# POLÍTICA DE PROTECCIÓN DE DATOS v7.0

## Tabla de contenido

## 1. Historial de revisiones

| Versió | Fecha | Autor | Resumen de cambios |
|---|---|---|---|
| 7.0 | Marzo 2025 | Diana Stirbu | • Se agregó 'Tabla de contenido' para una navegación más sencilla.<br>• Se modificaron todas las referencias de responsable de Protección de Datos a Gerente de Gobernanza de la Información cuando correspondía.<br>• Se agregó una cláusula que describe el marco y los roles de gestión de la gobernanza de la información.<br>• Se agregó un requisito para que todo el personal informe las solicitudes de acceso a información dentro de un día hábil.<br>• Se eliminó la referencia obsoleta al caso Schrems II.<br>• Se agregó una sección que describe el requisito de registrar de forma central y "actualizar" periódicamente el consentimiento del titular de los datos.<br>• Se agregó nueva sección de Inteligencia Artificial.<br>• Se eliminaron referencias obsoletas a las políticas de seguridad de TI y redes sociales.<br>• Se amplió la cláusula de auditoría para aclarar más cómo se supervisará el cumplimiento.<br>• Se eliminaron o cambiaron algunas oraciones para mayor brevedad o mayor claridad para el lector. |

## 2. Introducción

2.1. Esta política regula la adquisición, el almacenamiento, el procesamiento, la compartición y la eliminación adecuada de datos personales por parte de la Universidad Dō. En adelante, en este documento, las referencias al Grupo de la Universidad Dō se simplificarán a «Grupo». El alcance de esta política incluye a todas las personas, la información, las tecnologías, los recursos y las instalaciones que gestionan información relativa a una persona identificable, directa o indirectamente.

2.2. Esta política no formará parte del contrato laboral formal, pero es condición para el empleo que el personal cumpla con las normas y políticas establecidas por el Grupo. El incumplimiento de esta política podrá dar lugar a procedimientos disciplinarios.

2.3. Cualquier miembro del personal que considere que no se ha seguido la política con respecto a los datos que se conservan sobre él debe plantear el asunto al Gerente de Gobernanza de la Información. Si tiene alguna duda, también puede consultar el sitio web de la Oficina del Comisionado de Información para obtener más información.

2.4. El Grupo debe recopilar datos sobre su personal, estudiantes, clientes y otros usuarios para poder supervisar su rendimiento, logros, salud y seguridad. También es necesario procesar estos datos para poder pagar al personal, organizar cursos y cumplir con las obligaciones legales con los organismos de financiación y el gobierno.

2.5. Los datos también se hacen públicos a través de redes sociales y correos electrónicos. Por lo tanto, la seguridad de los datos transferidos por estos medios también está sujeta a los principios de protección de datos.

2.6. En la gestión diaria de datos, el Grupo se adherirá a los principios de protección de datos prescritos por la legislación vigente en materia de protección de datos y la normativa asociada.

2.7. Es un requisito que el Grupo sea responsable y pueda demostrar el cumplimiento de los principios de protección de datos detallados en la sección 3.1 a continuación, como, así como con los principios, derechos y requisitos para el tratamiento de datos personales del apartado 3 siguiente.

## 3. Principios, derechos y requisitos para el tratamiento de datos personales

3.1. El término «tratamiento» en este contexto tiene la misma definición que el artículo 4(2) del RGPD del Reino Unido.

3.2. El Grupo debe contar con una base legal válida para el tratamiento de datos personales. Estas son:

- Cumplimiento de obligaciones contractuales.
- Cumplimiento de obligaciones legales o de derecho consuetudinario.
- Para proteger la vida de alguien.
- Para que una organización cumpla su tarea pública.
- Los llamados "intereses legítimos", en los que los datos personales se utilizan de maneras que los individuos esperarían razonablemente que se utilizaran y que tienen un impacto mínimo en la privacidad.

- Consentimiento explícito basado en una declaración de consentimiento muy clara y específica por parte de la persona. Existen otras normas en torno al consentimiento, como la exigencia de consentimiento expreso y la simplificación de la revocación del mismo. El consentimiento solo debe utilizarse cuando el Grupo no pueda basarse en una base legal alternativa. El consentimiento puede revocarse fácilmente con un aviso mínimo.

