Acreditada
en Alta Calidad
Res. n°. 023654 del Mineducación.
10/12/21 vigencia 10/12/27

MANUAL INTERNO DE DIRECTRICES Y PROCEDIMIENTOS - PROGRAMA INTEGRAL DE DATOS PERSONALES

GESTIÓN JURÍDICA, LEGAL Y PROTECCIÓN DE DATOS PERSONALES

UNIVERSIDAD EAN

BOGOTÁ 2024

©Universidad Ean **SNIES 2812** | Vigilada Mineducación | **Personería Jurídica Res. nº. 2898** del Minjusticia - 16/05/69

El Nogal: Cl 79 nº 11 - 45 | NIT: 860.026.058-1
Centro de contacto: **60 1** 593 6464 | Bogotá D.C., Cundinamarca, Colombia, Suramérica
universidadean.edu.co

CO09/2794

1. OBJETIVO Y ALCANCE DE ESTE DOCUMENTO

La Universidad Ean es una institución de educación superior, comprometida con el respeto de las normas y las buenas prácticas, por lo tanto, mediante este Manual determina:

1.1. La estructura administrativa necesaria para el respeto al derecho al habeas data;

1.2. La adopción de mecanismos internos para poner en práctica la Política de Tratamiento de Datos Personales en la Universidad Ean;

1.3. Los procesos internos detallados para la atención y consulta de quejas y reclamos de los titulares.

1.4. Las directrices e instrucciones internas para prever y atender cualquier riesgo relacionado al tratamiento de datos personales, incluidos también los derivados del uso de nuevas tecnologías y/o IA.

1.5. Las directrices para la implementación de nuevas tecnologías y herramientas de Inteligencia Artificial (IA), dentro de los procesos que involucren el tratamiento de datos personales de los grupos de interés de la Institución y su comunidad Eanista.

2. ESTRUCTURA ADMINISTRATIVA

2.1. Compromiso de la Alta Dirección y de los Órganos de Gobierno y Administración

La Universidad Ean adoptó la Política de Tratamiento de Datos Personales desde 2014, y la más reciente versión puede consultarla en la página web de la Universidad www.universidadean.edu.co, y ha nombrado Oficiales de Protección de Datos que se encargan de elaborar y hacer seguimiento al Programa Integral de Gestión de Datos Personales de la Universidad, para cumplir con las normas sobre protección de datos personales, establecer los controles, evaluación y revisión permanente del mismo al interior de la Institución.

En el esquema de gobierno de la Universidad, la Rectoría, quién lidera la organización administrativa de la Institución en conjunto con la Gerencia General, conformó el Comité de Seguridad de la Información y Gestión Documental, donde reportan directamente el Oficial de Datos Personales y la Secretaria General, los temas relacionados con Habeas Data. Es de resaltar que estos cargos tienen línea directa de reporte con los órganos de

administración, gobierno y dirección de la Institución para estos asuntos (Resolución No. 078 de 2024).

Periódicamente la Secretaria General informa de la evolución del Programa Integral de Gestión de Datos Personales en la Institución, al Comité de Auditoría, conformado por miembros del Consejo Superior (máximo órgano de administración de la Universidad Ean), a la Gerencia General y a la Rectoría.

Es por esto que, consideramos indispensable, la inclusión de una estrategia de privacidad por diseño, dentro de la cual, la protección de los datos personales que trata la Institución, sean especialmente custodiados, dentro de los potenciales proyectos que impliquen el uso de nuevas tecnologías e IA, con el fin de continuar con las buenas prácticas que ya se han implementado en la materia y poderlas reforzar cuando de la entrada de nueva tecnologías se trate, mediante ejercicios preventivos y de medición de impacto que sigan proporcionando, buenos niveles de seguridad de la información y la posibilidad de generar una narrativa transversal, en materia de privacidad, desde los altos directivos de la Universidad hasta todas las áreas operarias que se vean involucradas en procesos relativos al tratamiento de datos personales de terceros, asegurando un monitoreo de este tipo de proyectos de innovación desde que son una opción potencial hasta la fase, en caso de ser viable, de su implementación y socialización.

2.2. Partes de interés en la Estructura Administrativa y sus roles

2.2.1. **Sala General:** máximo órgano de gobierno encargado estatutariamente de aprobar la política de tratamiento de datos.

2.2.2. **Consejo Superior:** máximo órgano de administración que conforma el Comité de Auditoría, ente en el cual se reporta periódicamente la evolución de Programa de Datos Personales.

