órganos de control interno, incluido el APBC, y, en su caso, aquellos encargados de la defensa legal de la Entidad.

El soporte de conservación utilizado por Correos garantiza la integridad, la correcta lectura de datos, la imposibilidad de manipulación y la adecuada conservación y localización de los documentos.

- **Manual de PBC**

  El Manual de Prevención es norma de obligado cumplimiento para todos los empleados y directivos de la Entidad. Su primera versión fue aprobada por el Comité de Dirección de Oficinas y por la Comisión de Control el 29 de junio de 2006 y remitido al SEPBLAC el 6 de julio de ese mismo año. En él se recogen las medidas de control interno establecidas para prevenir el blanqueo de capitales y la financiación del terrorismo y ha sido modificado posteriormente en diversas ocasiones para adaptar su contenido a las novedades legislativas, a los nuevos procedimientos desarrollados por la Entidad en esta materia y a las recomendaciones formuladas tanto por el Servicio Ejecutivo de la Comisión como por el experto externo.

  Las actualizaciones del Manual son aprobadas por la Comisión de Control, con la excepción de aquellas que afecten únicamente a la composición del listado de paraísos fiscales o a las posibles modificaciones que puedan realizarse en los formularios contenidos en sus Anexos.

  La Comisión de Control, en Correos, es el órgano competente para la aprobación del Manual de PBC y autoriza la disposición y distribución de este a todos los directivos y empleados mediante su publicación en la intranet de Correos (Conecta).

- **Ficha de consulta rápida**

  Con el fin de poder formar desde el primer momento al personal operativo de Correos, el portal del mando genera avisos de itinerario formativo en PBC (Básico o Medio) que debe recibir según el puesto.

  La formación está disponible en el Campus Virtual de Correos (CVC) para el personal de oficina y en el espacio formativo de la PDA para el personal de distribución.

  Formación controla el registro de la formación realizada y superada en los correspondientes sistemas.

B) Organización interna

Correos es la empresa matriz del Grupo Correos y posee una participación del 100% en las filiales Correos Express, Correos Nexea y Correos Telecom, aunque ninguna de estas tres filiales realiza actividades sujetas a la normativa de prevención del blanqueo de capitales y de la financiación del terrorismo.

El Consejo de Administración de Correos, como máximo órgano de dirección de la Sociedad, ostenta las funciones y responsabilidades que establecen las leyes en materia de prevención de blanqueo de capitales y de la financiación del terrorismo.

El Consejo de Administración de Correos recibirá el informe del experto externo en el plazo máximo de tres meses desde su emisión y adoptará las medidas necesarias para solventar las deficiencias identificadas.

La Comisión de Control llevará un registro de toda la documentación e informes sometidos al Consejo de Administración y de las decisiones tomadas en cada caso.

- **Comisión de control**
  La Comisión de Control es el Órgano de Control Interno en materia de PBC y de acuerdo con la Instrucción del presidente de Correos de fecha 24 de noviembre de 2020, que sustituye a la anterior de 4 de mayo de 2009.
  Composición
  En virtud de cuanto antecede y de conformidad con lo dispuesto en el artículo 35 del Real Decreto 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, se acuerda que la Comisión Interna creada mediante Instrucción de fecha 4 de Abril de 2006 está compuesta por los siguientes miembros:

  – **Miembros con voz y con voto:**

    - Presidencia: el titular de la Subdirección de Compliance y Buen Gobierno ostentará la Presidencia. El titular de la Subdirección designará a un suplente que deberá ser miembro del área de PBC adscrita a dicha Subdirección.
    - Secretaría: la ostentará un representante de la Subdirección de Servicios Jurídicos. Será la persona que ejerza la subdirección quien designe a un titular y a un suplente de entre los miembros de su Subdirección.
    - Vocales:

      › Un representante de la Dirección de Financiera. Será la directora o el director quien designe a un titular y a un suplente de entre los miembros de su Dirección.
      › Un representante de la Dirección de Tecnología. Será la directora o el director quien designe a un titular y a un suplente de entre los miembros de su Dirección.
      › Un representante de la Dirección de Operaciones y Desarrollo de Negocio. Será la Directora o el director quien designe a un titular y a un suplente de entre los miembros de su Dirección.

› Un representante de la Dirección Comercial. Será la directora o el director quien designe a un titular y a un suplente de entre los miembros de su Dirección.
› Un representante de la Dirección de Productos y Servicios. Será la directora o el director quien designe a un titular y a un suplente de entre los miembros de su Dirección.

– Asistentes con voz, pero sin voto:

- El presidente de la Comisión designará, en cada sesión a celebrar, a uno o varios integrantes del Área de PBC que informarán a los miembros de la Comisión sobre los asuntos de dicha Área que se vayan a tratar según el orden del día aprobado.
  De acuerdo con los temas a tratar, se podrá invitar a las sesiones de la Comisión a cualquier persona de la Sociedad previa autorización del presidente de la Comisión.

– Funcionamiento:

- La Comisión se reunirá tantas veces como sea necesario de forma presencial o telemática, previa convocatoria de su presidente y, en todo caso, una vez cada mes. Se levantará acta de cada una de las reuniones debiendo ser firmada por el presidente y el secretario de forma manual o digital.
- Las decisiones en el seno de la Comisión se adoptarán por mayoría simple, mediante voto no secreto. Excepcionalmente y previa motivación razonada, el presidente puede exigir que la decisión se adopte por unanimidad o mediante voto secreto. El presidente, en caso de empate, tendrá voto dirimente.

– Funciones de la Comisión y Direcciones afectadas:
La Comisión impulsará la implantación y el desarrollo de cuantos procedimientos sean necesarios para dar cumplimiento a las obligaciones que se indican a continuación, en los términos que señala la Ley 10/2020, de 28 de abril y Real Decreto 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de PBC y FT, coordinando la actuación de cada una de las Direcciones que se vean afectadas.
Obligaciones:

a) Aplicación de medidas de diligencia debida (personas físicas y jurídicas).
b) Obligaciones de información.
c) Deber de confidencialidad.
d) Deber de abstención de ejecución de determinadas operaciones.
e) Procedimientos de control y comunicación adecuados para conocer, prevenir e impedir la realización de operaciones relacionadas con el blanqueo de capitales.
f) Conservación de documentos.
g) Formación del personal.

Se faculta a cada una de las Direcciones de Correos para complementar y desarrollar en el ámbito de sus competencias las obligaciones y procedimientos ya establecidos o que sean necesarios, contenidos en la Ley 10/2020, de 28 de abril y en el

Real Decreto 304/2014, de 5 de mayo por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo enumerados en esta instrucción y realizar las adaptaciones necesarias.

La Comisión supervisará los documentos que, en su caso, puedan elaborar dichas Direcciones, descriptivos de los procedimientos y de las medidas adoptadas para el cumplimiento de las obligaciones.

La Comisión, como órgano de control interno y supervisión, analizará, controlará y comunicará al Servicio Ejecutivo de la Comisión del Blanqueo de Capitales toda la información relativa a las operaciones o hechos susceptibles de estar relacionados con el blanqueo de capitales o la financiación del terrorismo.

Para la válida constitución de la Comisión será necesaria la asistencia de un miembro de cada Dirección, entendiéndose que cada Dirección tendrá un voto.

Las actas originales firmadas por los miembros asistentes de la Comisión de Control serán conservadas en archivos confidenciales de este órgano. Por otra parte, se remitirá una copia de estas al representante ante el Servicio Ejecutivo de la Comisión.

- **Representante ante el SEPBLAC**

El SEPBLAC o Servicio Ejecutivo de Prevención de Blanqueo de Capitales es la Unidad de Inteligencia Financiera española.

Desempeña las actuaciones tendentes a la prevención e impedimento de la utilización del sistema financiero o de empresas o profesionales de otra naturaleza para el blanqueo de capitales, así como las funciones de investigación y prevención de las infracciones administrativas del régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior.

Sus funciones más importantes son:

– Análisis de operaciones sospechosas o de Declaración Mensual Obligatoria (DMO).
– Supervisar a los sujetos obligados.
– Informar a las autoridades competentes.

La persona designada como representante por Correos ante el Servicio Ejecutivo de la Comisión debe ser una persona residente en España, que ejerza cargo de administración o dirección de la sociedad y estará encargada de la comunicación de cuanta información sea necesaria de conformidad con lo dispuesto en la normativa vigente y del resto de atribuciones que esta señala.

Tanto la designación como el cese del representante son a propuesta del secretario general y es nombrado por el Comité de Dirección y aprobado por el Consejo de Administración.

El representante ante el Servicio Ejecutivo de la Comisión será responsable del cumplimiento de las obligaciones de información establecidas en la presente ley, para lo que tendrá acceso sin limitación alguna a cualquier información obrante en el sujeto obligado, así como en cualquiera de las entidades del grupo, en su caso.

El representante ante el SEPBLAC puede autorizar o apoderar hasta a dos personas con el fin de que actúen en su nombre ante el SEPBLAC, asumiendo siempre que toda actuación de esas personas se entenderá hecha por el propio representante, tanto a efectos internos como de sus consecuencias exteriores.
Su nombramiento deberá ser realizado por el propio representante y aceptado por la persona autorizada.
Para designar personas autorizadas, el representante ante el SEPBLAC deberá comunicar la identidad de las personas a quienes concede esas facultades.
El puesto de autorizado deberá ser comunicado al SEPBLAC.
La documentación mencionada, tanto para la comunicación del representante como de las personas autorizadas deberá ser enviada a la siguiente dirección: SEPBLAC, Calle Alcalá, 48, 28014, Madrid. Alternativamente, podrá ser presentada directamente en esa dirección ante el Registro General del Banco de España. Igualmente, podrá ser presentada electrónicamente a través del Registro Electrónico de la Oficina Virtual del Banco de España.
El cese o sustitución del representante o personas autorizadas cuando tenga carácter disciplinario será informado al Servicio Ejecutivo.
Actualmente, el representante es el Subdirector de Compliance y Buen Gobierno, y la persona autorizada es un asesor jurídico adscrito a la Secretaría General y del Consejo.

Son **funciones del representante:**

a) Actuar como coordinador de todas las actividades que realiza Correos en su lucha contra el blanqueo de capitales y de la financiación del terrorismo.
b) Canalizar todas las comunicaciones existentes entre el SEPBLAC y Correos, y especialmente la Declaración Mensual de Operaciones, las comunicaciones por indicio de operativas sospechosas y las respuestas a los requerimientos de información.
c) Participar en las reuniones que convoque el SEPBLAC cuando estas tengan una finalidad consultiva, bien con Correos, bien con el Sistema Financiero en general o divulgativa sobre nuevos procedimientos a desarrollar por las entidades sujetas a normativa.
d) Comparecer en toda clase de procedimientos administrativos o judiciales en relación con los datos recogidos en las comunicaciones al Servicio Ejecutivo de la Comisión o cualquier otra información complementaria que pueda referirse a aquellas cuando se estime imprescindible obtener la aclaración, complemento o confirmación de Correos.
e) Mantener constantemente informada a la Comisión de Control de cualquier circunstancia que pudiera o debiera alterar o modificar la política de prevención de blanqueo de capitales que realiza Correos.

Para el cumplimiento de estas funciones el representante tiene acceso ilimitado a toda la información obrante en Correos.

- **Área de PBC**
  La unidad técnica para el tratamiento y análisis de la información es el Área de Prevención del Blanqueo de Capitales, integrada en la Vicesecretaría General y del Consejo.

El Área de Prevención está formada por personas especializadas en la detección y análisis de operaciones sospechosas, con formación adecuada y dedicación exclusiva a sus funciones de prevención.

Destacan las siguientes **funciones:**

a) Diseñar e implementar en Correos los programas de cumplimiento, seguimiento y control de la normativa vigente en materia de prevención de blanqueo de capitales y de la financiación del terrorismo, de acuerdo con las directrices que establezca la Comisión de Control.

b) Elaborar los planes de acción correctivos que se deriven de las novedades que vayan surgiendo (legislativas, tecnológicas, etc.) siguiendo las directrices establecidas por la Comisión.

c) Trasladar al representante de la Comisión las propuestas de revisión y actualización del Manual de Prevención de Capitales y de la Financiación del Terrorismo, así como de los Manuales de Procesos y del resto de normativa interna que se vean afectados por la política de blanqueo de capitales.

d) Supervisar el funcionamiento de los procedimientos de prevención e informar, periódicamente, al representante de la Comisión de las debilidades de control y cumplimiento detectadas.

e) Evaluar los riesgos a los que se enfrenta Correos y que pueden tener una mayor probabilidad de realizar blanqueo de capitales, con el fin de reforzar los procedimientos de prevención existentes y que se adapten al perfil de riesgo de la entidad, estando entre ellos la posibilidad de rehusar operaciones con determinados clientes.
Con este fin, elaborará y presentará un Informe de Autoevaluación del Riesgo a la Comisión de Control para que proceda a su aprobación. Este informe será actualizado anualmente, teniendo en cuenta la evolución del negocio y las actividades desarrolladas por Correos, así como otros factores tales como las nuevas tipologías de blanqueo de capitales y financiación del terrorismo, las modificaciones producidas en las listas de países considerados de riesgo, etc.

f) Analizar e investigar las comunicaciones de operaciones sospechosas recibidas de la Red de Oficinas, documentando apropiadamente aquellas que se consideren susceptibles de ser comunicadas al Servicio Ejecutivo dentro de los informes de «operaciones específicamente sospechosas de blanqueo de capitales» y decidiendo las que deben ser objeto de seguimiento, informando en todo caso a los empleados del curso dado a sus comunicaciones dentro del plazo definido.

g) Presentar al representante de la Comisión la Declaración Mensual de Obligaciones (DMO) y proceder al

análisis de las operaciones contenidas en la misma para apreciar la posible existencia de operaciones susceptibles de ser comunicadas también por indicio al SEPBLAC.

h) Presentar al representante de la Comisión la relación de operaciones con indicios de blanqueo de capitales para su análisis y control previo en la Comisión y la comunicación al SEPBLAC de las que así se hayan aprobado. A las actas de la Comisión se adjuntará un listado con todas las operaciones analizadas por el Área de Prevención, indicando expresamente si se ha procedido al examen especial de las mismas.

i) Elaboración de una base de datos de examen especial, en la que se registren los elementos básicos de las operaciones y una explicación motivada que justifique la decisión adoptada en cada caso (comunicación al SEPBLAC, mantener en seguimiento o archivo).

j) Llevar a cabo pruebas y muestreos sobre el nivel de eficacia del procedimiento establecido para la aplicación de medidas reforzadas de diligencia debida en la Red de Oficinas y Unidades de Reparto. Una vez revisada la documentación por el Área, se marcará con riesgo alto o pendiente de documentación a los clientes en los que se observe que la documentación presentada es insuficiente y se les solicitará documentación adicional.

k) Recabar y elaborar las informaciones requeridas por el SEPBLAC y otras autoridades, en materia de prevención de blanqueo de capitales.

l) Proponer al representante de la Comisión el alcance y contenidos en materia de formación sobre prevención de blanqueo de capitales y colaborar en el diseño y la elaboración de los módulos de formación del personal de Correos en esta materia.

m) Elaborar una Memoria Anual con las actuaciones e información estadística más relevante en materia de prevención: modificaciones en los procedimientos, implantación de nuevas herramientas informáticas, datos sobre el número de alertas, operaciones objeto de examen especial, comunicaciones por indicio al SEPBLAC, requerimientos de información, proceso de implantación de las recomendaciones propuestas por el experto externo, etc.

El Área de Prevención dispone de un manual interno que regula sus propias funciones y que solo se encuentra accesible para sus miembros, en el que se definen los procedimientos internos para el cumplimiento de sus fines, que serán conformes con las directrices que establezca la Comisión de Control.

Para el cumplimiento de sus funciones, el Área de Prevención contará con todos los medios humanos, materiales y técnicos necesarios.

- **Responsables de oficina/Unidad de distribución**

  En cada Oficina/Unidad de Distribución, el director, jefe de Unidad o quien haga sus funciones será el responsable encargado de velar por el cumplimiento de la normativa y será el interlocutor con la Unidad Técnica, todo ello con independencia de la responsabilidad propia de cada uno de los empleados de la Oficina/Unidad de Reparto.

  Sus funciones en materia de prevención del blanqueo de capitales son:

- Estar informado e informar a los empleados de la Oficina/Unidad de Reparto de la normativa interna sobre prevención, cumpliendo y exigiendo su cumplimiento dentro de la misma.
- Analizar con detalle cualquier operativa que muestre sospechas o indicios de posible vinculación al blanqueo de capitales comunicándolo, con la mayor brevedad, a través del procedimiento establecido en este proceso, así como cualquier circunstancia relacionada con la misma que se produzca posteriormente.
- Validar los conocimientos y formación de los empleados que realicen operaciones de envío y pago de dinero previamente a la designación de los mismos para tales funciones.
- Analizar la documentación acreditativa de la actividad profesional o empresarial y del origen lícito de los fondos de los clientes en aplicación de las medidas reforzadas de diligencia debida y decidir si se ejecuta la operación una vez verificada su validez y coherencia con el giro.
- Revisar la documentación aportada por las personas jurídicas, así como la DAE que debe traer debidamente cumplimentada incluyendo los titulares reales de la persona jurídica, para el inicio de la relación comercial.
- Controlar el archivo de las documentaciones relativas a clientes en cumplimiento de la normativa en materia de Prevención de Blanqueo de Capitales y de la Financiación del Terrorismo.
- Autorizar las operaciones con PEP y operaciones en las que se apliquen medidas reforzadas.

- **Empleados de oficinas/Unidad de distribución**

  Sus funciones, en lo que a prevención del blanqueo de capitales se refiere, serán cumplir con las indicaciones que se señalan en el manual de procesos internos, en particular:

  - Realizar la identificación y verificación de los clientes, así como la correcta introducción de los datos del mismo y escaneado de las documentaciones aportadas en los sistemas informáticos.
  - Comprobarán que los datos e informaciones incluidos en los sistemas coinciden con los grabados; una vez verificados, se deben modificar en caso de variación.
  - Identificar cualquier operación que dé lugar a sospechas o indicios de posible vinculación con el blanqueo de capitales, comunicándolo a la mayor brevedad al responsable de la Oficina/Unidad de Distribución.
  - Recibir los cursos de formación sobre prevención del blanqueo de capitales establecidos, así como conocer y poner en marcha los procedimientos para prevenir el blanqueo de capitales.
  - Mantener el deber de confidencialidad con respecto a todas las operaciones o clientes que hayan sido considerados como sospechosos de blanqueo de capitales.

C) Política de admisión de clientes

A fin de cumplir con la obligación establecida en el artículo 26.2 de la Ley 10/2010, de 28 de abril y el artículo 33 del RD 304/2014, de 5 de mayo, Correos tiene definida una

política de admisión de cliente de carácter gradual, que adopta precauciones reforzadas para aquellos clientes que presentan un riesgo superior al promedio.

Para prevenir eficazmente el blanqueo de capitales y la financiación del terrorismo, es fundamental la evaluación de posibles riesgos de los clientes. Por tanto, se entiende como prioritario el conocimiento de estos y se establecen diferentes categorías de clientes que serán evaluados en función de los siguientes factores:

- Frecuencia y cuantía de los envíos.
- Actividad que motiva los envíos.
- Origen o destino del dinero enviado.

Así se podrá determinar su grado (perfil) de riesgo y, en función de este, se aplicarán las medidas.

Según la política de admisión de clientes definida, se distinguen los siguientes **tres perfiles de riesgo:**

a) **Riesgo bajo:** clientes que, por sus características y tipo de operativa llevada a cabo, se considera que disponen de un riesgo reducido de blanqueo de capitales y financiación del terrorismo. No necesitan ninguna autorización específica para ser admitidos como clientes y se les aplican las siguientes medidas normales de diligencia debida:

   - Identificación formal del cliente y comprobación de su identidad.
   - Identificación del titular real y adopción de medidas adecuadas a fin de comprobar su identidad, con carácter previo a la operación.
   - Cuando se trate de una persona jurídica, cumplimentación de la DAE específica de personas jurídicas. Conocimiento de la actividad profesional o empresarial del cliente.
   - Conocimiento del propósito y la índole que motiva la operación.
   - Seguimiento continuo de la relación de negocio.

b) **Riesgo medio:** clientes cuyo riesgo en materia de prevención se considera superior al promedio y, por tanto, se les deben aplicar medidas reforzadas de diligencia debida. La admisión de este tipo de clientes requiere la autorización expresa del área de Prevención, otorgada tras la presentación y aprobación de la documentación adicional obtenida y la firma del formulario DAE.

   La Entidad cuenta con un desarrollo informático (SEDI/PBC) que permite detectar automáticamente a aquellos clientes, que, atendiendo a las reglas establecidas, superan los umbrales determinados. En estas reglas intervienen factores como su actividad profesional o empresarial, residencia (provincia) o nacionalidad, el país de destino u origen de sus operaciones y la superación de un importe establecido en el periodo de un mes natural.

c) **Riesgo alto:** personas que no son admitidas como clientes de Correos.

   - Clientes que realicen operaciones que se consideren fuera de lo normal, inusuales o que presenten indicios de sospecha en relación con la prevención de blanqueo de capitales.

- Personas a las que no sea posible aplicar las medidas de diligencia debida.
- Personas incluidas en listas oficiales de terroristas o de las que se tenga conocimiento de que están involucradas en operaciones de blanqueo de capitales.
- Clientes relacionados en peticiones de juzgados, Policía, requerimientos del Servicio Ejecutivo de la Comisión.
- Las personas jurídicas, o estructuras jurídicas sin personalidad, cuya estructura de propiedad y de control no haya podido determinarse.

- **Abstención de realizar operaciones**

  En ningún caso se admitirán clientes que:

  – Rehúsen entregar la documentación que permita su identificación.
  – Presenten documentos de identificación que alberguen dudas sobre su legalidad, legitimidad, no manipulación, etc.
  – Faciliten datos falsos o erróneos.
  – Pongan fin a la relación al ser requeridos para que faciliten información.
  – A los que no sea posible aplicar alguna de las medidas de diligencia debida previstas en el manual interno.
  – Oculten al titular real. Cuando utilicen a otros clientes, en un intento de evitar que se apliquen los requisitos de medidas de diligencia debida, y colaboren en suplantar al titular para enviar una operación o dividir una transacción en dos o más transacciones.
  – Realicen operaciones que presenten indicios de estar relacionadas con el blanqueo de capitales o la financiación del terrorismo.
  – Sean personas jurídicas cuya estructura de propiedad o de control no haya podido determinarse.

  El Área de Prevención podrá emitir instrucciones específicas a las Oficinas y Unidades de Reparto, informando sobre determinadas tipologías de operaciones que no deben ser aceptadas por presentar elementos de riesgo comunes con otras operaciones que ya han sido calificadas como operaciones con indicios. Estas comunicaciones escritas deben estar a disposición del SEPBLAC.

  Cualquier operación que dé lugar a sospechas o indicios puede no ser aceptada por el empleado y dará lugar a la comunicación inmediata como operación sospechosa. Cuando la abstención no sea posible o pueda dificultar la persecución de los beneficiarios de la operación, podrá llevarse a cabo con la comunicación de la operación sospechosa al Área de Prevención de Blanqueo de Capitales informando de los motivos que justificaron la ejecución de la operación.

  El Área de Prevención es la encargada de adoptar las decisiones finales sobre la abstención y de informar a los empleados sobre la forma de actuar en cada caso.

  La comunicación de las operaciones sospechosas al SEPBLAC efectuada por la Comisión expondrá, en su caso, los motivos que justificaron la ejecución de la operación.

  Cuando, en aplicación de la política interna o por la imposibilidad de aplicar las medidas de diligencia debida, los fondos recibidos deban ser devueltos al cliente, el reintegro de los mismos se efectuará a través del mismo medio de pago utilizado inicialmente para su ingreso.

- **Bloqueo de operaciones**
  Cuando el emisor o el receptor de un giro sea una persona incluida en alguna de las listas públicas relacionadas con el terrorismo o grupos afines, el sistema bloqueará la operación, a efectos de la aplicación del procedimiento previsto en la Ley 12/2003.
  Para ello, el sistema informático consulta automáticamente el listado elaborado por la Unión Europea y el listado de sanciones de Naciones Unidas, cruzando sus datos en el momento de procesar cada giro con los contenidos en la ficha de los clientes. Periódicamente se lleva a cabo la actualización del listado mediante su descarga en la correspondiente página web oficial.
  En ningún caso podrá revelarse al cliente ni a terceros las actuaciones que se puedan estar realizando en relación a las obligaciones derivadas de la ley de prevención del blanqueo de capitales y de la financiación del terrorismo.
  No se realizará ninguna operación sin la previa identificación ni cuando haya dudas sobre la validez de la documentación aportada, con especial atención a posibles falsificaciones.

12.2.4. Nuestras obligaciones en materia de PBC

A) Obligaciones de información

- Examen especial de aquellas operaciones que puedan estar vinculadas al blanqueo de capitales o la financiación del terrorismo, con independencia de su cuantía.
- Comunicación de los empleados al Área de Prevención y de la Comisión y el Representante al SEPBLAC de cualquier hecho u operación sobre la que existan indicios o certeza de su vinculación con el blanqueo de capitales y la financiación del terrorismo, así como responder adecuadamente a los requerimientos del Servicio Ejecutivo de la Comisión.
- Abstención de ejecutar operaciones sospechosas sin efectuar previamente dicha comunicación al SEPBLAC o su comunicación posterior inmediata cuando la abstención no sea posible o pueda dificultar la persecución de los beneficiarios de la operación.
- Comunicación sistemática (DMO):

  – Mensualmente se comunicarán al SEPBLAC mediante DMO:

    - Declaraciones positivas, que contienen:

      › Las operaciones individuales por importe superior a 1.500€.
      › Las operaciones no ejecutadas (fallidas).