3.3. Todos los datos personales deberán ser:

- Obtenidos y tratados de forma lícita, justa y transparente.
- Se obtendrán con fines determinados y legítimos y no serán tratados ulteriormente de ninguna manera incompatible con dichos fines.
- Adecuadas, pertinentes y limitadas a lo necesario en relación con los fines para los que son tratadas
- Preciso y actualizado.
- Conservados en una forma que permita la identificación de los interesados durante no más tiempo del necesario para los fines para los que se tratan los datos personales.
- Procesados de manera que se garantice la seguridad adecuada de los datos personales, incluida la protección contra el procesamiento no autorizado o ilícito, así como contra su pérdida, destrucción o daño accidental, mediante medidas técnicas u organizativas apropiadas.
- No se transferirán a otra parte, como una empresa que procesa nuestros datos en nuestro nombre o un socio comercial, a menos que puedan proporcionar evidencia de que cumplen con los principios de la sección 3.1 y los principios completando la lista de verificación del contrato, los derechos y los requisitos en la sección

2. Todos los contratos con dichas partes incluirán los términos estándar que incluyen el cumplimiento de la legislación de protección de datos o harán referencia a un acuerdo de intercambio de datos establecido.

3.4. Derechos de las personas cuyos datos personales son tratados por el Grupo. Las personas tienen derecho a:

- Ser informado sobre la recopilación y uso de sus datos personales.
- Acceder a sus datos personales e información complementaria.
- A que se rectifiquen los datos personales inexactos o se completen si son incompletos.
- A tener borrados sus datos personales.
- Solicitar la restricción o supresión de sus datos personales.
- Para obtener y reutilizar sus datos personales para sus propios fines en diferentes servicios.
- Oponerse al tratamiento basado en «intereses legítimos»; para fines de marketing directo y para determinados tipos de investigación.
- Para impugnar la toma de decisiones automatizada y la elaboración de perfiles.

3.5. Violaciones de datos personales

- Todos los involucrados en el Grupo tienen la responsabilidad de proteger los datos personales de las personas que interactúan con el Grupo.
- Se espera que todos los usuarios del Grupo estén atentos a posibles infracciones de esta política. Si tienen conocimiento o sospechan de alguna infracción, deberán informarla INMEDIATAMENTE al responsable de Gobernanza de la Información.

- Todos los usuarios del Grupo deben estar especialmente atentos a cualquier evento que ponga en riesgo sus datos personales al infringir cualquiera de los principios de las secciones 2 y 3.1 de esta política. Es más probable que estas infracciones ocurran tras una vulneración de la seguridad de los sistemas informáticos. Sin embargo, esta no es la única forma en que los datos personales pueden estar en riesgo. Existen plazos estrictos para informar sobre cualquier infracción de este tipo a las personas afectadas y a las autoridades competentes. Por lo tanto, es imperativo que cualquier infracción, real o presunta, se notifique INMEDIATAMENTE al responsable de Gobernanza de la Información.

**4. Notificación de datos conservados y tratados**

4.1. Todo el personal, estudiantes, clientes y cualquier persona sobre la que el Grupo procese datos personales deberá:

- Conozca qué información conserva y procesa el Grupo sobre ellos y por qué.
- Sepa cómo acceder a los datos almacenados.
- Tenga en cuenta los procedimientos establecidos para mantener los datos actualizados.
- Conozca qué está haciendo el Grupo para cumplir con sus obligaciones bajo la legislación de Protección de Datos y la normativa asociada.
- Sepa cómo contactar al Gerente de Gobernanza de la Información y cómo presentar cualquier queja ante la Oficina del Comisionado de Información.

4.2. Recursos Humanos solicitará a todo el personal que revise anualmente sus datos personales almacenados en la base de datos de Recursos Humanos, utilizando la función de autoservicio de RR.HH.

4.3. Los estudiantes que deseen consultar y actualizar sus registros deberán hacerlo consultando a su tutor pastoral o visitando el centro de estudiantes.