2.2.3. **Oficial de protección de datos personales:** Actualmente, la Secretaría General como área y la Coordinadora de Gestión Jurídica y Legal de la Institución, adelantan esta labor, de conformidad con el Acuerdo No 026 de 2020 del Consejo Superior.

2.2.4. **Rectoría y Gerencia General:** Reciben reporte directo de la Secretaria General y crearon el Comité de Seguridad de la Información y Gestión Documental, para asegurar el cumplimiento de la normativa relacionada con la protección de datos personales.

2.2.5. Comité de Seguridad de la Información y Gestión Documental: está conformado por un equipo interdisciplinario de colaboradores de la Universidad Ean, quienes tienen competencias para promover la protección de la información, de los recursos tecnológicos, la aplicación de buenas prácticas en seguridad de la información y el cumplimiento de la normativa relacionadas con la protección de datos personales. Este Comité monitorea el manejo y organización del sistema de administración de documentos con los enunciados de finalidad, responsabilidad, confidencialidad, seguridad y accesibilidad.

2.2.6. Gestores de Datos Personales: Son las personas (empleados) responsables de gestionar las bases de datos en la Universidad Ean y se encuentran relacionadas en el Anexo No 2 (Gestores).

2.2.7. Encargados del tratamiento: Los encargados del tratamiento de datos son los terceros a nivel nacional o internacional con los cuales la Universidad Ean tiene un contrato o convenio y que actúan en nombre de la Universidad de acuerdo con la política de tratamiento de datos en cumplimiento de la Ley 1581 de 2012 y demás normas concordantes, con las finalidades directas e indirectas que se encuentran relacionadas con los propósitos y fines institucionales enunciados en el "Aviso de Privacidad". Los encargados pueden estar relacionados con cualquiera de las bases de datos que tiene la Universidad Ean registradas ante la SIC y que se encuentran en el aviso de privacidad en el siguiente link: https://universidadean.edu.co/la-universidad/quienes-somos/orientacion-estrategica/reglamentos-universidad-ean/aviso-de-privacidad

2.2.8. Líderes de proceso: Son los encargados en la estructura administrativa de gestionar, administrar y liderar los procesos de la Institución y así mismo, de resaltar la importancia de la debida gestión de los datos personales, conforme le sea informado por el Oficial de Protección de Datos Personales en la Institución.

2.2.9. Empleados y Contratistas (personas naturales) de la Universidad Ean: En virtud de los contratos que suscriben adquieren la obligación de cumplir con las normas internas y externas relacionadas con protección de datos.

2.2.10. Comunidad Eanista: Como comunidad educativa se comprometen a respetar las normas internas y externas relacionadas con datos personales. Hacen parte de la comunidad Eanista, los estudiantes, colaboradores, profesores, padres de familia, investigadores, visitantes, contratistas y demás personas que tengan un vínculo con las Institución.

2.2.11. Gerencia de Tecnología de la Información y Comunicación: Son los encargados de gestionar la infraestructura tecnológica de la Universidad Ean y a su cargo se encuentra la Coordinación de Seguridad de la Información.

2.3. Responsabilidades específicas

2.3.1. Responsabilidades específicas del Oficial de Datos Personales en la Universidad Ean: El Oficial de Protección de Datos Personales tendrá a cargo la supervisión del cumplimiento del Programa Integral de Gestión de Datos Personales incluidos sus anexos y actualizaciones y, en particular, tendrá las siguientes responsabilidades:

2.3.1.1. Gestionar, junto con el Coordinador de Seguridad de la Información y los invitados que se crean necesarios, la toma de decisiones operativas del Programa Integral de Gestión de Datos Personales.

2.3.1.2. Servir de enlace y establecer responsabilidades específicas para otras áreas de la universidad respecto a la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales.

2.3.1.3. Realizar seguimiento a la implementación de los planes de acción que mitiguen los riesgos identificados para la protección de los datos personales y el cumplimiento de la Ley sus actualizaciones y los lineamientos que la Autoridad local vaya generando conforme a las buenas prácticas y el avance regulatorio en la materia. Y conforme a lo anterior , emitir las recomendaciones que sean necesarias.

2.3.1.4. Coordinar la definición e implementación de los controles de este Manual Interno de Políticas y Procedimientos.

2.3.1.5. Hacer seguimiento, actualización y monitoreo a la matriz de riesgos en datos personales.

2.3.1.6. Hacer uso y socializar los instrumentos de evaluación de impacto con las instancias que deban conocer de nuevos proyectos cuando la potencial entrada e implementación de nuevas tecnologías, incluidas herramientas de IA estén siendo analizadas para generar nuevas eficiencias a favor de los niveles de servicio de la Universidad Ean, o hagan parte de proyectos de innovación específicos para cubrir necesidades puntuales internos o externos de la Institución.