    - Fraccionamientos, que contienen las operaciones de clientes que acumuladas en el mes superan los 1.500€, sin incluir las operaciones individuales de 1.500€.

El Departamento de Tecnología y Sistemas procesa la información contenida en los sistemas informáticos y filtra las operaciones realizadas por Correos, generando tres ficheros:

- Declaraciones positivas.

- Fraccionamientos enviados.
- Fraccionamientos recibidos:

  – Conservación de documentos acreditativos de las operaciones e identidad de quienes la realizan, así como todos los documentos exigibles en aplicación de las medidas de diligencia debida, durante un plazo de 10 años desde la ejecución de la operación.
  – Deber de confidencialidad, no revelar al cliente o a terceros las operaciones comunicadas o que están siendo objeto de examen especial.
  – Operaciones sospechosas. Se entenderá por operaciones sospechosas las siguientes:

    - Operaciones no ejecutadas (fallidas); denominación que conceptúa aquellas operaciones que no llegan a realizarse porque el cliente rehúsa terminarla cuando se le exige algún requisito esencial de identificación, cuando se niega a cumplimentar la Declaración de Actividad Económica o a aportar la documentación acreditativa de su actividad.
    - Operaciones inusuales o fuera de lo normal, en especial:

      › Operaciones en las que se aprecie que el cliente fracciona la operación en varias para eludir el deber de identificación adicional.
      › Cuando existan indicios o certeza de que los clientes no actúan por cuenta propia, intentando ocultar la identidad del cliente real.
      › Operaciones en las que, conociendo la actividad del cliente, no exista una explicación razonable sobre el origen o destino de las operaciones realizadas.
      › Operaciones en las que el cliente no disponga o rehúse presentar la documentación justificante de domicilio permanente o temporal en España.
      › Operaciones en las que el cliente trata de eludir las medidas de diligencia debida.

    - En general, operaciones que presentan indicios de blanqueo de capitales o conexión con actividad delictiva.

Los empleados que detecten operaciones que presenten estos indicadores de riesgo deben abstenerse de ejecutarlas y comunicarlas al Área de Prevención para que adopte una decisión sobre su comunicación por indicio al Servicio Ejecutivo de la Comisión.

- Comunicación de **operaciones sospechosas:**
  La operación se puede comunicar a esta Área de dos formas diferentes:

  – En Conecta, el responsable de la Oficina/Unidad de Distribución o el empleado que tuviera conocimiento de ella la comunicará al Área de Prevención del Blanqueo de Capitales, mediante el formulario establecido en Conecta.
  – En la aplicación, para que el usuario pueda acceder al formulario para el aviso de una operación sospechosa mientras realiza la operación pulsando el botón rojo «Avisar operación sospechosa». El citado formulario consta de un campo de observaciones que el usuario debe rellenar y los correspondientes botones de envío o de cancelar y se requerirá el tipo de operación sospechosa, que sería alguna de las siguientes:

- Documentación sospechosa (cuando la documentación es falsa).
- No aporta documentación (operación no ejecutada).
- Operación sospechosa (opción por defecto).

En el plazo máximo de 5 días desde la recepción de la comunicación, el Área de Prevención de Blanqueo de Capitales acusará recibo de la misma, por el medio que considere oportuno, siempre que permita tener constancia de su recepción. El Área de Prevención dispondrá de un plazo de 3 meses desde el acuse de recibo para notificar a la persona que atendió al cliente el estado de la comunicación, y dispondrá de un plazo máximo de 6 meses para finalizar el análisis y notificar las medidas adoptadas, a los efectos de que, en caso de no producirse dicha notificación, esta pueda actuar conforme a lo previsto en el artículo 18.4 de la Ley 10/2010, de 28 de abril. Dicha notificación se hará por el medio que el Área de Prevención considere oportuno, siempre que permita tener constancia de su recepción.

En cualquier momento, la persona que hubiera realizado la comunicación podrá requerir del Área de Prevención de Blanqueo de Capitales cualquier información relativa al estado de tramitación del asunto.

La documentación generada como consecuencia de la comunicación de operación sospechosa, así como las contestaciones del Área de Prevención de Blanqueo de Capitales, se archivarán en la oficina siguiendo la información recogida en el Proceso Archivo-Control de Documentos en un dosier.

Por último, el Área de Prevención dispone de una lista interna con los clientes comunicados al SEPBLAC por su intervención en operaciones con indicios de blanqueo de capitales y financiación del terrorismo, con el fin de bloquear su ficha en el sistema y evitar que puedan realizar nuevas operaciones con la Entidad.

- **Canal interno** de comunicación de operativa sospechosa:
  Todos los empleados de CORREOS se encuentran obligados a cumplir con los principios contenidos en el Programa de Prevención de Riesgos Penales del Grupo Correos, aprobado por el Consejo de Administración el 27 de noviembre de 2014, en el que se incluyen un canal interno de comunicación y denuncia del Grupo.
  Este canal tiene por objeto «establecer un procedimiento de comunicación con el Comité de Cumplimiento del Grupo para empleados del Grupo Correos y para terceros que conozcan o mantengan relación comercial o contractual de cualquier clase, o utilicen los servicios prestados por el Grupo Correos con alguna de las Sociedades que lo integran, sobre aquellas conductas o hechos relacionados con una actuación u omisión presuntamente delictiva».
  Para llevar a cabo la comunicación, se debe emplear preferiblemente el modelo de formulario disponible en la página web de Correos, debiendo adjuntar toda la documentación de la que se disponga y que sirva de soporte justificativo de la misma.
  La persona comunicante deberá estar disponible para cooperar con el Comité de Cumplimiento durante todo el proceso de investigación de los hechos comunicados.

B) Medidas de control interno

El artículo 26 de la Ley 10/2010 de prevención del blanqueo de capitales y de la financiación del terrorismo establece, con las excepciones que se determinen reglamentariamente, una serie de obligaciones de control interno a los sujetos obligados. Entre estas obligaciones están la de aprobar y aplicar políticas y procedimientos de prevención, la de establecer órganos adecuados de control interno responsables de la aplicación de aquellos y la de aprobar un manual de prevención.

Recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo (SEPBLAC):

- Se comprobará que la información y documentación disponible se encuentra actualizada.
- Establecimiento de medidas de control interno adecuadas para la actividad desarrollada por Correos.
- Formación, la Comisión de Control diseñará y aprobará un plan anual de formación en materia de prevención del blanqueo de capitales y de la financiación del terrorismo y transmitirá a los empleados de la entidad la concienciación de las exigencias derivadas de la Ley 10/2010, a través de planes y cursos de formación.
- Protección de datos, el tratamiento de datos personales que resulte necesario para el cumplimiento de las obligaciones establecidas en esta Ley 10/2010 se encuentra amparado por lo dispuesto en el artículo 8.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 6.1 c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no precisando del consentimiento del interesado.
  Los datos recogidos por los sujetos obligados para el cumplimiento de las obligaciones de diligencia debida no podrán ser utilizados para fines distintos de los relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo sin el consentimiento del interesado, salvo que el tratamiento de dichos datos sea necesario para la gestión ordinaria de la relación de negocios.

- Código de conducta, en cumplimiento de lo establecido en el artículo 30.2 de la Ley 10/2010 de 28 de abril de 2010 de prevención del blanqueo de capitales y de la financiación del terrorismo, se garantizarán altos estándares éticos en la contratación de directivos y empleados.
  Por otra parte, todos los empleados de esta sociedad estatal se encuentran sometidos a los principios contenidos en el Código General de Conducta aprobado por el Consejo de Administración de la Sociedad Estatal que entró en vigor el 1 de enero de 2005.

- Responsabilidad de los administradores y directivos, además de la responsabilidad que corresponda a la Entidad, aun a título de simple inobservancia, quienes ejerzan en la misma cargos de administración o dirección, sean unipersonales o colegiados, serán responsables de las infracciones cuando estas sean imputables a su conducta dolosa o negligente.

- Auditoría del sistema, sin perjuicio de las funciones atribuidas a la Dirección de Auditoría e Inspección relativa a auditar los servicios y procesos operativos, la Comisión de Control para la Prevención del Blanqueo de Capitales determinará anualmente la forma en que ha de auditarse el sistema de prevención, conforme al artículo 28 de la Ley 10/2010, de 28 de abril.

  De esta forma, se elegirá a un experto externo que reúna las condiciones académicas y de experiencia profesional, así como todos los requisitos exigidos por la normativa vigente en cada momento.

  Finalmente, cabe destacar que la Dirección de Auditoría e Inspección, anualmente, realizará, de acuerdo con el artículo 33.m) del Real Decreto, 304/2014, de 5 de mayo, auditorías de los órganos y medidas de control interno definidas por Correos. En estas auditorías, de acuerdo con el alcance definido, se incluirá una opinión sobre el grado de ajuste de los procedimientos a la normativa vigente y a las recomendaciones emitidas por el Servicio Ejecutivo de la Comisión y el experto externo.

  Asimismo, durante el proceso de revisión continua de la red de Oficinas y Unidades de Distribución, podrá verificar el cumplimiento de determinadas obligaciones en materia de prevención, como la conservación de los documentos de identificación de los clientes y de los impresos, así como de la obtención y conservación de los documentos obtenidos en aplicación de las medidas reforzadas de diligencia debida.

12.2.5. Fraude y estafas

El fraude es el resultado de delincuentes que operan esquemas o estafas para persuadir a los consumidores para que envíen dinero con fines específicos que podrían parecer financieramente atractivos para el consumidor, pero que en realidad solo son maneras de convencerlos de que se desprendan de su dinero. La mayoría de los fraudes al consumidor involucran la percepción por parte de la víctima de que recibirá algún tipo de ganancia financiera o de que ayuda a un amigo, pariente o ser querido.

Como ejemplo, comentamos algunos **tipos de estafas** que se han detectado en Correos en operativa de envío de dinero:

1. **Alquiler.** El estafador anuncia una propiedad en alquiler, con un descuento considerable para así obtener la mayor cantidad de respuestas o consultas posibles. Incluye fotografías o planos en el anuncio para que la propiedad parezca legítima. Cuando la víctima demuestra su interés en la propiedad, el estafador le pide a la víctima que envíe dinero en forma de giro inmediato para poder verificar los fondos u otros motivos que parecen ser legítimos y convincentes. La víctima envía el dinero y finalmente lo pierde debido a que la propiedad en alquiler no existe.

2. **Compras por internet.** La víctima demuestra interés en un producto, un artículo de subasta o un servicio anunciado en línea. El estafador utiliza una serie de tácticas

para que la venta parezca legítima, pero la víctima nunca recibirá el artículo que compró después de enviar el dinero. El anunciante (estafador) pidió al cliente que le mandara escaneado el resguardo de imposición del giro. El cliente, por precaución, mandó el resguardo tapando el localizador del giro. Seguidamente, el cliente recibió un enlace web simulando la página oficial de Correos donde debía introducir el código del localizador.

3. **Lotería nigeriana.** Se informa a la víctima (mediante una comunicación telefónica, correo electrónico o correo postal no esperado) que ganó un gran premio de la lotería o un sorteo y se le indica que debe pagar una pequeña suma de dinero para cubrir los gastos por concepto de impuestos o de procesamiento antes de reclamar tal premio. Las empresas legales organizadoras de sorteos no solicitan a los ganadores de premios que envíen dinero por adelantado para recibir un premio.

4. ***Phising***. Tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios.
   En una página web se ofrece un trabajo, con contrato legal, para «agentes aduaneros». Su cometido es recibir dinero en la cuenta bancaria y sacarlo para transferirlo, a través de una entidad internacional, a otra cuenta extranjera. A cambio se cobra el diez por ciento del montante total. En la confección del contrato de trabajo se obtienen la cuenta bancaria y datos personales de la «mula», necesario para recibir la transferencia que suele venir de una operación de fraude.

5. **Secuestro exprés.** En estos falsos secuestros exprés, la víctima suele recibir una llamada en la que se le informa de que su familiar ha sido secuestrado y debe enviar un dinero de manera inmediata para proceder a su liberación. En realidad no es más que un timo. No existe tal secuestro. Se trata de bandas que se dedican a hacer llamadas al azar, hasta que dan con alguna persona que coincida que no tiene a su familiar en ese momento con ella ni tampoco puede contactar telefónicamente con el supuesto secuestrado, bien porque esté trabajando, se encuentre de viaje, o cualquier otro motivo. De estas llamadas, alguna resulta efectiva y la víctima acaba enviándoles dinero a los estafadores. Se han detectado, por ejemplo, numerosas llamadas realizadas por internos de Centros Penitenciarios en Chile.

6. **Relaciones.** El estafador crea una relación falsa con la víctima, quien cree que es real (quizás mediante alguna aplicación en línea, un sitio web de citas u otra plataforma de redes sociales). En algún momento, la comunicación en línea avanza y el estafador solicita dinero a la víctima por diversas razones como viajes, asuntos médicos, etc.

7. **Personas de la tercera edad.** El estafador se comunica con una persona de la tercera edad y se hace pasar por su nieto o por una persona con autoridad, como un policía, un profesional médico o un abogado. El estafador describe una situación de urgencia o emergencia (gastos médicos, gastos de viaje de emergencia) en la que participa el nieto que necesita que le envíen dinero inmediatamente. Nunca hubo realmente una emergencia.

Puedes detectar transacciones inducidas fraudulentamente si observas:

- Indicadores de conducta:
  - Clientes que parecen inquietos o confundidos, especialmente ancianos y adultos dependientes.
  - Clientes que parecen muy entusiasmados por enviar dinero.
  - Clientes que expresan preocupación sobre enviar dinero para una situación de emergencia.
  - Clientes que parecen entusiasmados o ansiosos por recibir una suma de dinero importante o una «oportunidad única en la vida».
  - Clientes que podrían enviar dinero por primera vez y hacen preguntas sobre el proceso.
- Indicadores de la operación:
  - Clientes que realizan varias transacciones en un mismo día o durante algunos días.

12.3. Compromiso ético y transparencia

12.3.1. Cumplimiento normativo

Código General de Conducta del Grupo Correos. Aspectos clave

Correos es la **primera empresa pública que dispone de un Código General de Conducta desde el año 2005,** lo que refleja la firme apuesta por relacionarse con su entorno de una manera ética, honesta y transparente. Correos ha trabajado por mejorar y perfeccionar sus procesos y abordar desde la integridad todas las relaciones con sus grupos de interés. En 2014 se actualizó por primera vez y el 22 de julio del 2021 se aprobó en el Consejo de Administración su revisión.

El **Código General de Conducta** refleja los valores que marcan la forma de trabajar de Correos y contiene los principios generales que rigen la actuación de sus empleados. Además de ser de obligado cumplimiento, supone un marco de actuación útil para que todos los que trabajan en el Grupo conozcan qué tipo de comportamiento se espera de ellos. Este código es uno de los mecanismos con los que se garantiza la ética empresarial, pero no el único, ya que además se cuenta con otros **instrumentos internos** como son:

- Comité de Cumplimiento.
- Programas de formación específica sobre cumplimento.
- Programa de Prevención de Riesgos Penales.
- Portal de Transparencia.
- Adhesión a los Principios del Pacto Mundial de Naciones Unidas.
- Política de Prevención de Blanqueo de Capitales.

El incumplimiento del contenido del Código de Conducta conlleva riesgos legales, pero algunos de ellos no son de carácter penal, sino de reputación. Las personas que trabajan en Correos son responsables de construir y proteger la reputación del Grupo. En este sentido, un comportamiento ejemplar mejora la percepción del público sobre Correos, mientras que un comportamiento incorrecto repercutirá negativamente en la compañía, aunque no conlleve necesariamente riesgos penales.

Por ello, el Código General de Conducta de Correos busca proporcionar una hoja de ruta para responder ante los problemas éticos de manera coherente con los principios del Grupo.

Objetivos del Código General de Conducta del Grupo Correos.

- **Establecer pautas generales de comportamiento.** Establece los principios y pautas que deben regir el desarrollo de las actividades y relaciones comerciales de las sociedades del Grupo Correos, tanto a nivel interno (empleados, directivos y administradores) como externo (mercado y resto de competidores).
- **Propiciar un entorno ético de trabajo.** Facilita un marco para el desarrollo de las tareas cotidianas en un contexto ético, profesional y honesto, de acuerdo con los principios de buena fe y con la legalidad vigente.
- **Proporcionar mecanismos para el cumplimiento.** Garantiza el cumplimiento a través de herramientas a disposición de los empleados en el caso de que se vean comprometidos los principios éticos de la compañía.

En Correos existen unos **valores corporativos** que definen sus actuaciones, y que se han construido y consolidado de forma participativa poniéndolos en común con todos los empleados del grupo. **Estos valores son** los siguientes:

- Confianza. Se trabaja por satisfacer las expectativas de los clientes, siendo para ellos Correos un *partner* confiable para sus proyectos.
- Sostenibilidad. Se toman decisiones que garanticen que la actividad de Correos se desarrolle teniendo en cuenta el futuro de la sociedad, el medioambiente y el país.
- Innovación. Anticipación a los cambios en la sociedad y en el mercado, explorando nuevas soluciones que permitan adaptarse a un entorno cambiante.
- Cercanía. A través de la capilaridad de la red de Correos, se facilita la vida de las personas y las empresas con independencia de dónde se encuentren.
- Compromiso. El conjunto de esfuerzos individuales construye un mejor equipo, y se trabaja por garantizar la calidad laboral y por promover su desarrollo profesional.

El Código General de Conducta es de **obligado cumplimiento para** las siguientes personas y entidades:

Personas:

- Todos los empleados y directivos de las sociedades integrantes del Grupo Correos.
- Los miembros del Órgano de Administración de las sociedades del Grupo Correos, independientemente de la forma adoptada.

- Los miembros de comités, direcciones u órganos colegiados similares que desempeñen funciones de dirección o gestión dentro del Grupo o de las sociedades del mismo.

Entidades:

- Las sociedades subcontratistas, intermediarios, agentes, comisionistas cuando carezcan de procedimientos internos o de códigos de conducta equivalentes.
- Las sociedades y organizaciones vinculadas con el Grupo Correos por una relación de control efectivo, o cuya gestión o administración esté encomendada a sociedades del Grupo Correos.

Además el Código General de Conducta persigue que:

- Ninguna clase de incumplimiento será tolerado o ignorado.
- Ningún empleado que denuncie actividades sospechosas, ilícitas o contrarias al presente Código podrá ser sancionado por este motivo.

A) Principios y pautas de conducta del Grupo Correos

Correos promueve de forma activa un entorno de trabajo inclusivo, impulsando la diversidad como pilar estratégico de la compañía, y con el respeto a los derechos humanos y las libertades fundamentales como base de este compromiso. Y lo hace de manera:

- Transversal. Impacta en todas las áreas de la compañía.
- Global. Se trabaja con las diferentes dimensiones de la diversidad en su conjunto.
- Social y comprometida. Con las iniciativas a nivel interno y externo que apoyan la diversidad y la inclusión.

La **política de Correos** se basa en **tres principios fundamentales** de la compañía:

1. Respeto e igualdad de trato

Las personas que integran Correos deben respetar la igualdad de trato de todas las personas con las que trabajan y se relacionan. En ningún caso se tolera:

- La conducta abusiva, hostil u ofensiva, así como la discriminación por razón de raza, sexo, orientación sexual, creencia, ideología, religión, origen social, discapacidad, nacionalidad, edad u otra circunstancia.
- El acoso en el trabajo, ya sea de carácter sexual o de cualquier otro tipo. Se puede consultar, en nuestro plan de igualdad, el protocolo a seguir contra el acoso sexual, laboral o moral.

2. Igualdad de oportunidades

- Contribución a la lucha contra la desigualdad de género.
- Impulsar la integración de personas en riesgo de exclusión social o con cualquier tipo de discapacidad.

- Trabajando por la no discriminación de personas en función de características como raza, origen, religión u orientación sexual.
- Fomentando la convivencia enriquecedora de distintas generaciones y culturas.

Por ello, se garantiza que todas las personas puedan vivir sus diferencias de forma abierta, independientemente de su edad, raza, género o capacidades, ofreciendo unas condiciones laborales dignas y justas para todas las personas que conforman el Grupo.

Todos los empleados deben disfrutar de las mismas oportunidades para su desarrollo profesional, por lo que las decisiones de promoción solo pueden estar basadas en parámetros objetivos como son:

- Formación.
- Mérito.
- Esfuerzo.
- Dotes de liderazgo.

3. Derechos humanos y libertades fundamentales

Todas las personas que integran el Grupo Correos están obligadas a respetar los siguientes derechos y normativas:

- Derechos fundamentales y libertades públicas recogidos en la Declaración Universal de los Derechos Humanos.
- Pacto Internacional de Derechos Civiles y Políticos.
- Pacto Internacional de Derechos Económicos, Sociales y Culturales.
- Constitución española.
- Toda normativa destinada a la protección de los derechos fundamentales y libertades públicas reconocidos en el territorio español.

Diversidad. Es la convivencia e interacción entre personas con diferencias de género, generación, discapacidad o cultura que hacen a las personas únicas y a Correos tan heterogéneo como la sociedad.

Inclusión. Es el establecimiento de un entorno laboral que genere oportunidades a todos y cada uno de los empleados respetando su singularidad, y que esta se refleje en su trabajo.

Acoso sexual. El acoso sexual puede consistir en una conducta verbal, física o visual de naturaleza sexual que una persona podría considerar ofensiva. Puede ser de muchos tipos:

- Insinuaciones sexuales, petición de favores sexuales o exigencia de citas no deseadas.
- Chistes, bromas, imágenes, mensajes de texto o correo electrónico de naturaleza sexual.

B) Seguridad y salud en el ámbito laboral

La seguridad y la salud en el trabajo es un aspecto fundamental. El Grupo Correos cumple rigurosamente con normativas y directrices sobre los siguientes aspectos:

- Salud e higiene en el trabajo.
- Prevención de riesgos laborales.
- Equipos técnicos necesarios para el desempeño de las funciones de los empleados.
- Cursos de formación para la protección de los trabajadores.

Uno de los objetivos del Grupo es fomentar el **equilibrio entre el trabajo y la vida personal.** Por ello, se persigue una adaptación en la medida de lo posible a las circunstancias personales y familiares de los empleados, directivos y administradores, ofreciendo:

- Modificación de las jornadas, horarios o turnos de trabajo que se someten a examen de la comisión de empleo central o de las comisiones de empleo provinciales.
- Teletrabajo en situaciones concretas.
- Programas de acción social que facilitan tratamientos sanitarios, estudios universitarios, educación infantil, atención a hijos con discapacidad, pensiones, anticipos y préstamos sin interés.
- Acciones de formación y sensibilización, así como medidas incluidas en su regulación interna.

El **riesgo laboral** es la posibilidad de que un trabajador sufra un determinado daño derivado del trabajo. Para saber si es grave, se valora la probabilidad de que se produzca y la severidad del mismo. Pueden ser, entre otros: un accidente que tenga lugar en el puesto de trabajo, al acudir a una reunión o al cargar con algún material pesado relacionado con sus tareas durante la jornada laboral.

Entre las **obligaciones y responsabilidades** de los órganos sociales de Correos, a los miembros del Consejo de Administración o de la Junta General de Accionistas del Grupo Correos, se les exige un comportamiento ejemplar basado en los **siguientes criterios:**

- **Lealtad:** ejerciendo el cargo con lealtad a la organización, socios, accionistas, clientes y sociedad. Se debe notificar al Comité de Dirección toda oportunidad de negocio que pueda resultar de interés para la compañía.
- **Legalidad:** respetando, en el ejercicio de sus funciones, la legalidad vigente.
- **Respeto:** hacia compañeros, clientes, proveedores y demás grupos de interés, así como al entorno que nos rodea (sociedad y medioambiente).
- **Confidencialidad:** cumplimiento del deber de reserva y confidencialidad sobre la información relativa al Grupo o cualquiera de las sociedades que lo integran, incluso después de haber cesado en sus funciones.
- **Actuación adecuada ante conflictos de interés:**

  – Absteniéndose de realizar funciones o desempeñar cargos, directa o indirectamente, en otras empresas o sociedades cuyas actividades o intereses sean concurrentes o estén en conflicto con el Grupo Correos. En este sentido, antes de aceptar un cargo, empleo o colaboración en otras sociedades o empresas, ya sean de ámbito privado o público, deberán obtener la autorización expresa y por escrito del Órgano de Adminis-

tración de la sociedad a la que se pertenezca, que deberá ser aprobada por mayoría de dos tercios.

– Absteniéndose de realizar, directa o indirectamente, transacciones profesionales o comerciales con el Grupo o con cualquiera de las sociedades que lo integran a título personal, salvo autorización expresa del Órgano de Administración por mayoría de sus miembros.

Uso adecuado de los materiales de la empresa. El Grupo Correos confía en sus empleados para que utilicen los recursos de la empresa de forma honesta, responsable y eficaz. La compañía espera que estos materiales sirvan para la ejecución de las tareas diarias y que, una vez se cese la actividad, se devuelvan en perfectas condiciones.