## 5. Responsabilidades del personal

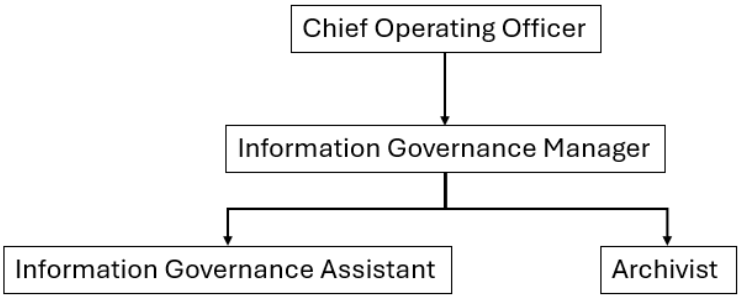
5.1. Todo el personal será responsable de:

- Cumplir plenamente con los principios, derechos y requisitos de protección de datos (3 y 4.1) en el tratamiento de datos personales.
- Realizar una Evaluación de Impacto de Protección de Datos cuando se prevea un nuevo tratamiento de datos personales.
- Plantear de inmediato inquietudes sobre protección o seguridad de datos ante el Gerente de Gobernanza de la Información.
- Garantizar que todos los datos que proporcionan al Grupo en relación con su empleo sean precisos y estén actualizados y que los cambios se realicen directamente en el autoservicio de RR.HH., cuando sea pertinente, o se notifiquen a Recursos Humanos mediante los formularios correspondientes.
- Revisar la información que el Grupo mantiene anualmente y corregir cualquier error.
- Todo el personal es personalmente responsable de mantener la seguridad de los datos personales.

5.2. Cualquier dato personal de otras personas que recopile un miembro del personal, como calificaciones o notas de cursos, referencias a empleadores u otras instituciones académicas, o cualquier información sobre circunstancias personales, deberá recopilarse y almacenarse de acuerdo con las directrices incluidas en el Manual del Personal, la Política de Protección de Datos y la Política de Conservación de Registros.

## 6. Marco de gobernanza de la información

6.1. La Gobernanza de la Información del Grupo se logra mediante un enfoque estructurado, tal como se describe en el siguiente marco:




- El responsable de Gobernanza de la Información es el responsable de la protección de datos del Grupo. A efectos de los artículos 37 a 39 del RGPD del Reino Unido, el responsable de Gobernanza de la Información es el delegado de Protección de Datos del Grupo.
- El Equipo de Gobernanza de la Información está compuesto por el Gerente de Gobernanza de la Información, el Asistente de Gobernanza de la Información y el Archivista del Grupo. Puede contactar con el equipo de Gobernanza de la Información a través de admin@vae-universityuk.uk o visitando la oficina de Gobernanza de la Información en el campus de la Universidad Dō.
- Los Propietarios de Activos de Información son miembros relevantes del personal responsables de uno o más activos de información identificados. Los Propietarios de Activos de Información se describen en la Política de Retención de Registros.
- El director de Operaciones es el miembro del Equipo de Liderazgo del Grupo responsable de la supervisión ejecutiva de los riesgos de información y la gestión de los riesgos de información.

- El Gerente de Gobernanza de la Información realiza informes mensuales tanto al director de Operaciones directamente como al Comité de Integración de Sistemas y Estrategia con respecto a los riesgos de la información.
- Posteriormente, el director de Operaciones informa sobre cualquier riesgo de información notable al Comité de Auditoría y Riesgos; el nivel de riesgo se establece en el segmento de Activos de Información del Registro de Riesgos de Operaciones del Grupo.

## 7. Seguridad de datos

7.1. El personal es personalmente responsable de garantizar que cualquier dato personal que haya adquirido, gestionado, procesado, compartido, almacenado o eliminado:

- Todos los datos personales que poseen se guardan de forma segura.
- La información personal no se divulgará, ni oralmente ni por escrito, de forma accidental o de otro modo, a ningún tercero no autorizado.

7.2. Todos los datos personales deben guardarse en un archivador o cajón cerrado con llave. Si se almacenan en una computadora, deben almacenarse de forma segura y solo quienes tengan acceso a ellos Se recomienda. Se desaconseja almacenar datos personales en medios extraíbles o dispositivos móviles, y el uso de cifrado es obligatorio en estos casos.

7.3. La solución oficial de almacenamiento en la nube para datos personales es el inquilino del Grupo Microsoft 365 y Docuware. Es obligatorio realizar una evaluación de impacto de la protección de datos antes de utilizar cualquier otro servicio de almacenamiento en la nube.

7.4. La creación de nuevos sistemas informáticos que incluyan el almacenamiento de información personal deberá integrar la privacidad en el proceso de diseño. El diseño deberá incluir, entre otras cosas, la capacidad de registrar y gestionar el acceso de los usuarios a la base de datos y atender las solicitudes de acceso y supresión de los datos de los interesados.

7.5. Los estudiantes deben asegurarse de que todos los datos proporcionados al Grupo sean precisos y estén actualizados. Cualquier cambio en los datos debe notificarse al Departamento de Registros Estudiantiles o a su Departamento de Estudiantes.

Tutor.

## 8. Transferencias internacionales de datos

8.1. El RGPD del Reino Unido restringe la transferencia de datos personales a países fuera del Reino Unido o a organizaciones internacionales. Estas restricciones se aplican a todas las transferencias, independientemente de... del tamaño de la transferencia o de la frecuencia con la que se transfieren los datos.

8.2. Las transferencias restringidas solo se realizarán cuando exista un acuerdo de adecuación o la transferencia esté amparada por as garantías adecuadas o, en circunstancias excepcionales, esté amparada por una de las exenciones del artículo 49 del RGPD del Reino Unido. No se podrá aplicar ninguna exención sin consultar previamente con el responsable de Gobernanza de la Información.

8.3. Cabe señalar que, tras el período de transición del Brexit, el gobierno del Reino Unido determina qué países y territorios reciben el estatus de adecuación, y estos pueden diferir del estatus de adecuación otorgado por la Comisión Europea en virtud del RGPD de la UE.

## 9. Acceso a los datos

9.1. Las personas cuyos datos el Grupo conserva tienen derecho a acceder a cualquier dato personal que se procese sobre ellas. La solicitud, conocida como Solicitud de Acceso del Sujeto (SAR), debe presentarse al equipo de Gobernanza de la Información y adjuntarse un documento de identidad (véase el Anexo A). En la mayoría de los casos, la SAR es gratuita. Si corresponde un cargo, se contactará a las personas para gestionar el pago. La SAR debe incluir suficiente información para que el Grupo pueda encontrar los datos personales solicitados sin mayor esfuerzo.

9.2. El Grupo procurará atender todas las solicitudes de información a la mayor brevedad posible, pero garantizará que, en todos los casos, la información se proporcione en el plazo de un mes natural, a menos que la solicitud se considere compleja, en cuyo caso se proporcionará en un plazo de tres meses naturales.

9.3. Todo miembro del personal que reciba o tenga conocimiento de un SAR, ya sea verbalmente o por escrito, deberá informarlo al equipo de Gobernanza de la Información. inmediatamente o al menos dentro de un día hábil desde su recepción.

9.4. La información personal nunca se divulgará por teléfono a entidades externas ni a personal interno que no sean los directivos correspondientes.

9.5. Ocasionalmente, podría ser necesario compartir datos personales con otras partes si existe una necesidad imperiosa y una justificación legal para hacerlo, incluyendo la protección de los intereses vitales de la persona o si existe un interés público. El método de transferencia deberá garantizar la seguridad continua de los datos y estar incluido en un acuerdo preexistente (por ejemplo, equipos de protección).

## 10. Publicación de información

10.1. La política del Grupo es hacer pública la mayor cantidad de información posible. La siguiente información estará disponible para consulta pública:

- Nombres y fotografías de los miembros de la Corporación.
- Resumen detallado de los logros de los estudiantes y de los éxitos en los exámenes.

Los detalles relacionados con un estudiante individual no se publicarán sin el permiso expreso de ese individuo.

- Participación estudiantil en producciones y eventos relacionados con sus estudios. Se requiere la autorización del estudiante antes de realizar esta actividad.