- Bienes físicos: ordenadores, móviles, tabletas, furgonetas, papel, etc.
- Recursos financieros: gastos de la organización en materia de desplazamientos, dietas, eventos, etc.
- Activos electrónicos: correo electrónico, número de teléfono, internet, etc.

El Grupo Correos es el propietario de todos los materiales que presta a sus empleados para el correcto desempeño de su trabajo y, por tanto, el periodo de utilización se corresponde con el de la relación contractual entre el trabajador y la compañía. Una vez que se finaliza un contrato, todos los empleados deben devolver, de manera obligatoria, todos los materiales al Grupo.

C) El cumplimiento ético y normativo

Todos los administradores, directivos, socios y empleados de las sociedades que integran el Grupo Correos están obligados a cumplir la legalidad vigente en la ejecución de sus respectivos trabajos, independientemente de su rango y ámbito de aplicación.

Del mismo modo, **toda empresa con la que el Grupo Correos tenga que subcontratar la prestación de un servicio o ejecución de una actividad deberá cumplir con la legalidad,** así como con lo establecido en el presente Código, siendo la empresa del Grupo Correos que la contrata la encargada de velar por el correcto cumplimiento del mismo.

El Grupo Correos no subcontratará empresas que:

- No respeten los derechos de los trabajadores, las disposiciones relativas a la salud, seguridad e higiene en el trabajo (incluidas las relativas a la prevención de riesgos laborales).
- Tengan contratado personal cuya situación laboral no cumpla con lo indicado en la legislación vigente.
- No ajusten su actuación al código de Correos. En el pliego debe existir una cláusula de buenas prácticas en el que la empresa contratada se compromete a cumplir con el código y el resto de normativa interna que lo desarrolla. Asimismo, los pliegos incorporan cláusulas sobre criterios medioambientales, sociales (como la igualdad de género o la seguridad laboral) y de innovación y desarrollo.

La **actividad contractual del Grupo Correos** está sujeta a los principios de publicidad, concurrencia, transparencia, confidencialidad, igualdad y no discriminación.

1. La privacidad y confidencialidad

Los integrantes del Grupo Correos tienen el deber y la obligación de guardar secreto sobre toda aquella información relativa a la empresa que pudiera ser clasificada como privilegiada, confidencial o reservada y, por tanto, no podrá ser revelada. Todos los archivos deberán ser celosamente conservados de acuerdo con la legislación vigente y las políticas y procedimientos internos del Grupo Correos.

¿Qué se entiende por información confidencial?:

- Toda aquella información no pública que afecta a los negocios del Grupo en su mayor amplitud: detalles de clientes, mercado, datos financieros, métodos o procesos.
- Información facilitada por terceros al Grupo y que esté sujeta a compromisos de confidencialidad.

Existen dos supuestos de divulgación de información confidencial:

- Cuando sea necesaria para el desempeño de una actividad deberán adoptarse todas las cautelas y medidas posibles para proteger su carácter reservado.
- Cuando esa información concierne a un tercero solo podrá ser divulgada con la aprobación de ese tercero.

Los empleados que, por razón de su cargo, manejen los datos de carácter personal de sus empleados, directivos, administradores o socios solo podrán hacer uso de ellos de acuerdo con lo señalado en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), así como la normativa que la desarrolla, atendiendo a los procedimientos internos implantados en el seno del Grupo.

El tratamiento de los datos de carácter personal deberá ajustarse al fin para el que fueron recabados.

2. Propiedad industrial e intelectual

Las sociedades que conforman el Grupo Correos protegen sus derechos de propiedad industrial e intelectual y respetan los derechos de terceros en la materia. Por ello, cuando se utilice este tipo de información, se deben adoptar medidas de diligencia y cuidado específicas.

Los derechos de propiedad industrial e intelectual protegen, entre otros:

- Procesos.
- Diseños.
- Métodos.
- Estrategias comerciales.

- Información de clientes.
- Precios.

Se prohíbe:

- La divulgación, obtención de copias o utilización para obtener un beneficio personal o ilegítimo.
- La cesión a terceros sin la previa y expresa autorización del Grupo Correos.
- La reproducción de material de terceros protegido por derechos de propiedad intelectual o industrial.
- El empleo de *software* y programas de ordenador sin la correspondiente licencia.

Propiedad industrial. La **propiedad industrial** protege todas las creaciones que están relacionadas con la industria: patentes y modelos de utilidad, signos distintivos y diseños.

Propiedad intelectual. La **propiedad intelectual** protege las creaciones en las que queda plasmada la personalidad del autor, tratándose de creaciones únicas, no producidas industrialmente o en serie.

3. Obsequios y regalos

El Grupo Correos prohíbe a todos sus empleados la aceptación u ofrecimiento de ventajas o incentivos de carácter ilícito con el fin de influir en la toma de una decisión de cualquier índole. En concreto, se prohíben:

- Regalos, promesas, concesiones, sobornos, atenciones excesivas o comisiones ocultas.
- Donaciones políticas, salvo que hayan sido divulgadas y cumplieran con lo establecido en la ley, siempre y cuando hubieran sido autorizadas por el Grupo Correos.

En cualquier caso, en materia de ofrecimiento y aceptación de regalos, se estará a lo dispuesto en los procedimientos internos instaurados en el Grupo Correos (Política de regalos y hospitalidades).

Estos principios se utilizan con proveedores, competidores, socios, inversores y agentes del mercado.

4. Liderazgo y transparencia

El liderazgo ejemplar, transparente y responsable de los profesionales de Correos aporta valor a la actividad y responde a las demandas de los grupos de interés, a la vez que favorece la eficiencia y calidad de los servicios.

En el Grupo Correos se persigue que tanto la directiva como los líderes de los equipos sean un ejemplo a seguir, ya que como empresa pública tienen el compromiso de actuar con transparencia y honradez. La selección de los perfiles de dirección se hace siempre según sus conocimientos, experiencia y capacidad de liderazgo, optando en todo momento por un modelo de dirección compartida.

Por consiguiente, la rendición de cuentas con los grupos de interés es importante para Correos, dando acceso público a la información a través del Portal de Transparencia de Correos, mediante el cual los ciudadanos pueden solicitar información sobre la compañía.

Rendición de cuentas. La **rendición de cuentas** es el proceso por el cual los grupos de interés de una organización (sociedad, clientes, accionistas, empleados, etc.) pueden vigilar y evaluar la gestión de sus servicios a través de mecanismos de transparencia y fiscalización.

El Grupo Correos exige a sus empleados que, en el ámbito profesional, sean responsables, comprometidos y respetuosos.

- Deben hacer abstracción de sus intereses personales cuando tomen decisiones empresariales.
- Deben procurar que la administración y gestión de la compañía se organice atendiendo al interés social y no al familiar o personal.
- Deben perseguir la creación de valor a largo plazo.
- Deben velar por el más completo compromiso con la legalidad, la seguridad y la adecuada gestión de riesgos.

El Grupo Correos se comporta de forma ética y legal en el mercado y con sus competidores. El compromiso del Grupo con la competencia leal incluye:

- Actuar para que se cumpla con lo establecido en la normativa de defensa de la competencia y competencia desleal, tanto nacional como comunitaria.
- Evitar todas aquellas actuaciones que, recogidas en dicha normativa, son consideradas por el legislador como conductas prohibidas, como pueden ser:
  - Actos de engaño.
  - Actos de confusión.
  - Omisiones engañosas.
  - Prácticas agresivas.
  - Actos de comparación.
  - Actos de imitación.
  - Explotación de la reputación ajena.

Competencia desleal. Se considera competencia desleal aquellos comportamientos contrarios a la buena fe que tratan de alterar el funcionamiento del mercado o de los consumidores y usuarios de manera ilícita.

La imagen y reputación del Grupo Correos que se proporciona al exterior es esencial. Por ello siempre se debe actuar con respeto, dignidad y profesionalidad, intentando cuidar y preservar la imagen del Grupo, evitando cualquier conducta que pueda dañar su imagen, marca o reputación.

5. Conflicto de interés

El Grupo Correos no acepta la existencia de conflictos de interés entre sus empleados, directivos o administradores. Se entiende por **conflicto de interés** aquellas decisiones que se toman en el ámbito profesional que no están influidas por criterios empresariales válidos, sino por intereses personales y familiares. Con frecuencia, se genera una situación en la que se busca un beneficio a título individual que, a su vez, puede causar un perjuicio al Grupo.

Cuando los intereses personales y profesionales sean contrarios, se debe informar al Comité de Cumplimiento a través de los canales internos establecidos al efecto (Canal de Comunicación y Denuncias) para actuar de manera adecuada.

Estar ante un conflicto de interés no constituye una infracción del Código, pero no divulgar esta circunstancia y no consultar cómo actuar sí lo es.

Principios que se utilizan en la relación con los miembros de la Administración

El comportamiento de los integrantes del Grupo Correos con los miembros de las Administraciones públicas, tanto nacionales como extranjeras, ha de ser siempre transparente, ético e íntegro. Nunca podrán llevarse a cabo, en nombre del Grupo Correos, acciones que supongan la entrega, aceptación, conformidad u ofrecimiento de regalos, atenciones excesivas o comisiones ocultas, entre otras formas, ni a los miembros de las Administraciones públicas ni a personas estrechamente relacionadas con estos.

- No serán susceptibles de autorización las donaciones que puedan influir en algún caso o comprometer a la Administración Pública o cuyo objeto sea la obtención de una ventaja comercial ilícita.
- Quedan igualmente prohibidas las contribuciones a partidos políticos, independientemente de su signo u orientación. No se podrá hacer valer la relación personal o familiar con una autoridad o funcionario público, tanto nacional como extranjero, con independencia de las razones que la motivaron u originaron.

La relación con la sociedad es uno de los tres pilares en los que se basa el Plan de Sostenibilidad del Grupo Correos. Por ello, el Grupo se compromete a llevar a cabo su actividad de forma respetuosa con las comunidades donde opera y con la sociedad en general, respetando:

- La diversidad cultural.
- La diversidad de costumbres.

El Grupo Correos pretende hacer más fácil la vida de las personas y empresas, con independencia de donde se encuentren y a través de la capilaridad de nuestra red. Por ello, el Grupo se adapta a las diferencias de los territorios donde desarrolla su labor profesional, entendiendo las necesidades locales y adaptándose a estas para impactar de manera positiva en las comunidades donde se opera.

D) Responsabilidad con el medioambiente

La sostenibilidad, uno de los valores del Grupo, define el comportamiento también frente al medioambiente. Por ello, la actividad se desarrolla de manera responsable, asumiendo los siguientes compromisos con el entorno:

- Negocio e innovación responsable. Se persigue el desarrollo y comercialización de productos y servicios sostenibles para responder a las nuevas demandas de los clientes, como evidencian las reducciones de CO_2 o la compra de vehículos eléctricos.
- Gestión responsable. Se apuesta por el desarrollo de soluciones y productos con un impacto social y ambiental positivo, que sean eficientes y reduzcan los impactos en el medioambiente.

Todos los empleados deben tener un comportamiento responsable con el medioambiente, siendo cuidadosos con la naturaleza e impactando de forma positiva en esta.

Los objetivos del Plan General de Sostenibilidad son:

- Economía circular.
- Reducción de emisiones.
- Valor local.
- Movilidad sostenible.

E) Canal de Comunicación y Denuncias

El Canal de Comunicación y Denuncias pretende establecer un procedimiento de comunicación con el Comité de Cumplimiento del Grupo sobre conductas o hechos relacionados con actuaciones u omisiones presuntamente delictivas o no éticas.

¿Quién puede utilizarlo?:

- Todos los empleados del Grupo Correos.
- Terceros que mantengan relación comercial.
- Terceros que utilicen los servicios del Grupo Correos con alguna de las sociedades que lo integran.

Procedimiento de denuncia:

a) Comunicación y tramitación. La comunicación se efectuará:

  - Rellenando el formulario de denuncia que está disponible en las páginas web de cada empresa del Grupo.

- Adjuntando toda la documentación de la que se disponga y que sirva de soporte justificativo de la misma.

La persona comunicante debe comprometerse a:

- Emplear el canal de manera honesta, no utilizándolo para hacer daño a otros profesionales o defender sus intereses personales.
- Estar disponible para cooperar con el Comité de Cumplimiento durante todo el proceso de investigación de los hechos comunicados.

b) Tramitación de la comunicación. La comunicación se enviará al Comité de Cumplimiento a través de las siguientes vías, que permiten acusar recibo del envío:

- **Canal verbal:** el denunciante informa al superior jerárquico, quien informará al Área de Cumplimiento o al Comité de Cumplimiento.
- **Canal postal:** el denunciante informa a través de la dirección disponible para tal efecto.
- **Canal electrónico:** el denunciante informa a la dirección de correo electrónico habilitada para tal efecto.
- **Canal electrónico en la web corporativa:** el denunciante informa a través del canal electrónico implantado en las páginas webs de cada una de las sociedades del Grupo Correos.

c) **Información al comunicante.** La persona que comunique una actuación u omisión susceptible de implicar un riesgo de imputación penal a través de este canal será informada por el Comité de Cumplimiento del resultado de su comunicación.

d) **Derechos del denunciante.** El Grupo Correos garantiza al usuario la no existencia de represalias contra el denunciante por parte de los superiores jerárquicos o cualquier persona relacionada con los hechos alegados.

Las **claves** que marcan el **comportamiento ético** son:

1. **Cumplimiento ético y legal.** Todos los empleados están obligados a cumplir la legalidad vigente y lo establecido en el Código de Correos. También están obligadas a hacerlo las empresas que el Grupo subcontrate.
2. **Igualdad de trato y oportunidades.** El equipo de Correos respeta y promueve la igualdad de trato y de oportunidades de todas las personas, por lo que las decisiones de promoción solo pueden estar basadas en parámetros objetivos.
3. **Diversidad.** El Grupo Correos promueve la diversidad e inclusión en el entorno de trabajo, teniendo muy presentes los derechos humanos y las libertades fundamentales.
4. **Tolerancia cero.** No se tolera el acoso en el trabajo ni ningún tipo de conducta abusiva, hostil u ofensiva. Además, no se acepta la existencia de conflictos de intereses entre sus empleados, directivos o administradores.
5. **Compromiso social y medioambiental.** El Grupo se compromete a llevar a cabo su actividad de forma respetuosa con el entorno en el que opera y con la sociedad en general.

6. **Materiales y recursos de la empresa.** Los recursos de la empresa se utilizan de forma honesta, eficiente y responsable con el entorno. Una vez cese la actividad, se deben devolver en perfectas condiciones.
7. **No se aceptan ni se ofrecen regalos.** Se prohíbe la aceptación u ofrecimiento de ventajas o incentivos de carácter ilícito. Esto es especialmente importante cuando hablamos de miembros de las Administraciones públicas.
8. **Confidencialidad y privacidad de datos.** Los integrantes del Grupo tienen el deber de guardar secreto sobre información clasificada como privilegiada, confidencial, reservada o secreta, así como respetar los derechos de propiedad intelectual del Grupo y de terceros.
9. **Propiedad intelectual.** Las sociedades que conforman el Grupo Correos protegen sus derechos de propiedad industrial e intelectual y respetan los de terceros. Cuando se utilice este tipo de información, se han de adoptar medidas de diligencia y cuidado específicas.
10. **Informar sobre un problema ético.** Si se quiere reportar una actividad o un hecho, se puede hacerlo de forma anónima a través del Canal de Comunicación y Denuncias, que establece el procedimiento de comunicación con el Comité de Cumplimiento del Grupo.

El vigente Código de Conducta ha sido aprobado por el Consejo de Administración el 22 de julio del 2021. El Comité de Cumplimiento emite las normas de ejecución que sean necesarias para el desarrollo de lo preceptuado en el mismo y es el encargado de velar por su actualización permanente, adaptándolo a la realidad social y legal de cada momento.

El Comité de Cumplimiento revisa el Código de Conducta de Correos al menos una vez cada dos años y, en cualquier caso, cuando se producen modificaciones de las normativas externas o internas que afectan al mismo.

Programa de prevención de riesgos penales

Finalidad y ámbito de aplicación

El Programa de Prevención de Riesgos Penales describe los elementos del Sistema de Compliance de la Sociedad Estatal Correos y Telégrafos, S.A. y de sus sociedades filiales (en adelante, las sociedades y, conjuntamente, Correos), en relación con el régimen de responsabilidad penal de las personas jurídicas que establece el artículo 31 bis del Código Penal.

A) Objeto

Las sociedades integrantes de Correos son entidades mercantiles que se rigen por el ordenamiento jurídico privado, salvo en las materias que le sea de aplicación la normativa presupuestaria, contable, de control financiero y de contratación, en su condición de sociedad integrante del sector público empresarial.

Las sociedades integradas en Correos desarrollan las siguientes **actividades principales:**

- Correos y Telégrafos. La actividad principal de la matriz es la gestión y explotación de cualesquiera servicios postales, la prestación de los servicios financieros relacionados con los servicios postales y los servicios de giro. Asimismo, la sociedad tiene por objeto la recepción de las solicitudes, escritos y comunicaciones que los ciudadanos dirijan a los órganos de las Administraciones públicas, entrega de notificaciones administrativas y judiciales, servicios de telegrama y cualesquiera otros servicios relacionados con las telecomunicaciones.

  En cuanto a los **servicios postales,** ha de precisarse que estos abarcan, entre otros, los servicios previstos en la Ley 43/2010, de 30 de diciembre, del Servicio Postal Universal (SPU), de los derechos de los usuarios y del mercado postal, considerados de interés general. Son **actividades principales** las siguientes:

  – Las actividades de recogida, admisión, clasificación, transporte, distribución y entrega de envíos postales nacionales y transfronterizos en régimen ordinario de:

    - Cartas y tarjetas postales que contengan comunicaciones escritas en cualquier tipo de soporte de hasta dos kilogramos de peso.
    - Paquetes postales, con o sin valor comercial, de hasta veinte kilogramos de peso.

  – La prestación de los servicios de certificado y valor declarado, accesorios de los envíos contemplados en este apartado.
  – Cabe destacar asimismo los servicios de emisión de sellos y de los restantes sistemas de pagos de los servicios postales, incluyendo las actividades de comercialización y distribución de sus productos y emisiones. Las actividades desarrolladas por la sociedad pueden ser asimismo relativas a la prestación de servicios que las propias Administraciones públicas le encomienden.

- Correos y Telégrafos, además de las actividades que desarrollan el servicio postal, también se dedica, entre otras, a las siguientes:

  – Proceso electoral. Correos y Telégrafos colabora en el desarrollo de los procesos electorales, poniendo a disposición de los ciudadanos la documentación que les permita ejercitar este derecho, sirviendo de enlace con las Delegaciones Provinciales de la Oficina del Censo Electoral y las Juntas y Mesas Electorales.
  – Giros postales. La sociedad ofrece el giro postal, tato nacional como internacional, como servicio de envío de dinero. El giro, a tenor de lo expresado en la Ley 43/2010 en su Disposición Adicional Tercera, se trata de un Servicio Complementario de los Servicios Postales.
  – Productos y servicios basados en las nuevas tecnologías. Correos y Telégrafos ha desarrollado diferentes herramientas para la localización de oficinas y búsqueda de envíos (Correos Info), para el envío de tarjetas postales físicas desde smartphones (Correos eCard), entre otros.

  - Comercialización de productos y servicios de Telecor. La sociedad actúa como comercial de Telecor prestando servicios de comercialización de productos y servicios de dicha empresa, dedicada a la prestación y desarrollo de productos y servicios e ingeniería en telecomunicaciones, internet e informática.

- **Correos Express.** Sociedad dedicada al estudio, la investigación y la prestación de un servicio de transporte terrestre abarcando la recogida y el libramiento de documentos y paquetes y su envío y entrega, tanto en España como en el extranjero. Las actividades desarrolladas están dirigidas a una clientela de empresas. No obstante, accesoriamente se dirige también a profesionales y particulares así como, de forma general a todo tipo de transporte.
- **Nexea.** Compañía dedicada a ofrecer servicios personalizados en gestión documental, para las comunicaciones masivas de las empresas con sus clientes. Desarrolla soluciones tecnológicas a medida para los procesos documentales, mediante un modelo multicanal de comunicaciones, en todo tipo de soportes y formatos.
- **Correos Telecom.** Gestiona la red de telecomunicaciones, comercializa la capacidad excedentaria de dichas infraestructuras y proporciona el soporte tecnológico al resto de empresas de Correos.

Correos cuenta con procedimientos y controles para prevenir la realización, por parte de todos sus empleados y personas bajo su autoridad, de actos y conductas encuadrables como riesgos penales.

B) Alcance

El alcance del **Programa de Prevención de Riesgos Penales** del Grupo Correos **incluye** a:

- Los empleados, directivos y miembros del Consejo de Administración de cualquiera de las sociedades integrantes de Correos, así como aquellos terceros que actúen en su nombre y representación.
- Sociedades contratistas que carezcan de procedimientos internos o de códigos de conducta equivalentes a los implantados en Correos.

El documento estará disponible para todos los empleados y será notificado a todos los consejeros, altos directivos y a cualquier persona que represente a Correos o a cualquiera de las sociedades que lo integran, cuando así lo requiera la naturaleza de su relación.

Referencias

A lo largo del programa, se hará mención de los siguientes documentos:

- Código General de Conducta.
- Política de Compliance.
- Política Anticorrupción.
- Estatuto del Comité de Cumplimiento de Correos.
- Reglamento de Funcionamiento del Canal de Comunicación y Denuncias de Correos.

Responsabilidades

El Comité de Cumplimiento será responsable de la aprobación, revisión y actualización del presente programa.

Actualización del programa

El Comité de Cumplimiento revisará el programa anualmente a los fines de adaptarlo, en su caso, a los cambios normativos u organizativos que acontezcan en el seno de cualquiera de las sociedades de Correos, así como por cualquier incumplimiento que evidencie la falta de eficacia y necesaria corrección, de los controles del Sistema de Compliance.

Régimen de responsabilidad penal de las personas jurídicas de Correos

A) Contexto normativo

El presente documento de Prevención de Riesgos Penales es el resultado de los trabajos ejecutados en el seno del Sistema de Compliance que se han desarrollado en Correos para prevenir y detectar la comisión de delitos en el seno de su actividad.

Todo ello se ha realizado para cumplir con lo establecido en el artículo 31 bis del Código Penal que introduce la responsabilidad penal de las personas jurídicas. Dicha responsabilidad penal es aplicable a las sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, siempre y cuando se den las siguientes premisas:

- Los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que, actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.
- Los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquellos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

B) Adecuación UNE 19601

El 18 de mayo de 2017 la Asociación Española de Normalización publicó la norma española UNE 19601 de sistemas de gestión de compliance penal, que desarrolla requisitos con el fin de cumplir con las indicaciones del Código Penal sobre los modelos de gestión y prevención de delitos, incorporando buenas prácticas internacionalmente aceptadas en materia de compliance.

El presente programa se encuentra adaptado a los preceptos establecidos por la norma UNE 19601, elaborada por el Subcomité Técnico CTN 307 SC1 Sistemas de gestión del cumplimiento y sistemas de gestión anticorrupción, en lo relativo al cumplimiento en materia de informes de compliance penal, y contenido de los mismos, cumpliéndose con lo relativo a la información requerida para conocer el contexto de la organización.

C) Objeto del Programa y medidas de control adoptadas

Objeto del Programa de Prevención de Riesgos Penales

La Ley Orgánica 1/2015, de reforma del Código Penal introduce importantes cambios entre los que destacan el nuevo artículo 31 bis del Código Penal, que exime de responsabilidad penal a la persona jurídica en los casos de delitos cometidos por representantes y administradores cuando concurran las siguientes circunstancias:

a) El órgano de administración haya adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyan las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;
b) la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado haya sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;
c) los autores individuales hayan cometido el delito eludiendo fraudulentamente el Sistema de Compliance, y
d) no se haya producido una omisión o un ejercicio insuficiente de las funciones de supervisión, vigilancia y control por parte del órgano de control.

Asimismo, el artículo 31.bis.4 establece que la persona jurídica estará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.

La Ley Orgánica 1/2015, establece que, para que el Sistema de Compliance sea eficaz para la mitigación de riesgos penales:

e) Se identifiquen las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.
f) Se establezcan protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquellos.
g) Se disponga de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.
h) Se imponga la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

i) Se establezca un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el Sistema de Compliance.
j) Se proceda a una verificación periódica del Sistema de Compliance y a su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

Adicionalmente, el artículo 31.1 *quáter* del Código Penal contempla como atenuante de la responsabilidad de la persona jurídica, entre otras, «haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica».

Como recoge la Circular 1/2016 de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas, se trata de: «Naturalmente, promover que las personas jurídicas se estructuren dotándose de sistemas organizativos y de control que, entre otras cosas, tiendan a evitar la comisión de delitos en su seno o, al menos, lograr su descubrimiento constituye un objetivo loable y merece una valoración positiva».

El régimen de responsabilidad de la persona jurídica ha sido completado por la Ley Orgánica 1/2019, de 20 de febrero, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para transponer Directivas de la Unión Europea en los ámbitos financiero y de terrorismo, y abordar cuestiones de índole internacional. Esta reforma introdujo cambios en alguno de los delitos imputables a las personas jurídicas.

Por lo tanto, los **objetivos últimos del presente Programa** son: (i) asegurar la efectividad de unas normas y procedimientos de control que minimicen el riesgo de comportamientos ilícitos por parte de los Consejos de Administración, directivos, mandos intermedios, empleados y colaboradores de Correos o de cualquiera de sus sociedades, y (ii) acreditar que esta ha ejercido el control debido sobre su actividad empresarial, cumpliendo de este modo con la exigencia contemplada en el Código Penal.