10.2. La lista telefónica interna del Grupo no será un documento público.

10.3. Cualquier persona que tenga buenos motivos para desear que alguno de estos detalles permanezca confidencial deberá ponerse en contacto con el equipo de Gobernanza de la Información.

## 11. Consentimiento del sujeto

11.1. De conformidad con la legislación de Protección de Datos, el Grupo obtendrá el consentimiento de los futuros estudiantes y nuevos miembros del personal para la recopilación y el tratamiento de datos, a menos que exista una base legal alternativa para el tratamiento de los mismos. Para los datos sensibles descritos en la legislación, se obtendrá el consentimiento expreso.
Esto incluirá información sobre antecedentes penales y necesidades de salud. En los casos en que los solicitantes estén en contacto con niños y jóvenes de entre 16 y 18 años (o adultos en riesgo), se realizarán verificaciones, de conformidad con la normativa vigente, para garantizar que sean aptos para trabajar en el Grupo.

11.2. Por consiguiente, la inscripción y el nombramiento de personal quedarán condicionados a la concesión de dicho consentimiento.

11.3. Las condiciones para el consentimiento se establecen en el artículo 7 del RGPD. En caso de que el consentimiento del interesado se utilice como tratamiento lícito de sus datos personales, el personal deberá cumplir lo siguiente:

- adoptar un lenguaje claro y directo al solicitar el consentimiento del interesado.
- El consentimiento del interesado debe ser específico e informado, debiendo informarse al interesado de:

- el nombre de su organización y los nombres de cualquier otro controlador que dependerá del consentimiento (el consentimiento para categorías de controladores externos no será lo suficientemente específico);
- por qué desea los datos (los fines del procesamiento);
- qué hará con los datos (las actividades de procesamiento);
- y que las personas pueden retirar su consentimiento en cualquier momento, así como informarles cómo pueden retirar su consentimiento.

11.4. El artículo 7(3) del RGPD otorga a los interesados el derecho a revocar su consentimiento en cualquier momento; además, debe ser tan fácil revocarlo como otorgarlo.

11.5. El equipo de Gobernanza de la Información también deberá registrar el consentimiento, el cual se actualizará periódicamente.

## 12. Procesamiento de información sensible

12.1. A los efectos de la aplicación de las políticas de baja por enfermedad, igualdad de oportunidades y otras políticas. Es necesario procesar información sensible sobre la salud de una persona, sus antecedentes penales, características protegidas (edad, origen étnico, género, religión o creencias, o discapacidad) y otros datos familiares. El Grupo es consciente de que esto podría causar especial preocupación o angustia y aclara el motivo de la solicitud y el uso que se hará de la misma.

Se requiere una condición del artículo 9, como el consentimiento explícito, antes de la recopilación y el procesamiento de datos personales sensibles.

## 13. Procesador de datos

13.1. Un «Encargado del Tratamiento» es una persona, autoridad pública, agencia u otro organismo que realiza el tratamiento (que puede consistir simplemente en consultar o conservar) de datos personales en nombre del Grupo. Por ejemplo, un subcontratista que imparte formación a nuestros estudiantes.

13.2. Debe existir un contrato que estipule niveles de protección de datos personales equivalentes a los implementados por el Grupo y estipulados por la legislación de protección de datos. El responsable de Gobernanza de la Información puede solicitar un modelo/anexo contractual para los Encargados del Tratamiento.

13.3. La realización de una Evaluación de Impacto de Datos es obligatoria cuando exista un riesgo para los derechos de las personas, antes de contratar a cualquier responsable del tratamiento de datos (véase la sección 17). Esto incluye completar la lista de verificación de contrato

## 14. Responsable del tratamiento de datos

14.1. Un responsable del Tratamiento es una organización que determina los fines y los medios del tratamiento de datos personales (decide por qué se recopilará la información personal y cómo se tratará). El Grupo es el responsable legal, en última instancia, de la aplicación de la legislación en materia de protección de datos.

## 15. Retención de datos

15.1. El Grupo conservará algunos datos durante más tiempo que otros. Sin embargo,

La información sobre el personal, los estudiantes y otras partes interesadas no se puede conservar indefinidamente.

15.2. El Grupo mantendrá una política de retención independiente que detalle las categorías clave de datos y su duración.

15.3. Todos los datos que alcancen el final de su periodo de conservación se eliminarán de forma segura y permanente. Esto incluye tanto los archivos informáticos como los documentos físicos.

15.4. Cualquier medio electrónico que contenga datos personales deberá eliminarse de forma segura al final de su vida útil (consulte las consultas con el Servicio de TI).

15.5. Los expedientes estudiantiles se conservarán durante un periodo de acuerdo con la política de retención. Estos expedientes incluyen información confidencial que estamos obligados a recopilar por los organismos gubernamentales de financiación. Esta información incluye el origen étnico y puede incluir detalles sobre la situación

personal. Puede obtener más información del equipo de Gobernanza de la Información.

15.6. Los registros del personal se conservarán durante un período de acuerdo con la política de retención.

La información sobre pensiones, impuestos, litigios potenciales o actuales relacionados con el empleo y los datos necesarios para las referencias se conservarán durante periodos más largos, según las circunstancias específicas. Los documentos relacionados con la salud y la seguridad se conservarán durante periodos más largos en determinadas circunstancias, como, por ejemplo, en caso de problemas de salud a largo plazo.

## dieciséis. Cookies y tecnologías similares

16.1. Las cookies son pequeños fragmentos de datos que un sitio web descarga en un ordenador y que permiten que el sitio web lo reconozca en visitas posteriores. A menudo se utilizan para rastrear la actividad de los visitantes o para usos a corto plazo, como el mantenimiento de carritos de compra.

16.2. La legislación exige que se solicite el consentimiento para el uso de cookies para ciertos fines. La legislación abarca no solo las cookies, sino también cualquier tecnología que pueda dejar datos. en la computadora de una persona.

16.3. El uso de cookies o tecnologías similares en sitios web externos del Grupo debe evaluarse con arreglo a la legislación vigente para determinar si se requiere el consentimiento de los visitantes.

## 17. Circuito cerrado de televisión (CCTV)

17.1. El Grupo opera un sistema de CCTV para la seguridad del personal y el alumnado. El funcionamiento de este sistema cumple con el Código de Práctica emitido por el Comisionado de Información. Consulte la política de CCTV.

17.2. Las solicitudes de acceso a datos de CCTV se tramitarán de la misma manera que el acceso a cualquier otro tipo de datos personales (véase la sección 7).

## 18. Cesión de datos personales a organismos oficiales

18.1. Ocasionalmente, organismos oficiales como la Policía o la Agencia Tributaria pueden solicitar la divulgación de información personal. Salvo en casos de emergencia, esta solicitud se remitirá al responsable de Gobernanza de la Información o a la persona que este designe, y se

evaluará conforme a las disposiciones pertinentes de la legislación sobre protección de datos.

18.2. Todas las solicitudes de datos personales por parte de las agencias policiales del Reino Unido deben ser

Acompañado de un formulario firmado de solicitud a una organización externa para la divulgación de datos personales a la policía, también conocido como DP2. Este formulario lo proporciona la agencia policial. Las solicitudes de agencias internacionales de aplicación de la ley deben ir acompañadas de la documentación equivalente.

## 19. Evaluaciones de impacto de la protección de datos

19.1. Una Evaluación de Impacto de la Protección de Datos es esencialmente un proceso de gestión de riesgos y debe realizarse antes de nuevos usos de datos personales para identificar cualquier problema relacionado con la protección de datos o la legislación relacionada.

19.2. Las Evaluaciones de Impacto de la Protección de Datos deben ser documentadas formalmente y firmadas por una persona pertinente designada por el responsable del Tratamiento de Datos antes de cualquier nuevo uso de datos personales.

19.3. En este contexto, «nuevos usos de datos personales» se refiere a cualquier uso que no esté contemplado en el registro ICO del Grupo ni en los consentimientos formales obtenidos de los interesados.

19.4. La Evaluación de Impacto de la Protección de Datos es una etapa obligatoria en la planificación previa de cualquier nuevo proyecto que implique el uso de datos personales o en cualquier caso en el que los

datos vayan a ser procesados por un encargado del tratamiento o un corresponsable del tratamiento en nombre del Grupo.