A tal fin, se ha delimitado en el presente Programa de Prevención de Riesgos Penales el **Sistema de Compliance** adoptado por Correos, y **definido en:**

a) Parte General. Incluye el diseño y estructura del (i) modelo de supervisión, seguimiento y verificación, (ii) órgano de control, (iii) sistema de gestión de recursos financieros y materiales, (iv) sistema disciplinario, (v) canal de comunicación y denuncias, (vi) formación, y (vii) controles generales con los que cuentan Correos y sus Filiales para prevenir la comisión de delitos.
b) Parte Especial. Identifica los riesgos penales que pueden hipotéticamente producirse en Correos y en sus filiales debido a las actividades que este realiza, de forma que dichos riesgos se detallan en anexos junto con el marco de control susceptible de mitigarlos.

El Programa tiene un carácter dinámico, por lo que se revisará su ámbito periódicamente en relación con los riesgos penales que pueden afectar a Correos y a cada una de las sociedades y, en su caso, será objeto de actualización.

Objetivos del Programa

El objetivo del Programa es describir los controles generales del Sistema de Compliance implantado en Correos, las políticas, pautas de actuación y comportamientos que regulan su actividad, así como el marco de control para prevenir la comisión de los delitos en el seno de su actividad.

A tal fin, los objetivos fundamentales del Programa son los siguientes:

- Optimizar y facilitar la mejora continua del Sistema de Compliance.
- Establecer un sistema estructurado y orgánico de prevención y control dirigido a la reducción del riesgo de comisión de delitos.
- Hacer seguimiento del cumplimiento del Sistema de Compliance, de los principios éticos y de la normativa interna de Correos.
- Informar a consejeros, directivos y empleados de Correos de que una infracción de las disposiciones contenidas en él implica la imposición de medidas disciplinarias a los empleados y la posible extinción de la relación de negocios existente al resto de grupos de interés que actúan en nombre, por cuenta, o de algún modo, en el interés de Correos.
- Dejar constancia expresa y pública de la condena tajante de Correos a cualquier tipo de comportamiento ilegal, destacando que, además de contravenir las disposiciones legales, es contrario a los principios éticos, que se configuran como valores clave de Correos para conseguir sus objetivos empresariales.
- Adecuar las medidas de control existentes a los procesos, de manera que permitan a Correos prevenir la comisión de estos delitos, así como, en caso de que se produjera la comisión de un delito (pese a los controles establecidos), intervenir de forma inmediata.
- Sensibilizar y formar a todos los profesionales de Correos sobre la importancia del cumplimiento normativo y, en especial, sobre la prevención de riesgos penales.
- Vigilar especialmente los controles implantados en las operaciones o procesos susceptibles de generar riesgos penales.
- Supervisar el funcionamiento del Sistema de Compliance implantado y del Programa, con su consecuente actualización periódica, ya sea por cambios organizativos dentro de Correos o de cualquiera de sus filiales o como consecuencia de modificaciones en la legislación vigente.

D) Adopción del Programa de Prevención de Riesgos Penales por parte de Correos

Ámbito de aplicación del Programa

El Programa cubre el análisis de los (i) posibles riesgos penales que pueden afectar a Correos y a las sociedades que lo integran, tanto como consecuencia de la actividad desarrollada en territorio español como fuera de dicho territorio cuando los tribunales españoles fueran competentes, así como de los (ii) controles mitigantes de tales riesgos.

Dicho documento deberá revisarse de conformidad con los cambios externos o internos que se puedan producir y que tengan impacto en el mismo. A estos efectos, cuando se

produzca su revisión, se incorporarán en el presente apartado los aspectos que se consideren necesarios.

Destinatarios del Programa: personas sujetas

El Programa de Prevención de Riesgos Penales es de aplicación, de acuerdo con la voluntad de Correos y conforme lo previsto en el Código Penal, a todos los directivos, mandos intermedios y empleados de Correos y Telégrafos y de las sociedades filiales y a aquellos que actúen en nombre o por cuenta de Correos y en su provecho, así como sus representantes legales, administradores de hecho o de derecho o personas con capacidad de decisión o con facultades de organización o control.

Adicionalmente, es aplicable a las empresas y profesionales a los que Correos pueda subcontratar, siempre que la actividad subcontratada sea sensible o relevante para sus actividades. En este sentido, se les requerirá a las empresas subcontratistas, en los respectivos contratos, que manifiesten que han adoptado medidas oportunas en el ámbito de la prevención de riesgos penales.

Es decir, el Sistema de Compliance tendrá siempre en cuenta a las partes interesadas:

- Administradores, alta dirección y empleados. Los principios y valores de la organización han de ser asumidos por el órgano de gobierno y el equipo directivo, de manera que, para garantizar la eficacia del Sistema de Compliance, el Comité de Cumplimiento debe contar con el apoyo explícito y evidente del órgano de gobierno y del equipo directivo, a través de la aplicación de los principios y políticas internas. Así serán trasladados al resto de empleados que estarán implicados en la aplicación de los protocolos, controles y tareas.
- Clientes. Además de un servicio de calidad, es necesario que el Sistema de Compliance se muestre eficaz, de forma que prevenga de consecuencias jurídicas o de escándalos reputacionales. Se ha observado en los últimos tiempos que muchas terceras partes, incluidos clientes, solicitan como parte de su *due diligence* contar con un modelo de cumplimiento.
- Entidades financieras. Es necesario que el Sistema de Compliance se muestre eficaz, de forma que prevenga de consecuencias jurídicas o de escándalos reputacionales, especialmente dirigidos a garantizar la imagen de solvencia de Correos y capacidad de atender las obligaciones con las entidades financieras y terceros.
- Proveedores. Los proveedores deben mostrar el mismo compromiso con el cumplimiento normativo, de manera que las alianzas estratégicas se puedan mantener bajo control en la selección y homologación de proveedores, y ofrezcan garantías.
- Administraciones públicas. Son cada vez más las administraciones que exigen contar con modelos de cumplimiento para poder contratar con ellas. Por ello, y dada la exigencia de la SEPI, es necesario que las relaciones con Administraciones públicas se lleven a cabo con total transparencia y a través de los mecanismos establecidos en el Sistema de Compliance.

Glosario

SEPI: Sociedad Estatal de participaciones Industriales.

Elementos del Sistema de Compliance

El programa se estructura principalmente en una parte general y una parte especial, como se ha esquematizado anteriormente, que recogen el marco de control adoptado por Correos en relación con los riesgos identificados en función de las actividades desarrolladas para cada una de las Sociedades que lo integran.

A) Políticas, procedimientos y controles generales

El Sistema de Compliance de Correos estructura la prevención de riesgos penales a través de:

- Controles Generales, que se constituyen como la base del control del riesgo y tienen eficacia para mitigar el riesgo genérico de comisión de delitos.
- Controles Específicos, constituidos por medidas concretas cuya finalidad es mitigar un riesgo penal específico o un grupo de riesgos penales concretos, que se corresponden con los controles de procesos específicos.

Los controles sobre los que se articula el Programa permiten que el Sistema de Compliance de Correos sea un sistema estructurado y orgánico de prevención y control eficaz para la reducción del riesgo de comisión de los delitos relacionados con sus actividades.

Por consiguiente, el Sistema de Compliance de Correos se estructura sobre las Políticas, Procedimientos y Controles Generales que se detallan a continuación:

- **Organigrama.** Correos y cada una de las sociedades que lo componen disponen de un documento en el que se define e identifica cada una de las direcciones, subdirecciones, departamentos, así como los procesos de negocio de Correos y la definición de las funciones de los mismos.
- **Funciones y responsabilidades.** Correos ha desarrollado un proceso de control de otorgamiento de poderes, segregación y funciones y niveles de autorización.
- **Código General de Conducta.** Correos ha aprobado un Código General de Conducta que sirve de guía para la actuación de los empleados de cada una de sus sociedades en el desempeño de su actividad.
- **Canal de Comunicación y Denuncias.** Correos dispone de un procedimiento relativo al Canal de Comunicación y Denuncias como instrumento para elevar cualquier posible irregularidad, incumplimiento o comportamiento contrario a la ética, la legalidad y las normas que rigen en Correos.
- **Plan de Formación y Comunicación.** Correos ha desarrollado un Plan de Formación y Comunicación anual que contiene las distintas formaciones a impartir en Correos en materia de compliance y materias relacionadas con los riesgos específicos de cada área.
- **Pack de Bienvenida.** Correos ha creado un Pack de Bienvenida para las nuevas incorporaciones que incluye todos aquellos documentos esenciales que deben ser conocidos por los nuevos integrantes de Correos.

- **Normas sobre uso de dispositivos tecnológicos.** Correos ha desarrollado normas que establecen los principios básicos de actuación en el uso de aquellos dispositivos que Correos pone a disposición de sus integrantes.
- **Sistema disciplinario.** Establece el régimen sancionador previsto en los convenios colectivos de aplicación para empleados y en normativa de aplicación a la alta dirección y contrataciones mercantiles aplicables a las sociedades de Correos.
- **Procedimiento para el seguimiento en el cumplimiento por empresa subcontratada de los procedimientos y políticas internos.** Describe el seguimiento del correcto cumplimiento de los procedimientos y políticas por las empresas o sociedades con las que subcontrate Correos la prestación de servicios o la ejecución de algún trabajo.

B) Gestión de recursos financieros

Controles en el ámbito de gestión presupuestaria y tesorería

Correos cuenta con controles financieros con las siguientes características fundamentales:

- Controles que asignan las tareas de gestión económica-financiera, así como el control financiero, de tesorería y contable en Correos con designación de funciones, otorgamiento de poderes, certificados de representantes de persona jurídica y delegación de funciones.
- Correos realiza auditorías de los estados financieros.
- El Comité de Cumplimiento será dotado anualmente de un presupuesto para el ejercicio de sus funciones en relación con la supervisión, seguimiento y actualización del Sistema de Compliance.

Los referidos sistemas de control y gestión resultan, asimismo, de utilidad para asegurar una adecuada gestión de los recursos financieros en los términos exigidos por el Código Penal, todo ello en la medida en que los mismos garantizan el mantenimiento de los libros, registros y cuentas de manera precisa, así como un sistema apropiado de contabilidad interna, y de control en el ámbito financiero.

Recursos financieros y materiales

El Comité de Cumplimiento deberá contar con los pertinentes recursos financieros necesarios para un correcto y eficaz funcionamiento del Sistema de Compliance, tal y como se describe a lo largo del manual.

Correos dota anualmente al Comité de Cumplimiento para la prevención de riesgos penales, de una partida o dotación económica específica para el correcto y eficaz cumplimiento del Sistema de Compliance:

- Recursos económicos que permitan el desarrollo de las funciones atribuidas al Comité de Cumplimiento.
- Recursos humanos del Área de Cumplimiento que permitan obtener información de todas las áreas de actividad de Correos, así como implantar, supervisar y actualizar el Sistema de Compliance de Correos.

- Recursos tecnológicos que ayuden a cumplir con la normativa de prevención de riesgos penales (control de permisos por usuario, control de accesos a archivos, carpetas, webs, etc.).

C) Seguimiento, cumplimiento y suficiencia del Programa: Comité de Cumplimiento

El ejercicio del control debido exigido por el Código Penal requiere la implantación en Correos de mecanismos de control continuo, así como la designación de órganos de control interno para el seguimiento de los eventuales riesgos penales y de las medidas implantadas para su mitigación.

Atendiendo a los requerimientos del Código Penal, Correos va a tener definida una estructura de control constituida por (i) el Consejo de Administración, como máximo órgano de decisión; (ii) el Comité de Cumplimiento como órgano de vigilancia y control, con las responsabilidades de implantación y ejecución de las políticas y controles de prevención de delitos (con apoyo en el equipo del Área de Cumplimiento) y (iii) los Responsables de los Controles.

La ejecución de las tareas de control y seguimiento se encomendarán en Correos al Comité de Cumplimiento, como órgano nombrado por el Consejo de Administración de Correos y Telégrafos, por disponer de autonomía e independencia en términos tanto de poder de control como de la iniciativa necesaria en el presente marco de control.

El Comité de Cumplimiento se servirá del Área de Cumplimiento para realizar las actividades diarias de revisión y otras funciones definidas en la Política de Compliance y en el Estatuto del Comité de Cumplimiento implantadas en Correos.

Gobierno corporativo

Correos se encuentra participado en su totalidad por la Sociedad Estatal de Participaciones Industriales (SEPI) en la que quedó integrada en junio de 2012.

La forma de gobierno de Correos y Telégrafos es el Consejo de Administración, cuyo funcionamiento se encuentra reglado, a los fines de determinar los principios de actuación y las reglas básicas de organización y funcionamiento, así como las normas de conducta de sus miembros y las funciones de supervisión y control que tengan encomendadas.

La administración de la Sociedad Estatal corresponde al Consejo de Administración, a su presidente y a la Comisión Ejecutiva.

Correos y Telégrafos se estructura a través de departamentos definidos y encabezados por el Consejo de Administración.

Los principales departamentos son: (i) Secretaría General y del Consejo de Administración; (ii) Relaciones Institucionales y Coordinación; (iii) Auditoría e Inspección; (iv) Comunicación; (v) Operaciones; (vi) Comercial y Marketing; (vii) Planificación y Finanzas; (viii) Recursos Humanos; (ix) Estrategia y Desarrollo de Negocio, y (x) Tecnología y Sistemas.

A continuación, se describen los órganos implicados en implantación, supervisión y actualización del Sistema de Compliance y las funciones que les corresponden, sin perjuicio de su desarrollo en el Estatuto del Comité de Cumplimiento de Correos.

Consejo de Administración de Correos y Telégrafos

El Consejo de Administración de Correos y Telégrafos es el máximo órgano de decisión y representación de la Sociedad. El presidente del Consejo de Administración es asimismo el presidente Ejecutivo de Correos y de todos sus órganos de gobierno y administración y es el responsable de las funciones de dirección, gestión y administración, de representación de dichos órganos, así como de la ejecución de los acuerdos que estos adopten.

El Consejo de Administración es, también, el responsable de vigilar la gestión del riesgo de cumplimiento de Correos, así como de aprobar todas aquellas políticas de Correos destinadas a identificar, evaluar, seguir, notificar y asesorar sobre riesgos de cumplimiento. En concreto, debe asegurarse de la debida implantación del Sistema de Compliance de Correos a través del nombramiento del Comité de Cumplimiento que llevó a cabo con fecha 27 de noviembre de 2014.

El Consejo de Administración deberá ser informado por el Comité de Cumplimiento de conformidad con lo previsto en el Estatuto del Comité de Cumplimiento, al menos semestralmente, sobre:

- Las necesidades económicas, humanas y materiales para el desempeño de las obligaciones de cumplimiento, a la vista de los dictámenes internos de conclusiones que se emitan.
- El estado de la implantación, supervisión y actualización del Sistema de Compliance.
- Las necesidades derivadas del Plan de Comunicación y Formación.
- Los resultados de las auditorías de compliance realizadas sobre la eficacia de los procedimientos de control del Sistema de Compliance.
- Las consultas, denuncias y comunicaciones recibidas a través del Canal de Comunicación y Denuncias de Correos.
- Los requerimientos de información o inspecciones realizadas a cualquiera de las sociedades de Correos.
- El resultado de los dictámenes sobre solicitudes de donaciones, colaboraciones o patrocinio.

En todo caso, el Consejo de Administración será informado de cualquier incumplimiento o noticia que pueda afectar a los intereses de Correos o que se considere relevante a efectos reputacionales.

Órganos de gobierno de las filiales

Corresponde a los órganos de gobierno de las diferentes sociedades integrantes de Correos nombrar al Comité de Cumplimiento de Correos como encargado de la llevanza, actualización y gestión del Sistema de Compliance.

Los órganos de administración de las filiales deberán ser igualmente informados de manera periódica, al menos semestralmente, de los resultados de las actividades llevadas a cabo por el Comité de Cumplimiento, así como del estado del Sistema de Compliance. También serán informados de cualquier incumplimiento o noticia que pueda afectar a los intereses de la filial concreta o que se considere relevante a efectos reputacionales por el Comité de Cumplimiento.

Comisión ejecutiva

La Comisión Ejecutiva está compuesta por el presidente y cuatro miembros del Consejo de Administración. Puede ejercitar todas y cada una de las facultades del Consejo de Administración, salvo las que resultan indelegables por Ley.

Comisión de Auditoría y Control

La Comisión de Auditoría y Control es un órgano dependiente del Consejo de Administración, constituido de conformidad con lo previsto en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Publicas. Está integrada por tres consejeros sin funciones ejecutivas elegidos por el Consejo de Administración de entre sus miembros.

La Comisión de Auditoría y Control deberá ser informada, con una periodicidad mínima semestral, del contenido y resultado de los dictámenes de conclusiones emitidos por el Comité de Cumplimiento, así como del estado de la revisión y actualización del Sistema de Compliance, de forma previa a reportar al Consejo de Administración.

Igualmente, será informada de cualquier incumplimiento o noticia que pueda afectar a los intereses de Correos o que se considere relevante a efectos reputacionales.

Comité de Cumplimiento

Correos ha implantado el Sistema de Compliance mediante la adopción de las necesarias medidas de vigilancia, supervisión y control para prevenir riesgos penales que pudieran cometerse en el seno de su actividad.

Para su implantación, supervisión y actualización, se ha constituido el Comité de Cumplimiento como órgano colegiado autónomo de vigilancia y control.

Habida cuenta las dimensiones de Correos y las características del cargo, sin perjuicio de la delegación de funciones en personal propio o externo, el nombramiento de los miembros de dicho Comité habrá de recaer en personas con titulación superior, de integridad y compromiso reconocido, conocimiento de la normativa externa e interna de aplicación a Correos, conocimiento del negocio, experiencia en gestión de riesgos, suficiente autoridad y ausencia de conflictos de interés.

En la actualidad, la composición del Comité de Cumplimiento es la siguiente:

- La Vicesecretaría General, que ostentará la Presidencia.
- Subdirección de Gestión, Organización y Desarrollo de Personas.

- Subdirección de Control y Estadística.
- Subdirección de Relaciones Internacionales y Sostenibilidad.

El Comité se reunirá en sesiones ordinarias, con una periodicidad mínima trimestral, con carácter general, pudiendo celebrar reuniones extraordinarias cuantas veces sea necesario o lo solicite cualquiera de sus miembros a consideración de su presidente, incluso de manera telemática siempre que quede constancia de su celebración.

La convocatoria se hará por el secretario del Comité de Cumplimiento a solicitud del presidente, indicando lugar de celebración y orden del día. El Comité quedará válidamente constituido con la presencia del presidente y, al menos, dos miembros del Comité más el secretario y los acuerdos se adoptarán por mayoría absoluta de sus miembros.

Igualmente, de manera semestral, el Comité de Cumplimiento reportará al Consejo de Administración de Correos y Telégrafos.

El Comité de Cumplimiento llevará a cabo las funciones recogidas en el Estatuto del Comité de Cumplimiento de Correos, con apoyo en el Área de Cumplimiento, que tiene delegada la gestión diaria de las funciones relativas a la supervisión del Sistema de Compliance, de vigilancia asociada a controles y de actualización de las medidas de prevención de delitos.

El Área de Cumplimiento está formada por la Secretaría del Comité de Cumplimiento y su equipo y se reúne de manera periódica para tratar las funciones que le han sido encomendadas.

El Área de Cumplimiento reportará al Comité de Cumplimiento de manera periódica (como mínimo trimestral) sobre el estado y resultado de la supervisión para su conocimiento, toma de decisiones y posterior reporte al Consejo de Administración, todo ello sin perjuicio de las comunicaciones continúas del Área de Cumplimiento con la Presidencia del Comité de Cumplimiento.

Responsables de los controles

Los responsables de los Controles son aquellas personas designadas como responsables de controles dentro de cada una de las áreas (direcciones o subdirecciones) de Correos que, por su posición en la misma, están en condiciones de poder llevar a cabo una supervisión y control de los riesgos y las acciones u omisiones de las personas de su departamento o área, que podían resultar en la comisión de un delito. Su implicación ha de permitir mitigar la posible comisión de los delitos por los cuales Correos o cualquiera de sus sociedades filiales pudiera ser penalmente responsable.

El Comité de Cumplimiento, a través del Área de Cumplimiento, establecerá y mantendrá los procedimientos adecuados para que los Responsables de los Controles:

- Conozcan los riesgos penales y eventos de riesgo dentro del área bajo su responsabilidad que puedan afectar al Sistema de Compliance de Correos.

- Validen las políticas y procedimientos que les aplican.
- Supervisen los controles diseñados para gestionar o mitigar los riesgos.

Para proceder a la validación anual de los controles mitigadores de los riesgos relativos a cada una de las áreas de Correos, los Responsables de los Controles deberán comunicar y remitir evidencias por las que se acredita la eficiencia de los mismos, además del cumplimiento de las políticas y procedimientos estipulados por Correos.

Resto de la organización

Toda la organización de Correos es responsable de la ejecución del Sistema de Compliance. Los riesgos penales y de cumplimiento afectan a todas las personas de la organización y, por tanto, son responsabilidad individual de cada una de ellas.

D) Supervisión y seguimiento del Sistema de Compliance

El principal objetivo de la supervisión, seguimiento y verificación del Sistema de Compliance es validar de forma continua su implementación, permitiendo comprobar periódicamente la eficacia de las políticas, procedimientos y controles existentes, así como la evolución de los mismos, para tomar las acciones correctivas necesarias.

Correos es consciente de que la supervisión, seguimiento y verificación son elementos esenciales para que el Sistema de Compliance sea eficaz en aras de evitar la comisión de delitos, y por ello ha diseñado su modelo con base en la gestión del riesgo, implicando a distintas áreas en la certificación de los procesos y controles.

Dicha supervisión es responsabilidad del Comité de Cumplimiento, en colaboración con el Área de Cumplimiento y las propias áreas responsables de los controles.

Los objetivos que deben regir dicha supervisión son: (i) comprobar la efectividad de las normas y procedimientos de control establecidos por Correos para minimizar el riesgo de comportamientos ilícitos por parte de los profesionales, y (ii) acreditar que Correos ha ejercido el control debido sobre su actividad empresarial, cumpliendo de este modo con la exigencia contemplada en el Código Penal.

Estructura del modelo de supervisión, seguimiento y verificación

La función de seguimiento, supervisión y verificación de los riesgos penales de Correos se articula según el siguiente organigrama:

El proceso de supervisión y seguimiento

El proceso de supervisión y seguimiento del Sistema de Compliance debe ser evaluado con una periodicidad mínima anual por el Comité de Cumplimiento, a través del Área de Cumplimiento, para asegurar su conveniencia, adecuación y eficacia.

Será necesario establecer un proceso de evaluación sobre el cumplimiento de los controles de prevención de los riesgos penales. El responsable/evaluador del control que mitiga el evento de riesgo debe asegurar que el control se ha realizado durante el periodo señalado de acuerdo con su descripción, por personal con autoridad y competencia suficiente para asegurar su efectividad, y de que se han guardado las evidencias necesarias que así lo prueban.

Seguimiento. El seguimiento del sistema comprende especialmente las modificaciones necesarias cuando se pongan de manifiesto infracciones relevantes o deficiencias de diseño de sus disposiciones, cuando se produzcan cambios en la organización, en la estructura de control, en la actividad desarrollada, o incluso modificaciones legislativas que hagan necesarias adaptaciones en orden a asegurar su correcto funcionamiento.

E) Notificaciones y análisis de incumplimientos o vulneraciones de las conductas (Canal de Comunicación y Denuncias)

El empleado o tercero que tuviere indicios o sospechas de comportamiento contrario a la legalidad o que pueda implicar la materialización de un riesgo de carácter penal debe ponerlo inmediatamente en conocimiento, a través del Canal de Comunicación y Denuncias.

En todo caso, se asegura la máxima confidencialidad acerca de la identidad de la persona que notifica, salvo cuando haya de ser identificado ante las autoridades de acuerdo con lo establecido en las leyes.

Queda rigurosamente prohibido tomar represalias contra cualquiera que de buena fe (i) ponga en conocimiento de la empresa una posible vulneración del Código General de Conducta, (ii) advierta de un posible comportamiento contrario a legalidad o, en su caso, que pueda implicar la materialización de un riesgo penal, (iii) colabore en su investigación o ayude a resolverla. No obstante, esta garantía no alcanza a quienes actúen de mala fe con ánimo de difundir información falsa o de perjudicar a las personas.

El Comité de Cumplimiento será responsable de tramitar, investigar y resolver las denuncias recibidas a través del Canal de Comunicación y Denuncias.

Su funcionamiento se regula en el Reglamento de Funcionamiento del Canal de Comunicación y Denuncias: mecanismo habilitado a los empleados para que puedan comunicar los posibles incumplimientos normativos de cualquier miembro de la organización, así como realizar consultas sobre la licitud o no de una conducta.

F) Sistema disciplinario

El Sistema disciplinario establecerá el Régimen Sancionador de Correos consistente en las acciones correctoras o medidas disciplinarias ante incumplimientos de las políticas, procedimientos y pautas de actuación que componen el Sistema de Compliance de conformidad con la normativa laboral vigente, el Estatuto Básico del Empleado Público, Estatuto de los Trabajadores y Convenios Colectivos de aplicación.

De igual forma, los incumplimientos de procedimientos internos se regirán por lo previsto en la normativa de aplicación en el caso de relaciones laborales de carácter especial, personal de alta dirección o relaciones mercantiles, todo lo anterior sin perjuicio de las sanciones administrativas o penales que en su caso pudieran resultar de ello.

En ningún caso se podrá justificar la comisión de un delito para la obtención de un beneficio para Correos. Desde Correos se rechaza cualquier beneficio directo o indirecto que pueda percibirse como consecuencia de una actuación delictiva de cualquiera de sus profesionales.

G) Difusión y formación

La implantación de las medidas de control recogidas en este manual debe ir acompañada de la difusión adecuada del mismo y de su explicación a los profesionales de Correos. Se enfatiza la importancia de su cumplimiento y la asunción por parte de Correos de principios de actuación tendentes a evitar la comisión de ilícitos.

A tal efecto, Correos pretende adoptar las siguientes medidas de difusión y formación:

- Inclusión de material formativo en materia de prevención de riesgos penales en el Pack de Bienvenida a recibir por todo nuevo empleado *(Welcome Pack)*.
- Elaboración de un Plan de Formación y Comunicación anual en el que se introduzca la formación y la comunicación de los controles, políticas y procedimientos contenidos en el Sistema de Compliance a los profesionales de Correos.
- Impartición de formación en materia de prevención de riesgos penales a todos los profesionales de Correos.

La asistencia a los cursos de formación en materia de prevención de riesgos penales es obligatoria, debiendo dejar los profesionales constancia por escrito de su asistencia y evaluación de los conocimientos adquiridos sobre los contenidos formativos, cuando así sean requeridos.

H) Archivo y documentación

El Sistema de Compliance genera evidencias en su implantación, seguimiento y supervisión que permiten acreditar que dicho sistema está en funcionamiento y en un proceso de mejora continua. En consecuencia, Correos identifica, estandariza y garantiza la custodia de las evidencias clave que muestran la aplicación de los controles diseñados.

Aprobación del Programa de Prevención de Riesgos Penales

El Programa ha sido aprobado por el Consejo de Administración de Correos y Telégrafos el 22 de julio del 2021.

El Comité de Cumplimiento, como órgano de vigilancia y control, podrá proponer al Consejo de Administración modificaciones al mismo con la finalidad de mantener en todo momento un debido control de los elementos del Sistema de Compliance de Correos que permita minimizar la comisión de delitos.

Prevención de Riesgos Penales: Comité de Cumplimiento. Aspectos clave

El Comité de Cumplimiento es un órgano autónomo y colegiado encargado de velar por el cumplimiento del Sistema de Compliance de Correos.

A) Nombramiento de los miembros del Comité de Cumplimiento

El Comité de Cumplimiento es un órgano colegiado cuyos miembros serán nombrados directamente por el Consejo de Administración.

El nombramiento de sus miembros recaerá en personas con titulación superior, de integridad y compromiso reconocido, conocimiento de la normativa externa e interna de aplicación a Correos, conocimiento del negocio, experiencia en gestión de riesgos, suficiente autoridad y ausencia de conflictos de interés con el cargo.

Tendrá la consideración de secretario del Comité de Cumplimiento un licenciado en Derecho designado por la Secretaría General y el Consejo de Administración, con voz y sin voto.

En la actualidad la composición del Comité de Cumplimiento es la siguiente:

- La Vicesecretaría General, que ostentará la Presidencia.
- Subdirección de Gestión, Organización y Desarrollo de Personas.
- Subdirección de Control y Estadística.
- Subdirección de Relaciones Internacionales y Sostenibilidad.

En caso de vacante, ausencia o enfermedad de cualquiera de los miembros del Comité de Cumplimiento, el Consejo de Administración lo sustituirá en el plazo de dos semanas, con otro nombramiento que reúna las condiciones ya expuestas, y de quien quede acreditada la absoluta ausencia de conflicto de interés con el cargo.

En caso de vacante, ausencia o enfermedad del presidente del Comité, actuará como presidente en funciones el subdirector de Relaciones Institucionales y Transparencia y, en su defecto, el miembro del Comité más antiguo en Correos.

En tal caso, el puesto ocupado en el Comité de Cumplimiento por el subdirector de Relaciones Institucionales y Transparencia, o, en su defecto, el miembro del Comité más antiguo

en Correos y Telégrafos será sustituido durante la vacante, ausencia o enfermedad del presidente por el subdirector de Asuntos Jurídicos Contenciosos y, en su defecto, por el de Asuntos Jurídicos Consultivos.

Además, podrán asistir al Comité representantes de las Direcciones de Planificación y Finanzas, Relaciones Institucionales y Coordinación, Comunicación, Tecnología y Sistemas, Comercial y Marketing, de Operaciones, y de Estrategia y Desarrollo de Negocio de la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E., así como de las direcciones generales de las filiales de Correos, cuando el orden de los asuntos a tratar así lo requiera.

B) Compromiso y deberes del Comité de Cumplimiento

El Comité de Cumplimiento actuará siempre de conformidad con las siguientes características:

a) Autonomía e independencia en su actuación y en su toma de decisiones.
b) Dispondrá de un presupuesto suficiente para el desarrollo de sus funciones con la debida solvencia y estabilidad económica.
c) Mantendrá siempre la más absoluta confidencialidad en el desarrollo de sus funciones, absteniéndose de revelar a terceros la información obtenida en el ejercicio del cargo.
d) Sus miembros contarán con amplia experiencia en las diferentes áreas de Correos.
e) El Comité de Cumplimiento podrá contar con el asesoramiento externo de expertos cuando lo estime necesario.
f) El Comité de Cumplimiento conocerá las denuncias que se efectúen sobre presuntos comportamientos inadecuados en el seno de cualesquiera sociedades de Correos que pudieran generar un riesgo de imputación, tanto para las sociedades de Correos como para cualquiera de sus empleados.
g) El Comité de Cumplimiento será competente para conocer las comunicaciones de las que se desprenda que alguna de las sociedades de Correos o de sus empleados se encuentren incursos en procedimiento judicial penal con motivo de hechos relacionados con las funciones desarrolladas en las distintas líneas de actividad.
h) El Comité de Cumplimiento será competente para conocer los requerimientos de documentación o información por órganos judiciales, Ministerio Fiscal o de las Fuerzas y Cuerpos de Seguridad del Estado sobre la existencia de un procedimiento judicial penal, por hechos relacionados con las funciones desarrolladas en las distintas líneas de actividad de cualquiera de las sociedades o de su personal.
i) El Comité de Cumplimiento será competente para conocer las solicitudes de informes realizadas por cualquiera de las áreas de actividad de Correos acerca de la conformidad a derecho, o no, de comportamientos llevados a cabo en nombre y por cuenta de cualquiera de las sociedades de Correos, y en provecho de ellas.

C) Causas de recusación de los miembros del Comité de Cumplimiento

Los miembros del Comité de Cumplimiento deberán abstenerse y, en su defecto, podrán ser recusados por las siguientes causas:

a) Tener relación de parentesco con alguna de las partes involucradas en los procedimientos de investigación internos.
b) Estar casado o mantener una relación de afectividad, aun sin convivencia, con alguna de las partes involucradas en los hechos que vayan a ser investigados.
c) Ser parte en los hechos investigados.
d) Tener la condición de superior inmediato en la cadena de mando en la unidad o departamento en que hayan tenido lugar los hechos que vayan a ser investigados.
e) Tener una relación notoria de amistad o enemistad con alguna de las personas involucradas en los hechos que vayan a ser investigados.
f) Haber sido sancionado con motivo de un proceso de investigación interno por hechos de posible trascendencia penal.
g) Haber sido sancionado con motivo de una conducta de acoso laboral.
h) Haber sido condenado por sentencia firme por la comisión de un delito.
i) Presentar claro conflicto de interés con los asuntos resueltos de forma habitual por el Comité de Cumplimiento.
j) Haber incumplido los procedimientos internos que dictan sus pautas de comportamiento.

D) Funcionamiento interno del Comité de Cumplimiento

El Comité se reunirá en sesiones ordinarias, con una periodicidad mínima trimestral, con carácter general, pudiendo celebrar reuniones extraordinarias cuantas veces sea necesario o lo solicite cualquiera de sus miembros a consideración de su presidente, incluso de manera telemática siempre que quede constancia de su celebración.

La convocatoria se hará por el secretario del Comité de Cumplimiento a solicitud del presidente, indicando lugar de celebración y orden del día. El Comité quedará válidamente constituido con la presencia del presidente y, al menos, dos miembros del Comité más el secretario, y los acuerdos se adoptarán por mayoría absoluta de sus miembros.

De manera semestral, el Comité de Cumplimiento reportará al Consejo de Administración de Correos y Telégrafos sobre:

- Las necesidades económicas, humanas y materiales para el desempeño de las obligaciones de cumplimiento, a la vista de los dictámenes internos de conclusiones que se emitan.
- El estado de la supervisión y actualización del Sistema de Compliance.
- Las necesidades derivadas del Plan de Comunicación y Formación.
- Los resultados de las auditorías de compliance realizadas.
- Las consultas, denuncias, comunicaciones recibidas a través del Canal de Comunicación y Denuncias de Correos.

Igualmente, de manera semestral, el Comité de Cumplimiento deberá reportar al Consejo de Administración y a la Comisión de Auditoría y Control el resultado de los dictámenes emitidos.

E) Funciones del Comité de Cumplimiento

Las funciones del Comité de Cumplimiento son:

- Definir y actualizar el mapa de riesgos penales, en el que se establecen las actividades de Correos en cuyo ámbito podrían cometerse los delitos identificados.
- Supervisar el cumplimiento de los objetivos de cumplimiento y anticorrupción definidos anualmente por Correos.
- Supervisar, controlar y evaluar el cumplimiento del Sistema de Compliance por todos los integrantes de Correos.
- Monitorizar y auditar los controles implantados en el Sistema de Compliance de manera periódica.
- Procurar la implicación de todos los empleados en el cumplimiento del Código General de Conducta y del Sistema de Compliance para lograr una adecuada conexión entre las sociedades que integran Correos.
- Promover los planes de formación y comunicación necesarios para la implementación y actualización del Sistema de Compliance.
- Identificar las debilidades de control y los Planes de mejora para mitigarlos.
- Asesorar al Consejo de Administración sobre la toma de decisiones que puedan implicar una responsabilidad penal para cualquiera de las Sociedades que forman Correos.
- Analizar con rigor, objetividad, autonomía, independencia y confidencialidad las denuncias recibidas sobre conductas presuntamente ejecutadas al margen de los estándares mínimos de ética de Correos y que podrían generar un riesgo de imputación delictiva.
- Las comunicaciones recibidas de las que se desprenda que alguna de las Sociedades de Correos o de sus empleados se encuentren incursos en procedimiento judicial penal con motivo de hechos relacionados con su actividad profesional.
- Los requerimientos de documentación o información recibidos sobre cualesquiera sociedades de Correos o sobre cualquiera de sus empleados por Autoridades Judiciales, Ministerio Fiscal, Tribunal de Cuentas, Administraciones públicas o de las Fuerzas y Cuerpos de Seguridad del Estado por hechos relacionados con las funciones desarrolladas en las distintas áreas de actividad actuando en nombre y por cuenta, y en provecho de cualquiera de las sociedades de Correos.
- Determinar si las denuncias recibidas tienen la suficiente base fáctica para generar la apertura de un proceso de investigación interna y, en su caso, comunicar a la unidad correspondiente la existencia de hechos que pudieran dar lugar a la incoación de un proceso interno disciplinario, de acuerdo con la normativa estatutaria o laboral y el convenio colectivo aplicable al infractor.
- Emitir un dictamen interno de conclusiones de las denuncias y dar respuesta a las comunicaciones y consultas recibidas.
- Colaborar y procurar la agilidad en las respuestas a los requerimientos de información o documentación que efectúen los órganos judiciales, el Ministerio Fiscal o las Fuerzas y Cuerpos de Seguridad del Estado.

- Cumplir y controlar los plazos establecidos en el procedimiento desarrollado en el Estatuto del Comité de Cumplimiento para la emisión de dictámenes, trámites de alegaciones o cualquier otro trámite sujeto a plazo previsto en el mismo.
- Emitir los preceptivos informes establecidos en los procedimientos internos aprobados en cada una de las sociedades de Correos que tienen por objeto validar el cumplimiento de los estándares exigidos en el Código General de Conducta.
- Revisar y actualizar el Estatuto relativo al funcionamiento del Comité de Cumplimiento.
- Reportar al Consejo de Administración y la Comisión de Auditoría y Control sobre la supervisión, revisión y actualización del Sistema de Compliance y sobre la gestión del Canal de Comunicación y Denuncias.

El Comité de Cumplimiento delega en el Área de Cumplimiento la gestión diaria de sus funciones relativas a la supervisión del Sistema de Compliance, de vigilancia asociada a controles y medidas de prevención de delitos.

El Área de Cumplimiento está formada por la Secretaría del Comité de Cumplimiento y su equipo y se reúne de manera periódica para tratar las responsabilidades que le han sido encomendadas.

El Área de Cumplimiento reportará al Comité de Cumplimiento de manera periódica (como mínimo trimestral) sobre el estado y resultado de la supervisión, para su conocimiento y posterior reporte al Consejo de Administración, todo ello sin perjuicio de las comunicaciones continuas del presidente del Comité de Cumplimiento con el Área de Cumplimiento.

El reporte se reflejará en acta del Comité de Cumplimiento que deberá custodiar la Secretaría del mismo.

F) Relaciones con otras áreas

En el desempeño de sus actividades, el Comité de Cumplimiento deberá coordinarse con otras áreas de Correos, ya que tiene que utilizar la información y documentación generadas por estas. En este sentido, una relación de trabajo de cooperación entre el Área de Cumplimiento y el resto de áreas y departamentos en Correos favorece una adecuada identificación y gestión de los riesgos de Compliance.

El Comité de Cumplimiento (y, por ende, el Área de Cumplimiento) tendrá acceso a todas las personas, archivos, datos, sistemas y bienes que se estime necesarios para el desempeño de sus funciones y la ejecución del plan de trabajo. La información solicitada tendrá que facilitarse dentro de un periodo razonable y ser fiel e íntegra.

Canal de comunicación y denuncias. Aspectos clave

A) Finalidad y ámbito de aplicación

El Reglamento de Funcionamiento del Canal de Comunicación y Denuncias tiene por objeto establecer un procedimiento de funcionamiento interno del Canal de Comunicación y

Denuncias de la Sociedad Correos y Telégrafos, S.M.E. y sus sociedades filiales, desde el momento en que se reciba comunicación de un hecho que pudiera estar relacionado con una actuación u omisión presuntamente delictiva o generadora de un riesgo de imputación penal relativo a alguna de las Sociedades que componen Correos.

a) Objeto

El Reglamento se aprueba por Correos y Telégrafos, S.A. (en adelante, Correos y Telégrafos o la sociedad) y por el resto de filiales de Correos (en adelante, Correos) en su voluntad de establecer los compromisos en materia de gestión, investigación y tramitación de denuncias y comunicaciones recibidas.

b) Alcance

El alcance del Reglamento incluye al Comité de Cumplimiento que se regirá por su propio Estatuto y por el presente Reglamento.

B) Implantación del Canal de Comunicación y Denuncias

a) Definición de denuncia o comunicación

La **denuncia o comunicación** se define como una inquietud comunicada de buena fe y conscientemente por un empleado o tercera parte identificado en cualquiera de los medios de que dispone Correos y relacionado con temas de contabilidad, finanzas, corrupción, prácticas anticompetitivas, divulgación de información confidencial, conflictos de interés, seguridad del producto, procesos o trabajadores, calidad, acoso o cualquier otra práctica contraria al Código General de Conducta, así como a las dudas, mejoras o diferencias de interpretación sobre el mismo.

Si las denuncias se refieren a diferencias de opinión profesional en la llevanza organizativa u operativa de alguna área del negocio y no tuvieran implicación ética alguna, se remitirán al responsable del área correspondiente.

Las denuncias que se refieran a deficiencias de productos o servicios por parte de clientes o usuarios se remitirán a Atención al Cliente para su gestión, acusando recibo.

b) Principios básicos del Canal de Comunicación y Denuncias

El Consejo de Administración de Correos y Telégrafos manifiesta que el Canal de Comunicación y Denuncias está basado en los siguientes **principios:**

- **Principio de buena fe y compromiso de no represalia.** Los empleados y los terceros que hagan uso del canal deben actuar de buena fe y no hacer acusaciones falsas al manifestar sus inquietudes. La buena fe consiste en dar información sin malicia, sin considerar el beneficio personal y considerando la información veraz de forma razonable y con los medios de los que dispone. El empleado que deliberadamente haga declaraciones falsas

o engañosas o de mala fe podrá ser objeto de acciones disciplinarias de conformidad con la legislación vigente. Por otra parte, Correos establece formalmente que no tolerará represalias de ningún tipo contra aquellas personas que hagan uso de los procedimientos establecidos para la comunicación de conductas irregulares.

- **Confidencialidad.** Se adoptarán las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a todas las personas afectadas por la información suministrada en las denuncias. En especial, en el caso de denuncias no anónimas, la identidad del denunciante deberá mantenerse confidencial en todas las etapas del proceso de investigación y resolución de la denuncia, por lo que no se divulgará a terceros ni, por tanto, a la persona denunciada, ni tampoco a los superiores jerárquicos del denunciante.
- **Derecho al honor,** a la presunción de inocencia y de defensa. El derecho al honor de las personas es una de las máximas de actuación de Correos. Pondrá la mayor atención en velar por tales derechos, garantizando los derechos de las personas denunciadas a defenderse de cualquier acusación que se dirigiera contra él con las máximas garantías legales.

C) Implantación del Canal de Comunicación y Denuncias

El Canal de Comunicación y Denuncias de Correos permitirá la presentación de comunicaciones o denuncias por las siguientes vías:

- Canal verbal: el denunciante informa al superior jerárquico, quien informará al Área de Cumplimiento o al Comité de Cumplimiento.
- Canal postal: el denunciante informa a través de dirección postal.
- Canal electrónico: el denunciante informa a la dirección de correo electrónico habilitada al efecto.
- Canal electrónico en la web corporativa: el denunciante informa a través del canal electrónico implantado en las páginas web de cada una de las sociedades que lo componen.

El Canal de Comunicación y Denuncias de Correos permite a los empleados informar de las conductas sospechosas de las que tengan conocimiento, a través del **formulario que se encuentra en el Anexo,** al final de este apartado.

El Canal de Comunicación y Denuncias requiere la implantación de medidas de seguridad oportunas que garanticen la protección de los datos personales, la confidencialidad del denunciante y el acceso único por personas autorizadas.

D) Información al denunciante

El Canal de Comunicación y Denuncias incluirá un *checkbox* de aceptación que se enviará al informante, cuya marcación ha de ser un requisito *sine qua non* para la comunicación de la irregularidad (esta cláusula se actualizará en cada momento a la legislación vigente) junto

a la siguiente cláusula en cumplimiento del deber de información derivado de la normativa en materia de protección de datos:

> Correos agradece tu colaboración:
>
> Te informamos de que Correos velará por el respeto al derecho al honor y del cumplimiento del compromiso de no represalia por la comunicación efectuada de buena fe.
>
> Te informamos de que la confidencialidad de tu denuncia estará en todo momento garantizada de acuerdo a las buenas prácticas y la normativa vigente.
>
> Te informamos de que los datos relacionados en el registro de irregularidades/infracciones serán tratados de manera confidencial y se conservarán en el Canal de Comunicación y Denuncias por el tiempo estrictamente necesario para la tramitación de las actuaciones de investigación necesarias.
>
> Te informamos de que los datos de carácter personal se incluirán en el Canal de Comunicación y Denuncias a los solos efectos de investigar la denuncia. Los datos se eliminarán del canal de comunicaciones una vez termine dicha investigación y siempre dentro del límite temporal de tres meses. Transcurridos dichos tres meses tus datos serán eliminados del canal o serán anonimizados si la denuncia se utiliza para garantizar el funcionamiento Sistema de Compliance por Correos.
>
> Te informamos que, solo en caso de ser necesario al objeto de la investigación, tramitación o resolución, la información podrá ser cedida a terceros en cumplimiento de las obligaciones legales oportunas.
>
> Puedes ejercer tus derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, mediante la remisión de un escrito con la referencia «Protección de Datos», en el que se concrete la solicitud correspondiente a la dirección de correo electrónico habilitada al efecto.

E) Información al denunciado

Para dar cumplimiento a la obligación de informar al denunciado en plazo, se le informará de conformidad con los requerimientos establecidos en la normativa laboral y el régimen sancionador aplicables.

Si los hechos son constitutivos de un delito o de una infracción o sanción grave o muy grave, después del análisis del Área de Cumplimiento, se remitirá al empleado denunciado de forma personal y ante un responsable de Recursos Humanos, su inmediato superior o cualquier compañero que acceda como testigo una comunicación informando de la denuncia realizada y el régimen de tratamiento de los datos.

Igualmente, se le informará de sus deberes y obligaciones:

- Derecho a informar al representante de los trabajadores, tener acceso a la investigación y a su intervención activa en el procedimiento de investigación proponiendo las pruebas que considere.
- Se le prohíbe expresamente eliminar o modificar documentos o datos de cualquier tipo que estén en su poder o en poder de terceros, bien en formato físico o electrónico.
- Se le prohíbe expresamente entablar contacto con personal interno o externo de Correos para tratar cualesquiera cuestiones relativas a la investigación en curso, con obligación expresa de mantener la debida confidencialidad. Sin perjuicio del resultado de las investigaciones, la violación por el empleado de las prevenciones advertidas en esta acta dará lugar, en su caso, a las correspondientes medidas disciplinarias, sin perjuicio de la presentación de la oportuna denuncia ante las Fuerzas y Cuerpos de Seguridad, Fiscalía o el juzgado de instrucción correspondiente, por la destrucción de pruebas en el caso más grave.
- Se le requerirá para que entregue en este acto el ordenador, memorias externas, discos duros internos y extraíbles, teléfono móvil o cualquier dispositivo propiedad de la empresa que se le haya facilitado.
- Se le podrá informar de que se le facilita permiso remunerado permaneciendo siempre a disposición de Correos dependiendo de los hechos objeto de denuncia.
- Se le informará de que se está instruyendo un procedimiento de investigación por hechos ilícitos o ilegales que pudieran serle atribuidos. En el plazo más breve posible, se le comunicarán los hechos objeto de investigación y velará por el legítimo respeto a sus derechos de defensa y presunción de inocencia.
- Se le informará de que sus datos han sido obtenidos a través del Canal de Comunicación y Denuncias cuya finalidad consiste en investigar, tramitar y resolver las denuncias recibidas. Solo en caso de ser necesario, al objeto de la investigación, tramitación o resolución, la información podrá ser cedida a terceros en cumplimiento de las obligaciones legales oportunas.
- En todo caso podrá ejercer sus derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, mediante la remisión de un escrito con la referencia «Protección de Datos», en el que se concrete la solicitud correspondiente a la dirección de correo electrónico habilitada al efecto.

F) Procedimiento de denuncia

a) Plazos y conservación documental

Los datos personales que se obtengan o se generen con motivo del funcionamiento del Canal de Comunicación y Denuncias serán eliminados de dicho sistema en un plazo que no excederá de tres meses desde la incorporación de tales datos en el mismo, salvo que los hechos denunciados revistan relevancia penal, en cuyo caso podrán conservarse para dejar evidencia del funcionamiento del Sistema de Compliance, siempre anonimizando aquellos datos que no sean necesarios para tal finalidad. Las denuncias a las que no se hubiere dado curso solamente podrán constar de forma anonimizada en el sistema del Canal de Comunicación y Denuncias.

Si, transcurrido el plazo de tres meses antes mencionado, no hubiera concluido la investigación de la denuncia, los datos personales podrán seguir siendo tratados por el órgano al que corresponda dicha investigación, pero debiendo eliminarse del propio sistema del Canal de Comunicación y Denuncias.

Canal de Comunicación y Denuncias

CONCEPTO		PLAZO PROPUESTO DE CONSERVACIÓN	PLAZO TOTAL
Investigación, instrucción y curso de la denuncia	Investigación e instrucción de la alerta y plazo máximo de conservación	Plazo imprescindible para decidir si procede o no abrir investigación sobre los hechos denunciados Plazo máximo de 3 meses tras la introducción de los datos en el Canal	3 meses salvo que se pretenda dejar evidencia del funcionamiento del Canal
	Denuncias a las que no se han dado curso	Plazo máximo de 3 meses tras la introducción en el Canal, constando de forma anonimizada tras este periodo	3 meses
Utilización de los datos finalizar el plazo	Finalizado el plazo máximo de conservación de 3 meses	Tras finalizar este plazo no se debe conservar dato alguno en el sistema del Canal, sin perjuicio de que los datos puedan ser utilizados por otros departamentos de Correos	

La custodia física y lógica de los documentos se confía al Área de Cumplimiento.

Inicio del procedimiento. El procedimiento se iniciará:

- De oficio o mediante denuncia dirigida al Comité de Cumplimiento, en la que conste que se ha tenido conocimiento de que en el seno de Correos se ha producido o se está produciendo una conducta o hecho al margen de los estándares mínimos de ética, generadores de un riesgo de imputación penal.
- Mediante comunicación llevada a cabo por la unidad correspondiente, de conformidad con los procedimientos internos aprobados en cada una de las sociedades.
- Mediante consulta por parte de empleados sobre hechos susceptibles de constituir ilícitos penales interviniendo en nombre de cualquiera de las sociedades de Correos y en provecho de ellas.
- Mediante comunicación o denuncia recibida a través del Canal de Comunicación y Denuncias.