19.5. Si tiene alguna duda sobre la necesidad de una Evaluación de Impacto de la Protección de Datos, consulte al equipo de Gobernanza de la Información.

## 20. Inteligencia artificial

20.1. El uso de cualquier inteligencia artificial (IA) que involucre datos personales debe estar sujeto a una evaluación de Impacto de Protección de Datos completa antes de su implementación.

20.2. Siempre que la IA utilice datos personales, también debe tenerse debidamente en cuenta el artículo

22 del RGPD, que otorga a los interesados el derecho no a ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, si dichas decisiones «producen efectos jurídicos sobre él o le afectan significativamente de modo similar».

## 21. Uso de datos personales con fines comerciales

21.1. De conformidad con la legislación de Protección de Datos, el Grupo obtendrá el consentimiento de las personas para la recopilación y el tratamiento de datos con fines comerciales. Para los datos sensibles descritos en la legislación, se obtendrá el consentimiento expreso.

21.2. Cualquier solicitud de permiso para comercializar con una persona debe realizarse con consentimiento expreso.

21.3. Todas las nuevas propuestas de tratamiento de datos personales con fines de marketing serán evaluadas por el responsable de Gobernanza de la Información.

## 22. Enlaces a otras políticas

22.1. La política de uso aceptable define requisitos específicos en términos de seguridad de datos.

22.2. La Política de Retención de Registros define los cronogramas de retención y describe los requisitos para la eliminación segura de los activos de datos.

## 23. Más información

23.1. Para obtener más información sobre la Ley de Protección de Datos de 2018, el RGPD del Reino Unido y el RGPD de la UE, consulte el sitio web de la Oficina del Comisionado de Información.

## 24. Ley de Protección de las Libertades de 2012

24.1. La Ley de Protección de las Libertades de 2012 detalla las obligaciones legales relativas al almacenamiento, uso y destrucción de datos biométricos (por ejemplo, huellas dactilares y ADN).

El Grupo no almacena ni utiliza datos biométricos. Los dispositivos móviles más modernos, como smartphones y tabletas, sí utilizan datos biométricos como el reconocimiento facial y de huellas dactilares. Estos datos solo se almacenan en el dispositivo y deben borrarse al transferirlo a otro usuario.

## 25. Revisión de cuentas

25.1. El Grupo realizará auditorías documentadas para comprobar el cumplimiento del personal con las políticas y procedimientos de protección de datos, así como con la legislación pertinente. Las auditorías se centrarán en áreas o procesos de negocio específicos e incluirán comprobaciones puntuales de cumplimiento.

25.2. Las auditorías serán supervisadas por el equipo de Gobernanza de la Información y quedarán registradas.

Los casos de incumplimiento serán objeto de controles de seguimiento después de un intervalo apropiado.

25.3. Los encargados del tratamiento y los corresponsables del tratamiento de datos serán auditados mediante un enfoque basado en el riesgo, proporcional al tipo y volumen de datos que procesen en nombre del Grupo.

## 26. Estado de esta política

26.1. El funcionamiento de esta política será revisado periódicamente por el Gerente de Gobernanza de la Información.

26.2. Esta política podrá ser revisada y modificada periódicamente por el Equipo de Liderazgo del Grupo.

# Anexo A

## Formas aceptables de identificación

Para verificar la identidad de una persona que solicita información personal, se deberá proporcionar una forma de identificación de cada categoría.

Identidad con fotografía

- Permiso de conducir
- Pasaporte
- Tarjeta de identidad de las fuerzas armadas

Comprobante de domicilio

- Extracto bancario reciente o factura de servicios públicos, etc.

| | |
|---|---|
| Área de revisión de políticas | ÉL |
| Gerente principal/propietario | JOSEP FABRA SEGARRA |
| Nivel de aprobación | Equipo de liderazgo del grupo/corporación |
| Fecha de aprobación | MARZO de 2025 |
| Ciclo de revisión | Cada cinco años |
| Próxima revisión | Marzo de 2030 |