Denuncia. La denuncia se efectuará cumplimentando el modelo de formulario disponible en la página web de cada una de las sociedades, debiendo adjuntar toda la documentación de la que disponga el denunciante y que sirva de soporte justificativo de la misma.

Evaluación de la denuncia. Una vez que se reciba la denuncia, el Área de Cumplimiento, acusará recibo a la persona denunciante (en el plazo máximo de 7 días) y procederá a su inmediato análisis y comprobación.

El Área de Cumplimiento, tras efectuar el análisis y comprobación de la denuncia, podrá:

a) **Inadmitir** la denuncia por no apreciar conducta o hecho que pudiera acarrear implicaciones penales poniendo, en su caso, los hechos en conocimiento del Departamento correspondiente si se apreciasen otro tipo de implicaciones, en especial la posible comisión de conductas constitutivas de infracción. Tal comunicación deberá realizarse en un plazo máximo de 5 días hábiles a contar desde el día siguiente a su recepción. Si se inadmite la denuncia, el Área de Cumplimiento remitirá un informe justificativo al Comité de Cumplimiento en un plazo máximo de 5 días. En todo caso, el Comité de Cumplimiento deberá estar informado de la resolución de la denuncia recibida y las medias de corrección o mejora que se aplicarán en Correos.
b) **Admitir** la comunicación presentada por apreciar hechos o conductas que pudieran conllevar implicaciones penales. En caso de admitir la comunicación, el Comité de Cumplimiento informará al comunicante de su decisión en un plazo máximo de 5 días hábiles a contar desde el día siguiente a su recepción y abrirá el correspondiente procedimiento de investigación interna.

Cada uno de los procedimientos abiertos por el Área de Cumplimiento constituirá un expediente que deberá estar debidamente clasificado.

En el momento de recepción de la denuncia, el Área de Cumplimiento estudiará si existe algún tipo de incompatibilidad para comenzar la investigación. Si algún componente del Área de cumplimiento presenta algún conflicto de interés con alguna de las partes o es parte de la denuncia, se le separará y serán el resto de componentes del área los encargados de llevar a cabo la investigación, manteniendo el deber de reserva de la misma.

G) Procedimiento investigador

Inicio. El procedimiento investigador se iniciará desde el momento en que el Área de Cumplimiento admita una denuncia presentada por los medios de envío señalados anteriormente. Podrá también iniciar de oficio el procedimiento si conoce hechos que objetivamente revistan los caracteres de delito por actos cometidos en nombre de alguna de las sociedades y en su provecho.

Investigación. El trámite de investigación tiene por objeto realizar todas las entrevistas, análisis e indagaciones necesarios para esclarecer los hechos comunicados. A tal efecto, se podrá requerir a los interesados en el procedimiento, así como a cualquier otra persona o titular, u órgano de la Sociedad afectada para el cumplimiento de su objetivo instructor.

Se dejará constancia de todo lo realizado en el expediente abierto al efecto, incluidas declaraciones y documentación recibidas.

El plazo máximo de tramitación del procedimiento será de 2 meses desde la recepción de la denuncia por parte del Área de Cumplimiento o del conocimiento por el órgano del hecho asociado al riesgo penal, pudiéndose prorrogar por periodos de 1 mes en el supuesto de

estimarlo así necesario por motivos justificados y con el correspondiente permiso del Comité de Cumplimiento.

La decisión de prórroga del procedimiento deberá ser motivada, constar por escrito y ser firmada por el presidente del Comité de Cumplimiento.

El procedimiento se adecuará a los siguientes principios básicos rectores, a los que deberán atenerse todas las personas que participan en el mismo:

- Rapidez: procedimiento ágil, sin demoras injustificadas en su tramitación.
- Confidencialidad: protección al honor, a la intimidad y dignidad de todas las personas implicadas.
- Presunción de inocencia de cualquier persona implicada.
- Objetividad, autonomía e independencia del procedimiento mediante la investigación exhaustiva y rigurosa de los hechos comunicados, sin injerencias de ningún tipo por parte de otros departamentos u órganos de gobierno de la sociedad afectada.

Obtención de pruebas. El procedimiento de obtención de pruebas, por parte del Área de Cumplimiento, deberá realizarse respetando la legalidad vigente y constar en un informe por escrito. Una vez obtenidas todas las pruebas y, en todo caso, antes de 3 meses desde el inicio de la investigación, el instructor deberá comunicar el resultado del informe:

- Al Comité de Cumplimiento.
- Al Área de Recursos Humanos cuando proceda llevar a cabo un procedimiento sancionador.
- Al denunciado para que este alegue lo que estime conveniente y pueda aportar las pruebas de descargo que considere oportunas.
- Al superior jerárquico del denunciado.

H) Conclusión del procedimiento

Una vez realizadas las actuaciones tendentes al esclarecimiento de los hechos comunicados, el Área de Cumplimiento finalizará el procedimiento investigador emitiendo un informe que será remitido al Comité de Cumplimiento en alguno de los siguientes sentidos:

1. Que no se ha ejecutado conducta alguna que haya generado un riesgo de imputación delictiva o que pueda constituir una infracción de otro tipo.
2. Si la conducta pudiera ser constitutiva de infracción no penal.
3. Que se ha ejecutado una conducta que pudiera ser constitutiva de delito.

Una vez recibido el informe por el Comité de Cumplimiento, sus integrantes revisarán las pruebas y la conclusión del Área de Cumplimiento y, sobre la propuesta de resolución, por mayoría simple, decidirán motivadamente:

1. En el caso de que la conducta no constituya infracción, se procederá al archivo del expediente.

2. En el caso de que la conducta pueda ser constitutiva de infracción no penal, se dará traslado a Recursos Humanos para que adopte la medida pertinente de conformidad con el Régimen Sancionador aplicable.
3. En el caso de que la conducta sea constitutiva de infracción penal, se comunicarán los hechos al Ministerio Fiscal o a los órganos judiciales pertinentes.
4. En el caso de que se haya constatado la falta de eficacia de un procedimiento de control de Correos, el Comité de Cumplimiento corregirá las deficiencias detectadas en el mismo.

En caso de empate, el presidente tendrá voto de calidad.

I) Resolución por el Consejo de Administración

El Comité de Cumplimiento someterá a la ratificación del Consejo de Administración de la sociedad la decisión final adoptada:

1. Si los hechos son de especial trascendencia.
2. Por razón del cargo ostentado por la persona infractora.
3. Por la posible repercusión de los hechos en la organización o en la reputación de la Sociedad.

El Consejo de Administración ratificará, o no, por mayoría simple de sus miembros, la decisión informada por el Comité de Cumplimiento, dándole traslado de su decisión.

J) Procedimiento de Adopción de Medidas

a) Denuncia falsa

Si de la investigación realizada se acredita que los hechos denunciados son falsos, y que se han realizado por parte del denunciante a sabiendas de su falsedad y por motivos espurios, el denunciante será sancionado de conformidad con el régimen sancionador aplicable.

b) Denuncia verdadera

Si de la investigación realizada se acredita la realidad de los hechos y se puede determinar al responsable de los mismos, se adoptarán las sanciones correspondientes de conformidad con el régimen sancionador aplicable y se implantarán las medidas correctivas de los procedimientos incumplidos, cuando proceda.

c) Denuncia no acreditable al sujeto infractor

Si de la investigación realizada se hubiera acreditado la veracidad de los hechos, pero no pudiera determinarse al responsable de los mismos, el Comité de Cumplimiento pondrá en conocimiento del área correspondiente dicha situación. Una vez realizadas todas las acciones de investigación posibles, y no identificado el infractor, se procederá al registro y archivo del expediente.

d) Tipología de infracciones y sanciones

La tipología de las sanciones será en todo caso coincidente con el Convenio Colectivo de aplicación, con el fin de respetar al máximo los derechos de los trabajadores y la paz social. En todo caso, si del resultado de la investigación se concluyera que el denunciado ha cometido un hecho ilícito, el resultado del informe se pondrá en conocimiento de los Cuerpos y Fuerzas de Seguridad del Estado, tomando las medidas disciplinarias cautelares de forma inmediata.

K) Procedimiento de consulta

Cuando se solicite el parecer del Área de Cumplimiento respecto de una conducta aún no realizada, la respuesta en forma de informe deberá realizarse en un plazo no superior a 15 días hábiles a contar desde la recepción de la solicitud.

L) Conservación de la documentación

Será obligatorio conservar todos aquellos documentos que puedan servir de soporte probatorio de la conducta o hechos objeto de la comunicación durante el periodo de tiempo en que exista obligación legal de conservación de dichos documentos, si bien no podrán conservarse en el Canal de Comunicación y Denuncias más a allá de 3 meses desde su recepción.

Tendrá la consideración de documento todo soporte tangible o intangible que contenga información lo suficientemente precisa y relevante como para poder determinar que una conducta presuntamente delictiva se está produciendo, y las personas o sociedades de Correos se encuentran involucradas en la misma.

En particular, se conservarán especialmente, para su eventual uso en toda investigación o análisis en caso de iniciarse una investigación por un órgano administrativo, judicial, el Ministerio Fiscal, el defensor del pueblo, el Tribunal de Cuentas u organismo análogo o con funciones investigadoras, los documentos o registros que acrediten adecuadamente:

a) Las conductas de riesgo presuntamente detectadas.
b) Los intervinientes.
c) Los informes del Área de Cumplimiento y los Dictámenes de Conclusiones emitidos por el Comité de Cumplimiento.
d) Las comunicaciones generadas en el curso de la tramitación del procedimiento.
e) La totalidad de informes internos y externos emitidos, notas internas, correos electrónicos intercambiados al respecto de la incidencia, etc.
f) Las actas del Comité de Cumplimiento y de otros órganos en las que se recoja información relacionada con incidencias comunicadas o detectadas.

El inicio del cómputo del plazo de custodia comenzará desde que se emita el Dictamen de Conclusiones por el Comité de Cumplimiento del riesgo de imputación penal o desde el acuerdo adoptado por el Consejo de Administración.

En todo caso, el sistema de archivo deberá asegurar la adecuada gestión y disponibilidad de la documentación, tanto a efectos de control interno, como de atención en tiempo y forma de los requerimientos de cualesquiera autoridades u organismos y entes públicos que vengan amparados por la normativa que resulte de aplicación.

Los documentos se almacenarán en soportes que garanticen su integridad, confidencialidad, la correcta lectura de los datos, su no manipulación y su adecuada conservación y localización, ello sin perjuicio de que también puedan ser almacenados en soporte papel.

M) Reserva y confidencialidad de la información y documentación

Se impone la obligación de guardar reserva y confidencialidad sobre la información y documentación que sean objeto de denuncia, comunicación y consulta a través del Canal de Comunicación y Denuncias a todas aquellas personas que tuvieran conocimiento de la misma.

El incumplimiento de esta obligación podrá conllevar la incoación de procedimiento disciplinario de conformidad con el convenio colectivo, normativa laboral y estatutaria que fuere de aplicación al infractor.

No se dará a conocer la identidad de la persona comunicante, quien será siempre protegida de cualquier represalia que, con motivo de su comunicación, pudiera dirigirse contra él, salvo en aquellos supuestos en los que haya actuado de mala fe.

Lo anterior se entiende sin perjuicio de la obligación de identificar al comunicante a petición de autoridades judiciales o administrativas.

N) Información a la Comisión de Auditoría y Control de la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E.

El Comité de Cumplimiento deberá elevar, en todo caso, cada seis meses al Consejo de Administración de la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E. por medio de la Comisión de Auditoría y Control, informe sobre:

- El contenido y resultado de los dictámenes de conclusiones que se emitan sobre las comunicaciones y denuncias recibidas.

El Comité de Cumplimiento remitirá copia del informe a cada una de las Sociedades de Correos afectadas por su contenido.

Anexo. Formulario de denuncia

	FORMULARIO DE DENUNCIA
Nombre y apellidos del denunciante. (Campo no obligatorio)	
Cargo, departamento que ocupa en la Sociedad y teléfono de contacto/Relación con la sociedad.	
Fecha en la que ingresó en la Sociedad./ Fecha de contacto con la sociedad.	
Nombre y apellidos del trabajador o trabajadores presuntamente infractores.	
Comunicación de la incidencia.	
Documentación Adjunta.	No □ Sí □ En caso afirmativo, relacione, por favor, la documentación que se adjunta:
Fecha:	Firma:

12.3.2. Transparencia

Marco legal

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno representa una nueva forma de entender las relaciones entre la Administración y los ciudadanos, partiendo de la base de que la transparencia, el acceso a la información pública y las normas de buen gobierno deben ser los ejes fundamentales de toda acción política. Solo cuando la acción de los responsables públicos se somete a escrutinio, los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones; podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos.

A los efectos que interesan al Grupo Correos, la Ley 19/2013 tiene **dos impactos** principales:

1. Incrementa y refuerza la transparencia en la actividad pública (que se articula a través de obligaciones de publicidad activa).
2. Reconoce y garantiza el acceso a la información (regulado como un derecho de amplio ámbito subjetivo y objetivo).

En cuanto a la transparencia de la actividad pública a través de publicidad activa, antes de la publicación de la Ley 19/2013 ya existían en el ordenamiento jurídico español normas sectoriales que contenían obligaciones concretas de publicidad activa para determinados sujetos. Así, por ejemplo, en materia de contratos, subvenciones, presupuestos o actividades de altos cargos, nuestro país contaba con un destacado nivel de transparencia. Sin embargo, esta regulación resultaba insuficiente y no satisfacía las exigencias sociales y políticas del momento. Por ello, con la Ley 19/2013 se avanzó y se profundizó en la configuración de obligaciones de publicidad activa que debían vincular a un amplio número de sujetos, entre los que se encuentran, entre otros, todas las Administraciones públicas, los órganos de los poderes legislativo y judicial en lo que se refiere a sus actividades sujetas a Derecho Administrativo o las sociedades mercantiles estatales como Correos.

Respecto al segundo impacto, la Ley 19/2013 también regula el derecho de acceso a la información pública que, no obstante, ya había sido desarrollado en otras disposiciones de nuestro ordenamiento. En efecto, partiendo de la previsión contenida en el artículo 105.b) de nuestro texto constitucional, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones públicas y del Procedimiento Administrativo Común (derogada), ya desarrollaba en su artículo 37 el derecho de los ciudadanos a acceder a los registros y documentos ubicados en los archivos administrativos. Sin embargo, esta regulación contenía una serie de deficiencias que fueron puestas de manifiesto de forma reiterada al no ser claro el objeto del derecho de acceso, al estar limitado a documentos contenidos en procedimientos administrativos ya terminados y al resultar su ejercicio extraordinariamente limitado en su articulación práctica. En este sentido, la vigente Ley de Procedimiento Administrativo Común de las Administraciones públicas (Ley 39/2015, de 1 de octubre) ya reconoce como derechos de las personas en sus relaciones con las Administraciones públicas «el acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico» (artículo 13.d).

Igualmente, pero con un alcance sectorial y derivado de sendas Directivas comunitarias, otras normas contemplan el acceso a la información pública. Es el caso de la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente, y de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, que regula el uso privado de documentos en poder de Administraciones y organismos del sector público.

La Ley 19/2013, por lo tanto, no parte de la nada ni colma un vacío absoluto, sino que ahonda en lo ya conseguido, supliendo sus carencias, subsanando sus deficiencias y creando un marco jurídico acorde con los tiempos y los intereses ciudadanos.

Por otro lado, la Disposición final séptima de la Ley 19/2013 establece que «El Gobierno, en el ámbito de sus competencias, podrá dictar cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta Ley». En relación con ello, el IV Plan de Gobierno Abierto 2020-2024 recoge el compromiso de aprobar el Reglamento de desarrollo de la Ley 19/2013, al considerar que durante los años de vigencia de la citada ley se ha constatado la necesidad de solventar algunos problemas prácticos, aclarar conceptos y apostar por nuevos enfoques de acuerdo con las demandas de la ciudadanía y de las Administraciones públicas. Se pretende así completar la regulación en lo que se refiere a aspectos relativos al Portal de Transparencia, como punto que posibilite el acceso a la información facilitando el cumplimiento de las obligaciones de publicidad activa y favoreciendo el ejercicio del derecho de acceso a la información por las personas interesadas con las máximas garantías.

Dicho Plan de Gobierno Abierto también incluye el compromiso de reformar la Ley 19/2013. El alcance de esta reforma deberá perfilarse en los procesos de consulta y audiencia pública, si bien el Plan considera necesario profundizar en las cuestiones más demandadas por la ciudadanía tales como la ampliación de las obligaciones de publicidad activa, las máximas garantías en el ejercicio del derecho de acceso y en la actividad de los órganos garantes y el impulso de la participación ciudadana en los asuntos públicos.

La Ley 19/2013 y su aplicación al Grupo Correos

Ámbito subjetivo de aplicación de la Ley 19/2013

El Título I de la Ley 19/2013, denominado «Transparencia de la actividad pública», incluye las disposiciones sobre Publicidad activa y Derecho de acceso a la información pública que, de acuerdo con el artículo 2 de dicha Ley, serán de aplicación a:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las ciudades de Ceuta y Melilla y las entidades que integran la Administración Local.
b) Las entidades gestoras y los servicios comunes de la Seguridad Social, así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.
c) Los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y las entidades de Derecho Público que tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad.
d) Las entidades de Derecho Público con personalidad jurídica propia, vinculadas a cualquiera de las Administraciones públicas o dependientes de ellas, incluidas las Universidades públicas.

e) Las corporaciones de Derecho Público, en lo relativo a sus actividades sujetas a Derecho Administrativo.
f) La Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo.
g) **Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50%.**
h) Las fundaciones del sector público.
i) Las asociaciones constituidas por las Administraciones, organismos y entidades previstos en este artículo. Se incluyen los órganos de cooperación previstos en los artículos 145 y siguientes de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en la medida en que, por su peculiar naturaleza y por carecer de una estructura administrativa propia, le resulten aplicables las disposiciones de este título.

A los efectos de aplicación de las disposiciones sobre Transparencia de la actividad pública (Título I de la Ley 19/2013), se entiende por Administraciones públicas los organismos y entidades incluidos en las letras a) a d).

Asimismo, la Ley 19/2013 establece que las disposiciones relativas a publicidad activa (Capítulo II del Título I) —por tanto, no las disposiciones sobre derecho de acceso— serán también aplicables a:

a) Los partidos políticos, organizaciones sindicales y organizaciones empresariales.
b) Las entidades privadas que perciban durante el periodo de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40% del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros.

De conformidad con lo expuesto, las sociedades del Grupo Correos se encuentran incluidas en el ámbito subjetivo de aplicación de la Ley 19/2013, dado que todas ellas ostentan la condición de «sociedades mercantiles estatales» con participación pública superior al 50%. En este sentido, recordamos que el accionista único de la Sociedad Estatal Correos y Telégrafos, S.A., S.M.E. (Correos) es la Sociedad Estatal de Participaciones Industriales (SEPI), dependiente del Ministerio de Hacienda y Función Pública. A su vez, Correos, matriz del Grupo, posee una participación del 100% en las filiales Correos Express, Nexea y Correos Telecom.

El hecho de que las sociedades del Grupo Correos se encuentren incluidas dentro del ámbito subjetivo de aplicación de la Ley 19/2013 implica que quedan sujetas a las obligaciones en materia de publicidad activa y derecho de acceso a la información pública que detalla dicha Ley, con excepción de aquellas exigencias de las que quedan exoneradas expresamente.

Publicidad activa: obligaciones de las sociedades mercantiles estatales

El capítulo II de la Ley 19/2013, dedicado a la publicidad activa, establece una serie de obligaciones para los sujetos incluidos en el ámbito de aplicación del Título I (Transparencia de la actividad pública), que habrán de difundir determinada información sin esperar una solicitud concreta de los ciudadanos.

Las sociedades del Grupo Correos quedan sujetas a dichas obligaciones, excepto a aquellas dirigidas expresamente a las Administraciones públicas o a otros sujetos.

Los **contenidos que deben publicar** de forma proactiva las sociedades mercantiles estatales son los siguientes:

- Información institucional, organizativa y de planificación (artículo 6 Ley 19/2013):
  - Funciones que desarrollan.
  - Normativa que les sea de aplicación.
  - Su estructura organizativa, incluyendo un organigrama actualizado que identifique a los responsables de los diferentes órganos y su perfil y trayectoria profesional.
- Información económica, presupuestaria y estadística (artículo 8 Ley 19/2013):
  - Contratos.
  - Convenios de colaboración y encomiendas de gestión.
  - Subvenciones y ayudas públicas concedidas.
  - Información presupuestaria.
  - Cuentas anuales e informes de fiscalización emitidos por parte de los órganos de control externo.
  - Retribuciones percibidas anualmente por los altos cargos y máximos responsables, así como las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo.
  - Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos, así como las que autoricen el ejercicio de actividad privada al cese de los altos cargos.
  - La información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia.

Cabe señalar nuevamente que quedan fuera de esta relación aquellas obligaciones de las que se excluye expresamente a las sociedades mercantiles estatales, como las recogidas en el artículo 7 de la Ley 19/2013 («información de relevancia jurídica», enfocada a las Administraciones públicas) o en el artículo 6 bis («registro de actividades de tratamiento», dirigida a los sujetos enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales).

Principios generales de la publicidad activa

Los sujetos enumerados en el artículo 2.1 de la Ley 19/2013, entre ellos las sociedades mercantiles estatales, publicarán de forma periódica y actualizada la información cuyo

conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

La información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada, así como su identificación y localización.

Toda la información será comprensible, de acceso fácil y gratuito.

Derecho de acceso a la información pública

Todas las personas tienen derecho a acceder a la información pública en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por la Ley 19/2013.

Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación del Título I de la Ley 19/2013 y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Procedimiento de solicitud de acceso a la información

El procedimiento para el ejercicio del derecho de acceso se iniciará con la presentación de la correspondiente solicitud, que deberá dirigirse al titular del órgano administrativo o entidad que posea la información.

La solicitud podrá presentarse por cualquier medio que permita tener constancia de:

a) La identidad del solicitante.
b) La información que se solicita.
c) Una dirección de contacto, preferentemente electrónica, a efectos de comunicaciones.
d) En su caso, la modalidad que se prefiera para acceder a la información solicitada.

El solicitante no está obligado a motivar su solicitud de acceso a la información. Sin embargo, podrá exponer los motivos por los que solicita la información y que podrán ser tenidos en cuenta cuando se dicte la resolución. No obstante, la ausencia de motivación no será por sí sola causa de rechazo de la solicitud.

Causas de inadmisión de solicitudes de información (artículo 18 Ley 19/2013)

No se admitirán a trámite, mediante resolución motivada, las solicitudes:

a) Que se refieran a información que esté en curso de elaboración o de publicación general.
b) Referidas a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas.

c) Relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración.
d) Dirigidas a un órgano en cuyo poder no obre la información cuando se desconozca el competente.
e) Que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta ley.

A estas causas de inadmisión debe agregarse otra recogida en la Disposición adicional primera de la Ley 19/2013, sobre regulaciones especiales del derecho de acceso a la información pública:

> 1. La normativa reguladora del correspondiente procedimiento administrativo será la aplicable al acceso por parte de quienes tengan la condición de interesados en un procedimiento administrativo en curso a los documentos que se integren en el mismo.
>
> 2. Se regirán por su normativa específica, y por esta ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.
>
> 3. En este sentido, esta ley será de aplicación, en lo no previsto en sus respectivas normas reguladoras, al acceso a la información ambiental y a la destinada a la reutilización.

Límites al derecho de acceso (artículos 14 y 15 de la Ley 19/2013)

Artículo 14. Límites al derecho de acceso

El **derecho de acceso** podrá ser limitado cuando acceder a la información suponga un perjuicio para:

a) La seguridad nacional.
b) La defensa.
c) Las relaciones exteriores.
d) La seguridad pública.
e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.
f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva.
g) Las funciones administrativas de vigilancia, inspección y control.
h) Los intereses económicos y comerciales.
i) La política económica y monetaria.
j) El secreto profesional y la propiedad intelectual e industrial.
k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión.
l) La protección del medio ambiente.

La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.

Artículo 15. Protección de datos personales

Si la información solicitada contuviera **datos personales** «especialmente protegidos» (ideología, afiliación sindical, religión o creencias, etc.) el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Con carácter general, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará en consideración, entre otros, los siguientes criterios:

a) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.
b) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

Resolución de solicitudes de información

La resolución en la que se conceda o deniegue el acceso deberá notificarse al solicitante y a los terceros afectados que así lo hayan solicitado en el plazo máximo de un mes desde la recepción de la solicitud por el órgano competente para resolver.

Este plazo podrá ampliarse por otro mes en el caso de que el volumen o la complejidad de la información que se solicita así lo hagan necesario y previa notificación al solicitante.

Serán motivadas las resoluciones que denieguen el acceso, las que concedan el acceso parcial o a través de una modalidad distinta a la solicitada y las que permitan el acceso cuando haya habido oposición de un tercero.

Cuando la mera indicación de la existencia o no de la información supusiera la vulneración de alguno de los límites al acceso, se indicará esta circunstancia al desestimarse la solicitud.

Transcurrido el plazo máximo para resolver sin que se haya dictado y notificado resolución expresa, se entenderá que la solicitud ha sido desestimada.

Las resoluciones dictadas en materia de acceso a la información pública son recurribles directamente ante la Jurisdicción Contencioso-administrativa, sin perjuicio de la posibilidad de interposición de la reclamación potestativa ante el Consejo de Transparencia y Buen Gobierno, prevista en el artículo 24.

El incumplimiento reiterado de la obligación de resolver en plazo tendrá la consideración de infracción grave a los efectos de la aplicación a sus responsables del régimen disciplinario previsto en la correspondiente normativa reguladora.

Régimen de impugnaciones (artículo 24)

Frente a toda resolución expresa o presunta en materia de acceso podrá interponerse una reclamación ante el Consejo de Transparencia y Buen Gobierno, con carácter potestativo y previo a su impugnación en vía contencioso-administrativa.

La reclamación se interpondrá en el plazo de un mes a contar desde el día siguiente al de la notificación del acto impugnado o desde el día siguiente a aquel en que se produzcan los efectos del silencio administrativo.

La tramitación de la reclamación se ajustará a lo dispuesto en materia de recursos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Cuando la denegación del acceso a la información se fundamente en la protección de derechos o intereses de terceros se otorgará, previamente a la resolución de la reclamación, trámite de audiencia a las personas que pudieran resultar afectadas para que aleguen lo que a su derecho convenga.

El plazo máximo para resolver y notificar la resolución será de 3 meses, transcurrido el cual la reclamación se entenderá desestimada.

Las resoluciones del Consejo de Transparencia y Buen Gobierno se publicarán, previa disociación de los datos de carácter personal que contuvieran, por medios electrónicos, una vez se hayan notificado a los interesados.

El presidente del Consejo de Transparencia y Buen Gobierno comunicará al Defensor del Pueblo las resoluciones que dicte en aplicación de este artículo.

La competencia para conocer de dichas reclamaciones corresponderá al Consejo de Transparencia y Buen Gobierno, salvo en aquellos supuestos en que las comunidades autónomas atribuyan dicha competencia a un órgano específico, de acuerdo con lo establecido en la Disposición adicional cuarta de esta Ley.

El Portal de Transparencia de Correos

Introducción

De acuerdo con lo establecido en la Ley 19/2013, los sujetos incluidos en su ámbito subjetivo de aplicación (entre ellos, las sociedades mercantiles estatales como Correos), deberán publicar de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

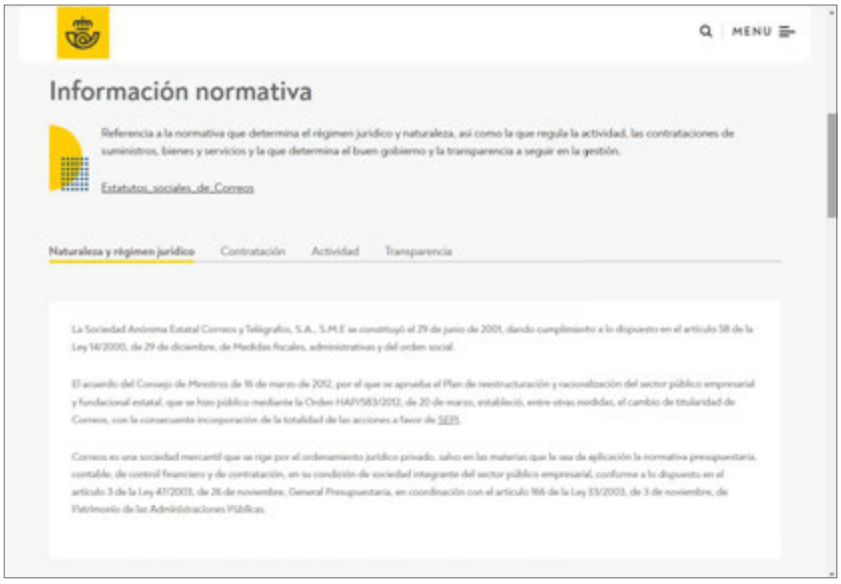
Asimismo, la Ley dispone que la información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados.

En línea con lo anterior, Correos cuenta con su propio Portal de Transparencia, ubicado dentro de la web corporativa, mediante el que da cumplimiento a sus obligaciones en materia de publicidad activa.

Contenidos del portal

El Portal de Transparencia de Correos presenta la información estructurada en tres grandes bloques:

1. **Información normativa**
   Este apartado del Portal responde a una de las exigencias en materia de publicidad activa contempladas en el artículo 6 de la Ley 19/2013: la publicación de la normativa que resulta de aplicación a Correos.



En cumplimiento de dicha obligación, el apartado recoge la referencia a la normativa que determina el régimen jurídico y naturaleza de Correos, así como la que regula la actividad, las contrataciones de suministros, bienes y servicios y la que determina el buen gobierno y la transparencia a seguir en la gestión.

2. **Información organizativa**
   Dentro de la sección «Información organizativa» se publica el resto de los contenidos a los que alude el mismo artículo 6, es decir:

- Funciones desarrolladas por Correos.
- Estructura organizativa.
- Organigrama actualizado.
- Perfil y trayectoria profesional de los responsables de los diferentes órganos.

3. Información económica

Este bloque incluye los contenidos de naturaleza económica, presupuestaria y estadística, a los que se refiere el artículo 8 de la Ley 19/2013:

- Información sobre contratos.
- Relación de convenios y encomiendas de gestión.
- Subvenciones y ayudas públicas concedidas.
- Información presupuestaria.
- Cuentas anuales e informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo.
- Retribuciones e indemnizaciones percibidas por quien ostente la condición de alto cargo y máximo responsable (en el caso de Correos, el presidente).
- Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos.
- Información estadística sobre el grado de cumplimiento y calidad del servicio postal universal.

Canal de acceso

Además de la publicidad activa de contenidos, el Portal de Transparencia de Correos cumple otra función: ofrecer información a los ciudadanos sobre el ejercicio del derecho de acceso a la información pública de Correos.

En este sentido, la sección «Derecho de acceso» detalla el procedimiento que se ha de seguir para el envío de solicitudes de información pública:

> El procedimiento para el ejercicio del derecho de acceso se iniciará con la presentación de la correspondiente solicitud, que deberá permitir tener constancia de la identidad del solicitante, la información que se solicita, la dirección de contacto a efectos de comunicaciones y, en su caso, la modalidad que prefiera para acceder a la información solicitada.

A efectos de acreditación de identidad, se indica que la solicitud «deberá incluir su nombre y dos apellidos; fotocopia del DNI o Pasaporte, o bien firma electrónica reconocida en el caso de las solicitudes enviadas por correo electrónico».

A continuación, se especifican las tres vías que se ponen a disposición de los interesados para el envío de solicitudes:

Adicionalmente, el bloque «Derecho de acceso» del Portal de Transparencia de Correos incluye otros contenidos que no resultan obligatorios de acuerdo con la Ley 19/2013, pero que se consideran de interés para los ciudadanos en el marco del compromiso de Correos en materia de transparencia y rendición de cuentas. Son los siguientes:

- «Resoluciones»: incluye dos tipos de contenidos:
  - Resoluciones denegatorias de Correos en virtud de los límites al acceso previstos en los artículos 14 y 15 de la Ley 19/2013.
  - Resoluciones del Consejo de Transparencia y Buen Gobierno (CTBG) sobre reclamaciones interpuestas frente a Resoluciones de acceso emitidas por Correos.
- «Estadísticas de acceso»: comprende información de interés sobre el ejercicio del derecho de acceso a la información pública por parte de los ciudadanos, ofreciendo datos estadísticos relativos al número de solicitudes recibidas anualmente desde la creación del Portal de Transparencia y su distribución mensual, temática y canal de recepción.

Es necesario mencionar, finalmente, que las filiales de Correos (Correos Express, Correos Telecom y Nexea), como sociedades mercantiles estatales con participación pública superior

al 50%, también disponen de sus propios Portales de Transparencia, alojados dentro de sus páginas web, cuya estructura y diseño es similar a la del Portal de Correos.

El Consejo de Transparencia y Buen Gobierno

Introducción

La Ley 19/2013 crea y regula el Consejo de Transparencia y Buen Gobierno, un órgano independiente al que se otorgan competencias de promoción de la cultura de transparencia en la actividad de la Administración Pública, de control del cumplimiento de las obligaciones de publicidad activa, así como de garantía del derecho de acceso a la información pública. Se crea, por lo tanto, un órgano de supervisión y control para garantizar la correcta aplicación de la Ley.

El Consejo de Transparencia y Buen Gobierno se configura como un órgano independiente, con plena capacidad jurídica y de obrar, y cuenta con una estructura sencilla que, a la vez que garantiza su especialización y operatividad, evita crear grandes estructuras administrativas. La independencia y autonomía en el ejercicio de sus funciones vendrá garantizada, asimismo, por el respaldo parlamentario con el que deberá contar el nombramiento de su presidente.

Para respetar al máximo las competencias autonómicas, expresamente se prevé que el Consejo de Transparencia y Buen Gobierno solo tendrá competencias en aquellas Comunidades Autónomas con las que haya firmado convenio al efecto, quedando, en otro caso, en manos del órgano autonómico que haya sido designado para el ejercicio de las competencias que a nivel estatal asume el Consejo.

El Consejo de Transparencia y Buen Gobierno se rige por lo dispuesto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como por las disposiciones que la desarrollen y por su Estatuto, aprobado por Real Decreto 919/2014, de 31 de octubre.

Funciones y principios

El Consejo de Transparencia y Buen Gobierno tiene por finalidad promover la transparencia de la actividad pública, velar por el cumplimiento de las obligaciones de publicidad, salvaguardar el ejercicio de derecho de acceso a la información pública y garantizar la observancia de las disposiciones de buen gobierno.

A) Funciones

Para la consecución de sus objetivos, el Consejo de Transparencia y Buen Gobierno tiene encomendadas, entre otras, las siguientes funciones:

a) Adoptar recomendaciones para el mejor cumplimiento de las obligaciones contenidas en la Ley 19/2013.
b) Asesorar en materia de transparencia, acceso a la información pública y buen gobierno.
c) Informar preceptivamente los proyectos normativos de carácter estatal que desarrollen la Ley 19/2013 o que estén relacionados con su objeto.
d) Evaluar el grado de aplicación de la Ley. Para ello, elaborará anualmente una memoria en la que se incluirá información sobre el cumplimiento de las obligaciones previstas y que será presentada ante las Cortes Generales.
e) Promover la elaboración de borradores de recomendaciones y de directrices y normas de desarrollo de buenas prácticas en materia de transparencia, acceso a la información pública y buen gobierno.

B) Principios

a) Transparencia

Las resoluciones del Consejo, una vez notificadas y previa disociación de los datos de carácter personal, serán publicadas en su propia página web y en su Portal de la Transparencia.

El resumen de la memoria anual del Consejo será publicado en el Boletín Oficial del Estado, con especial atención al nivel de cumplimiento por parte de la Administración de las disposiciones de la Ley de transparencia, acceso a la información pública y buen gobierno.

b) Participación ciudadana

El Consejo, a través de los cauces de participación que se establezcan, colaborará con los ciudadanos para el mejor desempeño de sus funciones y para favorecer el cumplimiento de la normativa de transparencia y buen gobierno.

c) Rendición de cuentas

El Consejo de Transparencia y Buen Gobierno elevará anualmente a las Cortes Generales una memoria sobre el desarrollo de sus actividades y sobre el grado de cumplimiento de las disposiciones establecidas en la Ley.

El presidente del Consejo de Transparencia y Buen Gobierno comparecerá ante la Comisión correspondiente para dar cuenta de tal memoria cuantas veces sea requerido para ello.

d) Colaboración

El Consejo de Transparencia y Buen Gobierno convocará reuniones, con periodicidad al menos anual con los representantes de los organismos que hayan sido creados a nivel autonómico para el ejercicio de funciones similares a las encomendadas al Consejo.

El Consejo celebrará convenios de colaboración con las Comunidades Autónomas y Entidades Locales para la resolución de las reclamaciones que puedan presentarse ante la denegación expresa o presunta del derecho de acceso.

Asimismo, celebrará convenios de colaboración con las Administraciones públicas, las organizaciones sociales, las universidades, los centros de formación y cualquier otro

organismo nacional o internacional cuyas actividades se relacionen con buen gobierno y transparencia.

e) Funcionamiento
La información del Consejo de Transparencia y Buen Gobierno se ajustará al principio de accesibilidad, especialmente en relación con las personas que sufran alguna discapacidad.
La información difundida por el Consejo se ajustará al Esquema Nacional de Interoperabilidad, aprobado por el Real Decreto 4/2010, de 8 enero, así como a las normas técnicas de interoperabilidad.
Se fomentará que la información del Consejo sea publicada en formatos que permitan su reutilización.

Estructura orgánica

El Consejo de Transparencia y Buen Gobierno se estructura en los siguientes órganos:

1. El presidente del Consejo de Transparencia y Buen Gobierno.
2. La Comisión de Transparencia y Buen Gobierno.
3. Otros órganos: la Subdirección General de Reclamaciones y la Subdirección General de Transparencia y Buen Gobierno, como órganos jerárquicamente dependientes del presidente del Consejo.

1. Presidente del Consejo de Transparencia y Buen Gobierno

A) Funciones

El presidente del Consejo de Transparencia y Buen Gobierno, además de impulsar la acción del mismo para el cumplimiento de sus objetivos, ejerce las funciones de dirección, de gestión y de representación de dicho órgano.

Es el órgano competente para desarrollar, entre otras, las siguientes funciones:

a) Ostentar la representación legal e institucional del Consejo.
b) Adoptar criterios de interpretación uniforme de las obligaciones contenidas en la Ley 19/2013, de 9 de diciembre o en el reglamento que desarrolle dicha ley.
c) Velar por el cumplimiento de las obligaciones de publicidad y adoptar, en su caso, las medidas necesarias para el cese del incumplimiento de estas obligaciones.
d) Conocer de las reclamaciones que se presenten en aplicación del artículo 24 de la Ley 19/2013, de 9 de diciembre.
e) Responder las consultas que, con carácter facultativo, le planteen los órganos encargados de tramitar y resolver las solicitudes de acceso a la información.
f) Aprobar el anteproyecto de presupuesto del organismo.
g) Elaborar y proponer a la Comisión de Transparencia y Buen Gobierno para su aprobación el proyecto de memoria anual del organismo en el que se analice el grado de aplicación

de la Ley 19/2013, de 9 de diciembre, y se proporcione información detallada sobre el cumplimiento de las obligaciones en ella previstas.

h) Convocar y presidir las reuniones de la Comisión de Transparencia y Buen Gobierno.
i) Suscribir convenios con entidades públicas y privadas.
j) Formular y aprobar las cuentas anuales del organismo.
k) Proponer, previo informe de la Comisión de Transparencia y Buen Gobierno, modificaciones a la normativa de rango legal o reglamentario que regule las materias de competencia del Consejo.
l) Resolver recursos contra actos y las decisiones adoptadas en materias de su competencia.

B) Nombramiento y cese

El presidente del Consejo de Transparencia y Buen Gobierno será nombrado por real decreto del Consejo de Ministros a propuesta del titular del Ministerio de Hacienda y Función Pública. Con carácter previo a su nombramiento, el candidato propuesto deberá comparecer ante la comisión competente del Congreso de los Diputados que, por acuerdo adoptado por mayoría absoluta, deberá refrendar la propuesta de nombramiento en el plazo de un mes natural desde que se haya recibido la correspondiente comunicación.

El nombramiento se producirá entre personas de reconocido prestigio y competencia profesional por un periodo no renovable de cinco años.

El cese en el cargo de presidente del Consejo de Transparencia y Buen Gobierno se producirá por expiración del mandato, a petición propia o por separación acordada por el Gobierno tras la instrucción del correspondiente procedimiento por parte del titular del Ministerio de Hacienda y Función Pública por incumplimiento grave de sus obligaciones, incapacidad permanente para el ejercicio de su función, incompatibilidad sobrevenida o condena por delito doloso.

C) Independencia

El presidente del Consejo de Transparencia y Buen Gobierno desempeñará su cargo con dedicación absoluta, plena independencia y total objetividad. No estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna.

2. La Comisión de Transparencia y Buen Gobierno

A) Funciones

Corresponde a la Comisión de Transparencia y Buen Gobierno el ejercicio de las siguientes funciones, entre otras:

a) Asesorar en materia de transparencia, acceso a la información pública y buen gobierno.

b) Informar preceptivamente los proyectos normativos de carácter estatal que desarrollen la Ley 19/2013, de 9 de diciembre, o que estén relacionados con su objeto.
c) Aprobar la memoria anual del Consejo de Transparencia y Buen Gobierno.
d) Proponer al presidente la adopción de recomendaciones, directrices o guías de buenas prácticas en materia de transparencia, acceso a la información pública y buen gobierno.
e) Articular mecanismos de colaboración con órganos de naturaleza análoga a nivel autonómico o internacional.
f) Emitir informe sobre las cuestiones que le someta el presidente.
g) Aprobar el Reglamento de Funcionamiento Interno del Consejo de Transparencia y Buen Gobierno.

B) Composición

La Comisión de Transparencia y Buen Gobierno estará compuesta por un presidente, que será el del Consejo, y los siguientes Vocales:

a) Un diputado.
b) Un senador.
c) Un representante del Tribunal de Cuentas.
d) Un representante del Defensor del Pueblo.
e) Un representante de la Agencia Española de Protección de Datos.
f) Un representante de la Secretaría de Estado de Administraciones Públicas.
g) Un representante de la Autoridad Independiente de Responsabilidad Fiscal.

El Ministerio de Hacienda y Función pública trasladará al Gobierno las propuestas de nombramientos y, en su caso, ceses de los miembros de la Comisión de Transparencia y Buen Gobierno. El Gobierno efectuará dichos nombramientos o ceses, respetando el principio de presencia equilibrada de mujeres y hombres.

C) Mandato

Los vocales de la Comisión de Transparencia y Buen Gobierno desempeñarán su cargo durante cinco años, pudiendo prorrogase su mandato por un periodo de igual duración.

Serán causas de cese en su mandato:

a) Nombramiento del vocal como presidente del Consejo de Transparencia y Buen Gobierno.
b) Renuncia anticipada.
c) Pérdida de la condición que le habilitó para ser propuesto en los supuestos de diputado, de Senador o de Consejero del Tribunal de Cuentas.
d) Propuesta de cese en caso de incumplimiento sobrevenido de las condiciones que motivaron su nombramiento en el caso del representante del Defensor del Pueblo, de la Agencia Estatal de Protección de Datos, de la Secretaría de Estado de Administraciones Públicas o de la Autoridad Independiente de Responsabilidad Fiscal.

e) Expiración del mandato por incumplimiento grave de sus obligaciones, incapacidad permanente para el ejercicio de su función, incompatibilidad sobrevenida o condena por delito doloso.

D) Funcionamiento

La Comisión adoptará sus acuerdos en sesión plenaria, ostentando la Presidencia el presidente del Consejo. Actuará como secretario de la Comisión, con voz y sin voto, el titular de la Subdirección General de Transparencia y Buen Gobierno. En caso de vacante, ausencia o enfermedad, actuará de secretario un funcionario adscrito a la Subdirección General de Transparencia y Buen Gobierno designado a tal efecto por el presidente.

El presidente convocará a la Comisión de Transparencia y Buen Gobierno al menos una vez al mes. También se reunirá cuando así sea solicitado por la mayoría de sus miembros.

La Comisión quedará válidamente constituida, en primera convocatoria, si están presentes el presidente, el secretario y la mitad de sus miembros y, en segunda convocatoria, si están presentes el presidente, el secretario y la tercera parte de los miembros.

3. Otros órganos

La Subdirección General de Transparencia y Buen Gobierno y la Subdirección General de Reclamaciones son órganos administrativos dependientes del presidente del Consejo de Transparencia y Buen Gobierno para la ejecución de aquellos proyectos, objetivos o actividades que les sean asignados, así como de la gestión ordinaria de los asuntos de su competencia.

Los Subdirectores Generales titulares de ambas serán nombrados y cesados por el presidente del Consejo de Transparencia y Buen Gobierno.

Los nombramientos se efectuarán entre funcionarios de carrera de la Administración General del Estado y, en su caso, de otras Administraciones públicas cuando así lo prevean las normas de aplicación, y que pertenezcan a Cuerpos y Escalas, a los que se exija para su ingreso el título de doctor, licenciado, ingeniero, arquitecto o equivalente.

Las Unidades y puestos de trabajo dependientes de las Subdirecciones Generales mencionadas se determinarán en las correspondientes relaciones de puestos de trabajo.

La Subdirección General de Transparencia y Buen Gobierno

La Subdirección General de Transparencia y Buen Gobierno tiene encomendadas, entre otras, las siguientes funciones:

a) Supervisar el cumplimiento de las obligaciones de publicidad activa contenidas en la Ley 19/2013, de 9 de diciembre.

b) Proponer al presidente la adopción de criterios de interpretación uniforme de las disposiciones previstas sobre publicidad activa en la Ley 19/2013, de 9 de diciembre.
c) Tramitar cuantas cuestiones y consultas le sean planteadas en relación a las materias de transparencia y buen gobierno.

La Subdirección General de Reclamaciones

La Subdirección General de Reclamaciones es el órgano del Consejo de Transparencia y Buen Gobierno que desempeña las competencias inherentes a la tramitación de la reclamación prevista en el artículo 24 de la Ley 19/2013, de 9 de diciembre. Asimismo, le corresponde tramitar las consultas que, con carácter facultativo, puedan presentarse ante el Consejo, relativas a la aplicación de las disposiciones reguladoras del derecho de acceso a la información pública.

12.4. Seguridad de la información y ciberseguridad

12.4.1. Introducción

Los empleados de Correos disponen de los recursos tecnológicos necesarios y del acceso a sistemas y herramientas informáticas con la finalidad de facilitar las tareas diarias, fomentar la comunicación, optimizar los envíos, hacer un tratamiento adecuado de la información, etc., exclusivamente con fines laborales. La disponibilidad de los sistemas, la confidencialidad de la información y la imagen corporativa de Correos dependen del uso correcto, legítimo y responsable de estos recursos. De la misma forma, el uso inadecuado de estas herramientas puede implicar consecuencias que afecten al propio usuario, a otros usuarios o, incluso, a la imagen de Correos.

Un incidente de seguridad implicaría un riesgo de pérdida de información de los clientes o empleados de Correos y un deterioro en la imagen de la compañía. Por este motivo, Correos debe establecer todas aquellas medidas necesarias para evitar cualquier incidente de seguridad, incluyendo, entre esas medidas, la **adopción de unas buenas prácticas en materia de seguridad de la información** por parte de todos los empleados que ayuden a preservar el mayor activo de Correos: la información.

Para garantizar la seguridad de la información, todos los empleados de Correos (empleados de oficinas, técnicos de sistemas, comerciales, gestores de datos/procesos, transportistas, etc.) deberán asumir un **rol de seguridad** proporcional a las responsabilidades que desarrollan, asumiendo unas nociones básicas en materia de seguridad de la información que ayuden a optimizar la seguridad en los procesos de trabajo de Correos.

¿Qué es la ciberseguridad?

En el mundo en el que nos encontramos donde la digitalización, el uso de internet y los dispositivos está muy extendido y normalizado, es fundamental proteger uno de los activos más importantes de la actualidad: la información. Para ello, debemos adoptar medidas técnicas, organizativas, jurídicas y humanas de manera transversal que nos permitan reducir los riesgos que puedan comprometerla.

En este contexto, es importante conocer los conceptos de seguridad de la información y ciberseguridad y sus matices y diferencias:

La seguridad de la información, por su parte, busca proteger la información en cualquier formato (físico o digital) ante posibles riesgos como ataques materiales e inmateriales (informáticos o incendios, por ejemplo).

El avance de la tecnología en los últimos años ha generado un uso incalculable de dispositivos con conexión a internet y un volumen enorme de información y datos, lo que da lugar a la necesidad de proteger la información en el entorno digital de manera mucho más específica. El incremento constante del volumen de ciberataques, la influencia humana en los mismos (según un estudio realizado por IBM, un 95% de las incidencias en ciberseguridad son originadas por errores humanos) o el impacto que puedan tener en las empresas ocasionando pérdidas económicas descomunales, interrupciones de las tareas operativas o fugas de información dan prueba de su impacto y necesidad.

Por tanto, la **ciberseguridad** es el conjunto de medidas de protección de la información en formato digital (ordenadores, servidores, móviles, PDA o cualquier dispositivo conectado a internet que tenga acceso a información o la almacene) alojada en sistemas de información interconectados, vulnerables a los ciberataques.

Glosario

Se destacan los siguientes términos clave que todo empleado debe conocer en materia de ciberseguridad:

Activo. Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos.

Amenaza. Circunstancia desfavorable que tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Autenticación. Procedimiento para comprobar que alguien es quien dice ser cuando accede a un ordenador o a un servicio *online.*

Impacto o consecuencia de una amenaza sobre un activo. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo.

Incidente de seguridad. Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa. Tiene origen en el acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad de la información de la compañía.

Ingeniería social. Tácticas utilizadas para obtener datos de naturaleza sensible de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

***Malware*.** Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

Phishing*.** Denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir información confidencial de usuarios legítimos (contraseñas, datos bancarios, etc.) de forma fraudulenta. Hay diferentes modalidades: ***smishing, si se realiza a través de SMS y ***vishing*** si se realiza a través voz.

Política de seguridad. Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

***Ransomware*.** Situación en la que el ciberdelincuente toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

Riesgo. El nivel de riesgo es una estimación de lo que puede ocurrir y se valora, de forma cuantitativa, como el producto del impacto (consecuencia) asociado a una amenaza (suceso), por la probabilidad de la misma.

Suplantación de identidad. Actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.

Vulnerabilidad. Debilidad que presentan los activos y que facilita la materialización de las amenazas.

Glosario

CID (confidencialidad, integridad y disponibilidad): Unidad de Reparto Ordinario.

Área de Seguridad de la Información

Con el objetivo de proteger la información de la compañía y de los clientes y de minimizar el riesgo de ciberseguridad, Correos ha desarrollado diferentes estrategias para gestionar la seguridad de la información, que funcionan como factor diferencial frente a otras empresas del sector.

Los ámbitos operativos del área de seguridad son los siguientes:

- Seguridad de redes y comunicaciones.
- Seguridad de sistemas y criptografía.
- Gestión frente a ciberamenazas y seguridad analítica.
- Control de acceso a la información.
- Auditoría y continuidad IT (Tecnología de la Información).
- Normativa, conformidad y comunicación.

Las estrategias del Área de Seguridad de la Información responden al compromiso de Correos con los clientes, pero también con la sociedad, en tanto que están orientadas a luchar contra el fraude (desde el punto de vista ténico y humano), a impulsar el negocio digital y los valores de la marca, a ofrecer servicios IT confiables y a promover la cultura de la ciberseguridad (para el personal de Correos y para los clientes). Entre las acciones dirigidas al personal de Correos se cuentan las siguientes:

- La difusión de materiales adaptados: alertas sobre fraudes, boletines con noticias y consejos, argumentarios para personal de atención al cliente, infografías explicativas sobre tipos de fraude, manuales de buenas prácticas, etc.
- La oferta de formaciones: charlas de concienciación, formaciones regladas, etc.
- Comunicaciones dirigidas al cliente para visibilizar el trabajo del área y como labor de concienciación social.

Cultura de ciberseguridad

Programa de ciberseguridad y cultura en Correos

Correos ofrece a su personal un programa de formación y concienciación en el que se pretende extender buenas prácticas para desarrollar una cultura de ciberseguridad. Este programa también desarrolla acciones dirigidas a clientes y a la sociedad en general.

Objetivos:

- Resolver problemas identificados, con acciones y criterios concretos.
- Alinear a los participantes con la estrategia de la compañía.
- Informar, formar y concienciar al usuario en tiempo y forma.
- Crear cultura de ciberseguridad.
- Cambiar conductas y comportamientos del usuario.

Formación en Seguridad de la Información para los empleados de Correos

Los empleados tienen un rol central en la seguridad en las empresas, ya que ellos son los que gestionan y utilizan los dispositivos tecnológicos de Correos para tratar el activo más importante de la compañía: la información.

Por esa razón Correos asume la responsabilidad de concienciar y formar al personal en materia de seguridad de la información. Esta formación crea una cultura de seguridad en la empresa, que sirve para establecer las bases de la protección de la información confidencial de Correos y de la información de los clientes y proveedores.

Estas medidas de seguridad, además de tener como objetivo central la prevención de ciberataques contra la compañía, están orientadas a cultivar en los empleados de Correos unas buenas prácticas en todo lo relacionado a la gestión de la información en sus tareas diarias. Para poder optimizar la seguridad en los procesos de trabajo, cada empleado deberá adquirir unas nociones básicas sobre seguridad de la información y velar, desde su rol dentro de la empresa, por la protección de esta, ya sea a partir de un uso adecuado tanto de los ordenadores y de las herramientas digitales como de la información en formato físico.

Algunas de las acciones llevadas a cabo en el marco de la ciberseguridad son:

- Formación en seguridad para empleados y empleadas.
- Establecimiento de políticas, normativas y procedimientos de seguridad.
- Supervisión de que se cumplen las buenas prácticas.
- Sensibilización y concienciación en seguridad para empleados.

Información de referencia y política de seguridad

Las políticas, normativas y procedimientos de seguridad aplicables en Correos surgen a partir de la gestión del Comité de Seguridad de la Información, el órgano de la compañía encargado de salvaguardar y fortalecer las actividades relacionadas con el manejo de la información.

El comité establece las políticas de seguridad a emplear en el tratamiento de la información y, además, coordina todas las actividades relacionadas con la misma. De ese modo, con el fin de gestionar de forma segura la información de la que dispone Correos, se han constituido los siguientes objetivos estratégicos y normativas obligatorias sobre Seguridad de la Información:

- Mantener unos niveles de seguridad —en términos de confidencialidad, integridad y disponibilidad— coherentes con las necesidades del negocio y la confianza de los clientes.
- Asegurar el funcionamiento del Comité de Seguridad Corporativo.
- Implantar las medidas técnicas y organizativas que proporcionan el nivel de seguridad adecuado para tratar la información y garantizar el cumplimiento del marco legal vigente.

- Difundir el marco normativo de Seguridad de la Información y promover la formación y concienciación en esta materia a todo el personal de Correos.
- Mantener un Sistema de Gestión de la Seguridad de la Información basado en estándares internacionales para identificar, cuantificar, priorizar y tratar los riesgos, así como para evaluar y revisar el desarrollo de la política de seguridad de la información como marco de definición de las directrices básicas de seguridad.

Los principales requisitos legales, regulatorios y normativos alcanzan el ámbito de la propiedad intelectual, tanto a nivel nacional como comunitario en las siguientes normativas:

- **Reglamento (EU) 2016/679** del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- **ISO 27001.** Esta certificación muestra el compromiso de Correos con garantizar las buenas prácticas en la seguridad de la información de que dispone, conociendo, gestionando y minimizando los riesgos y protegiendo a la empresa de las amenazas contra la información. El estándar de seguridad ISO 27001/27002 es un referente para establecer las medidas de seguridad a implantar en un tratamiento de la información, y abarca aspectos como el control de acceso a sistemas de información e instalaciones, las comunicaciones, la seguridad en la operación, el respaldo de la información, la seguridad en los RR. HH. y los proveedores.

12.4.2. Buenas prácticas y hábitos en el puesto de trabajo

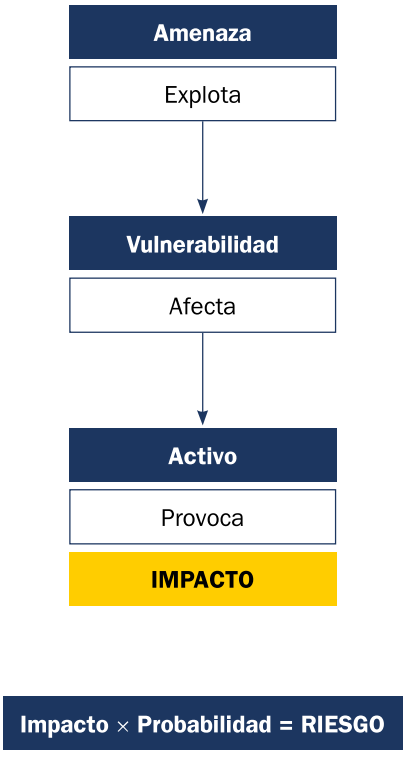
Correos dispone de un marco de seguridad de la información y un área de seguridad multidisciplinar (Área de Seguridad de la Información), con una gran experiencia, que son los que determinan las medidas a implantar en los sistemas de información y procesos de la compañía.

El Área de Seguridad de la Información no solo trabaja para implementar las medidas técnicas que velen por la seguridad de los sistemas e información de Correos, sino que marca unas recomendaciones generales a seguir por cada usuario de la organización para el desarrollo de unas buenas prácticas en el puesto de trabajo. Estas medidas de seguridad son el conjunto de procedimientos, controles y mecanismos técnicos que reducen o eliminan el riesgo. Pueden actuar de dos formas distintas:

- Reduciendo la probabilidad de que se manifieste la amenaza.
- Limitando el daño causado por esta.

Otra parte fundamental de la seguridad consiste en conocer los riesgos a los que está sometida la información y los efectos que una amenaza produce en cada una de las dimensiones de la información (confidencialidad, integridad, disponibilidad, etc.).

Cuando se habla de riesgo, se hace referencia al grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Cuanto mayores sean el daño ocasionado y la probabilidad de que la amenaza ocurra, mayor será el riesgo del activo, ocasionando daños personales, pérdidas financieras, interrupciones del servicio, pérdida de reputación y disminución del rendimiento.



Impacto × Probabilidad = RIESGO

Gestión de los dispositivos electrónicos

La PDA es el dispositivo utilizado por los carteros de Correos en el que se recoge toda la información relativa a clientes, envíos, datos personales, firmas, etc. A través de este dispositivo, el empleado de Correos maneja diariamente una gran cantidad de datos. Para proteger esta información, se deberá tener en cuenta lo siguiente:

- No se deberá conectar con la PDA a redes públicas, ya que podría ocurrir un robo de información confidencial.
- Habrá que bloquear la PDA siempre que no se esté utilizando; de esta forma, si se sufre un robo o pérdida, no se podrá acceder a la información.

- Habrá que utilizar una contraseña robusta de acceso a la PDA. No se compartirá con nadie y no se reutilizará.
- Se seguirán siempre las recomendaciones del Área de Seguridad de la Información.
- Se comunicará al CAU (Centro de Atención al Usuario) cualquier incidente de seguridad (robo o pérdida) mediante los canales oficiales y a la mayor brevedad posible.

Protección física de los datos

Información en papel

La información en papel puede resultar vulnerable en tanto que es fácilmente accesible para un usuario no autorizado. Para minimizar los riesgos de seguridad, se sugieren las siguientes recomendaciones:

- Custodiar la documentación en todo momento e impedir que personas no autorizadas puedan acceder a la información que contiene.
- No dejar la información accesible a terceras personas en la mesa de trabajo, en la impresora o en el fax.
- Guardar y almacenar la documentación de forma ordenada en armarios y cajones cerrados con llave.
- Destruir manualmente los documentos, usar destructoras de papel o los medios que Correos pone a disposición para hacerlo de forma segura.

Protección física de datos

La seguridad de los datos busca proteger la información de Correos que se usa a diario para evitar el acceso de terceros a los dispositivos y a la información sensible o la suplantación de la identidad.

Para evitar riesgos como estos, se recomienda a los empleados de Correos seguir una rutina de buenas prácticas como las que se mencionan a continuación:

- Seguir una política de mesas limpias. Mantener el espacio de trabajo ordenado y despejado, sin papeles, dispositivos extraíbles, etc.
- Bloquear siempre el dispositivo mientras no se esté utilizando (pulsando las teclas Windows + L) y guardarlo en un lugar seguro al finalizar la jornada laboral.
- No anotar contraseñas en papel ni compartirlas con nadie.
- Evitar dejar información o datos personales a la vista de posibles miradas indiscretas.
- Al finalizar la jornada, guardar los documentos en papel en un lugar seguro.
- Evitar reutilizar documentos en papel que contengan datos de clientes, facturas, etc.
- No abandonar documentos en impresoras o escáneres.
- Utilizar las destructoras para deshacerse de la documentación que ya no se necesite.

Uso del identificador de usuario y gestión de contraseñas

Los usuarios y contraseñas son las señas de identidad de los empleados de Correos en el sistema y son personales e intransferibles. Los empleados son responsables de las acciones que se realizan con ellos. Ante esto, es necesario protegerlos de posibles robos siguiendo estas recomendaciones:

- No comunicar la contraseña a nadie y no escribirla en ningún sitio.
- Ante la sospecha de que alguien conoce la contraseña de acceso, modificarla.
- Cambiar la contraseña periódicamente, como mínimo una vez al año.
- Recordar que una contraseña segura se compone, como mínimo, de ocho caracteres alfanuméricos, incluyendo letras mayúsculas, minúsculas, dígitos y signos de puntuación.
- Al crear una nueva contraseña, no utilizar información previsible, nombres comunes fáciles de adivinar o palabras que se puedan encontrar en el diccionario. El 90% de las contraseñas son vulnerables porque el usuario utiliza formatos sencillos y fáciles de recordar.

Buenas prácticas y rutinas en el puesto de trabajo

Según lo visto, la protección de la información de Correos depende tanto de la protección de la información almacenada en dispositivos como de la información alojada en elementos físicos. Por lo tanto, desde que el empleado o empleada comienza a utilizar los dispositivos al inicio de la jornada hasta que los apaga, debe seguir las buenas prácticas de ciberseguridad para evitar riesgos como:

- **Acceso a los dispositivos y a la información** a través de dispositivos sin supervisión o desbloqueados.
- **Suplantación de identidad**, a partir de una mala gestión de las claves de acceso de los dispositivos.

Suplantación de marca

Las organizaciones como Correos suelen ser objeto de suplantación de marca por parte de los ciberdelincuentes, que utilizan la imagen de empresas o instituciones de prestigio como señuelo para engañar a sus víctimas.

La suplantación de marca puede llevarse a cabo mediante diferentes técnicas, siendo las más conocidas el *phishing, smishing, vishing* o el robo de identidad empresarial. El objetivo principal es el robo de datos personales o la descarga de *malware,* un programa malicioso que se instala en nuestro dispositivo al descargarnos un archivo adjunto para infectarlo, robar la información o acceder a otros dispositivos de la empresa.

Phishing

El *phishing* es una técnica de ciberdelincuencia que utiliza el fraude y el engaño para manipular a sus víctimas y hacer que revelen información personal confidencial por correo electrónico.

Las campañas de *phishing* que utilizan la marca Correos como señuelo para engañar a clientes y ciudadanos son habituales, pero no por ello pierden efectividad ya que los ciberdelincuentes trabajan en mejorar sus técnicas y desarrollan acciones cada vez más difíciles de detectar. Las campañas de *phishing* más habituales con la marca Correos son aquellas en las que se solicita completar la dirección de entrega o pagar tasas de aduana para recibir un paquete, entre otras.

Es importante recordar que Correos nunca solicita datos personales o bancarios por correo electrónico, ni tampoco realizar pagos *online* para la recepción de un paquete.

Smishing y *vishing*

Otras técnicas de fraude en la misma línea que el *phishing,* pero con diferentes vectores de entrada, son el *smishing* y el *vishing.*

El *smishing* es una suplantación de identidad a través de SMS. Normalmente, en el SMS que recibimos en nuestro dispositivo móvil aparece un enlace para ejecutar una acción. Si pulsamos en el enlace, nos conducirá a una página web fraudulenta en la que se solicitarán nuestros datos.

El *vishing* también es una suplantación de identidad, pero, en este caso, mediante una llamada de voz. El interlocutor se hace pasar por un empleado de una empresa de confianza para solicitar datos personales o credenciales de acceso a los sistemas. Normalmente se utiliza la urgencia para que la víctima del fraude realice la acción lo antes posible.

Consejos para evitar caer en el fraude

- **Verificar** la **identidad del remitente** o de la **persona que nos llama,** así como la **dirección de *e-mail.***
- **Contactar** personalmente con la **entidad** antes de acceder o responder a algún enlace de un correo sospechoso.
- **Prestar atención al tono.** Es común que se use un **tono de urgencia** para que la víctima del fraude no tenga tiempo de pensar (por ejemplo, simulando falsas emergencias repentinas) o un **tono de amenaza** si la víctima no realiza la acción solicitada.
- **Desconfiar** de mensajes de **regalos, descuentos** y **sorteos,** así como de correos que contengan **imágenes** con **mala calidad** o **faltas de ortografía.**
- **Evitar** hacer **clic en enlaces** o **descargar adjuntos** en mensajes sospechosos.

- **No facilitar información personal** en páginas sospechosas.
- **Permanecer atento** a mensajes sospechosos a través de **redes sociales** o **aplicaciones de mensajería instantánea,** canales que también suelen utilizar los ciberdelincuentes.

Robo de identidad empresarial

El robo de identidad empresarial consiste en asumir la identidad de una compañía a través de la copia o clonación de su dominio, portal web, marca o aplicaciones móviles.

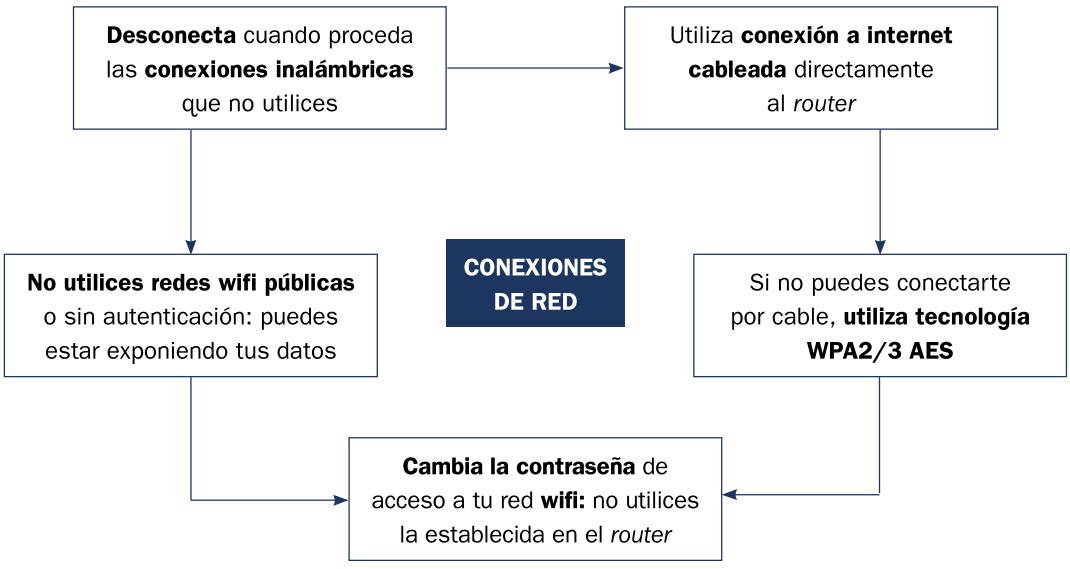
Los denominados sitios espejo son un fenómeno cada vez más recurrente por los ciberdelincuentes, que clonan la estructura de la web original con las mismas imágenes, colores, contenido, etc., de tal forma que a los usuarios les resulta muy difícil distinguir entre la página web original y la falsa. Una vez dentro de la página falsa, la víctima realizará las acciones habituales que acostumbra a hacer, introduciendo su usuario y contraseña en primer lugar para autenticarse. Al introducir estos datos, pasarán a manos de los ciberdelincuentes.

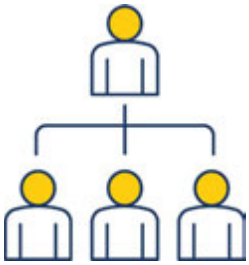
Consejos para evitar caer en páginas falsas

- **Verificar** siempre que la **conexión** sea **segura** y que aparezca el **icono de candado** junto con las letras **https://.**
- **Revisar** que el dominio se corresponda con el **dominio original** y que no aparezca alguna mayúscula o alguna letra de más. Por ejemplo: www.correoos.es o www.correOs.es

Navegación

Recomendaciones de conexión





Se recomienda seguir las recomendaciones que se enumeran a continuación para garantizar una sesión de navegación segura:

- Exclusivamente acceder a páginas cuyos datos viajen cifrados (la URL debe empezar por https).
- No iniciar sesión (usuario/contraseña) en ningún servicio mientras se esté conectado a una red pública.
- Evitar realizar transacciones bancarias, compras *online* o cualquier otra tarea que suponga el intercambio de datos privados desde redes wifi públicas.
- Tras la conexión, eliminar los datos de la red memorizados en el equipo.

Cómo actuar ante un incidente de seguridad

¿Cómo actuar ante un incidente de seguridad?

Si el empleado de Correos detecta cualquier incidente de seguridad, podrá reportarlo a través de cualquiera de estos dos canales:

- En el **botón «Informar sobre correo de *phishing*» de su correo electrónico.**
- En el **buzón de uso exclusivo interno.** Será importante recordar que este buzón es exclusivamente interno y por lo tanto no debe facilitarse ni a clientes ni a personal ajeno a Correos.

La detección y comunicación de un incidente de seguridad es esencial para su resolución temprana. Si no se lleva un protocolo y gestión del incidente adecuado las consecuencias podrían ser:

- Daños reputacionales y de imagen.
- Pérdidas económicas.
- Pérdida de confianza.
- Consecuencias legales.

Otros dominios relevantes

El desarrollo veloz de las nuevas tecnologías ha generado un impacto masivo en el intercambio de información, no solo en ámbitos laborales, sino también en la esfera de la vida privada. Por esta razón, será de crucial importancia que los empleados de Correos incorporen las rutinas de ciberseguridad en su uso diario de la tecnología para garantizar la protección de la información almacenada en dispositivos electrónicos o en soportes físicos. De esta forma, las buenas prácticas en materia de seguridad se trasladarán con naturalidad al quehacer diario en los puestos de trabajo.

A continuación, se enumeran una serie de recomendaciones adicionales que son importantes que las conozcan todos los empleados y empleadas de Correos con la finalidad de aumentar su nivel de seguridad.

Correo electrónico

Para **evitar incidentes de seguridad** derivados del uso erróneo o inadecuado del correo electrónico a la hora de enviar mensajes, habrá que tener en cuenta las siguientes recomendaciones:

- Antes de enviar un correo electrónico, comprobar el destinatario y la información que se envía.
- No responder correos de SPAM ni reenviar mensajes cadena.
- No difundir la clave de acceso del *e-mail.*
- Utilizar métodos corporativos para enviar información de forma segura y cifrar los archivos antes de enviarlos para garantizar la confidencialidad.
- Facilitar la dirección de correo electrónico solo a personas conocidas.
- No abrir mensajes de correo de origen desconocido; eliminarlos directamente para evitar el robo de datos personales o la descarga de *malware* a través de técnicas de cibercrimen como el *phishing, smishing* o *vishing* ideadas para suplantar la identidad del usuario o para robarle información a través de correos electrónicos falsos.
- No clicar en los enlaces que aparecen en los correos electrónicos, no descargar archivos adjuntos ni introducir datos personales a través de ningún enlace.
- Al navegar en sitios web, verificar que la conexión sea segura y que aparezca el icono de candado junto a las letras https://; la presencia de estas letras al comienzo de una URL son un indicador de que los datos viajan cifrados.
- Revisar que el dominio se corresponda con el dominio original de la página en la que se navegará y que no aparezca alguna mayúscula, letra o número de más. Por ejemplo: www.correoos.es o www.corre0s.es
- Cuando sea posible, no utilizar redes wifi públicas o sin autenticación, para evitar exponer los datos personales. Si se navegara utilizando una red pública, no iniciar sesión en ningún servicio que requiera el uso de un usuario y una contraseña (transacciones bancarias, compras *online,* etc.).
- Tras la conexión, eliminar los datos de la red memorizados en el ordenador.
- Al utilizar una red privada de wifi, reemplazar la contraseña del *router* por una contraseña segura.

Glosario

Spam: Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Wifi pública

La conexión a redes públicas

Al conectarse a las redes wifi públicas se asumen grandes riesgos, ya que se exponen los datos personales, el tráfico y la identidad de forma casi total. El riesgo se incrementa si se utiliza este tipo de redes para acceder o intercambiar información de valor o confidencial.

El problema con este uso de las redes públicas es que existen **redes fraudulentas** que simulan ser redes reales (en hoteles, estaciones de tren, aeropuertos, etc.) para espiar

o robar la información personal. Es importante tener en cuenta estos consejos antes de conectarse a una red pública:

- Deshabilitar cualquier proceso de sincronización del equipo si se va a usar una red pública.
- Mantener siempre el equipo actualizado, con el antivirus instalado correctamente.

La nube

Los servicios en nube son servidores *online* que permiten tener disponible la información las 24 horas del día para todos los usuarios que tengan acceso, por lo que compartir ficheros, realizar modificaciones sobre los mismos o descargar la documentación hace que mejore la relación de trabajo de los equipos.

Los servicios en nube son una opción cada vez más utilizada para tener copias de seguridad disponibles sin necesidad de un disco duro físico, por lo que hay que tener en cuenta una serie de recomendaciones que mitiguen cualquier riesgo al que la información se pueda ver expuesta:

- Utilizar exclusivamente servicios en nube que estén comprometidos con la política de privacidad de la Unión Europea.
- Configurar las opciones de seguridad que brinde el servicio (doble factor de autenticación, compartición de archivos, etc.).
- Almacenar de forma cifrada los ficheros que se compartan con información personal o confidencial.
- No almacenar la información únicamente en la nube; disponer de un medio alternativo de copia/recuperación.

Recomendaciones en el uso de las redes sociales

En los últimos años, la popularización de las redes sociales (Twitter, Facebook, Instagram) ha creado un entorno de exposición constante de datos de carácter personal en internet, por lo que los usuarios se han vuelto vulnerables al robo o uso privilegiado de su información por parte de usuarios no autorizados, a veces, incluso, sin ser conscientes de ello, por lo que es recomendable seguir estos consejos:

- No utilizar la cuenta corporativa para asuntos personales.
- Tener cuidado al compartir información: los datos de los empleados y los de Correos son muy valiosos.
- Aceptar únicamente a usuarios conocidos.
- Evitar exponer a menores.
- No compartir la ubicación bajo ningún concepto.
- Denunciar las conductas abusivas o sospechosas.

12.4.3. Decálogo de seguridad

Correos ha desarrollado, como medida preventiva, un decálogo básico que los empleados deben recordar con el objetivo de saber cómo reaccionar ante los principales desafíos de seguridad que se originan en el desempeño normal de sus funciones:

Para conocer las bases de la convocatoria, consúltese
https://www.correos.com/personas-y-talento/#convocatorias-publicas