2.3.1.7. Garantizar una implementación transversal del programa integral de gestión de datos personales, sirviendo de enlace y coordinando con las demás áreas de la Universidad.

2.3.1.8. Impulsar una cultura de protección de datos personales dentro de la Universidad mediante la supervisión en la ejecución de:

2.3.1.8.1. Entrenamientos generales, medición de la participación y calificación del desempeño en la protección de datos personales para los colaboradores de la Universidad.

2.3.1.8.2. Inducción a los nuevos colaboradores que dentro de su labor tenga acceso a, o gestionen datos personales gestionados por la Universidad.

2.3.1.8.3. Integración de las políticas de protección de datos personales en las actividades de la Universidad a través de las áreas con las cuales tiene interacciones.

2.3.1.8.4. Plan de capacitación en protección de datos personales e implementación de IA, específico para los diferentes grupos de interés de la Universidad.

2.3.1.9. Mantener un inventario de las bases de datos personales.

2.3.1.10. Registrar las bases de datos de la Universidad en el Registro Nacional de Bases de Datos – RNBD y actualizar el reporte atendiendo las instrucciones que emita la Superintendencia de Industria y Comercio – SIC con fundamento en la información entregada por parte de los Gestores de Datos Personales en la Universidad Ean.

2.3.1.11. Verificar la información, previa solicitud de los Gestores de Datos Personales, contenida en los contratos de transmisión y/o transferencia internacional que se suscriben con empresas extranjeras, con apoyo de la Secretaria General.

2.3.1.12. Validar, previa solicitud de los Gestores de Datos Personales, que los países a los cuales se realizará la transferencia de datos personales cuenten con el nivel adecuado de protección de datos personales de acuerdo con los parámetros de la SIC. En su defecto, realizar las gestiones necesarias para salvaguardar la seguridad, integridad y confidencialidad de los datos en el país de destino en el que se encuentre el destinatario de los Datos Personales y obtener las declaraciones de conformidad de la SIC, cuando sea requerido.

2.3.1.13. Notificar a la SIC cuando se evidencien incidentes de seguridad que afecten la protección de los datos personales, a través del procedimiento definido por la SIC, el cual puede ser consultado en el enlace: http://www.sic.gov.co/sites/default/files/files/Manual-de-Usuario-5-RNBD-01032017.pdf. Esta notificación se realizará

posterior a la revisión integral por parte de las áreas correspondientes y así mismo, del Comité de Seguridad de la Infromación.

2.3.1.14. Realizar seguimiento a este Manual de Políticas y Procedimientos.

2.3.1.15. Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de políticas y procedimientos adoptados por la Universidad para cumplir las normas de protección de datos personales y los lineamientos de la Autoridad local, incluyendo aquellos relacionados con el uso ético de nuevas tecnologías e IA.

2.3.1.16. Acompañar y asistir a la Universidad en la atención de las visitas y los requerimientos que realice la SIC.

2.3.1.17. Servir de enlace entre la Universidad y la SIC.

2.3.1.18. Gestionar las solicitudes de tratamiento de datos mediante el correo: habeasdata@universidadean.edu.co

2.3.1.19. Orientar a los Gestores de Datos Personales en la debida gestión y, en caso de aplicar, generar espacios de actualización en términos de nuevas exigencias y/u obligaciones provenientes de normas y/o regulaciones, por ejemplo, frente a la toma de decisiones sobre proyectos relacionados con la entrada y uso de nuevas tecnologías e IA.

2.3.1.20. Reportar al Comité de Seguridad de la Información y Gestión Documental, los hallazgos que se relacionen con el tratamiento de la protección de datos personales y los relacionados con el uso de nuevas tecnologías e IA durante dichos tratamientos de información personal.

2.3.1.21. Registrar la relación de las solicitudes recibidas de los titulares en ejercicio de sus derechos, para el posterior seguimiento de estas, incluyendo aquellas relacionadas con solicitudes de titulares que afirman o prueban verse impactados o afectados por el uso de una nueva tecnología o herramienta de IA en específico.

2.3.2. Responsabilidades específicas de los Gestores de Datos Personales en la Universidad Ean: La Universidad Ean es RESPONSABLE del tratamiento de datos personales que recolecta de los titulares en el desarrollo de su objeto social como entidad educativa. Para desarrollar la administración de los datos personales de una manera efectiva, ha designado en su interior, a GESTORES DE DATOS PERSONALES, quienes gestionan directamente las bases de datos y tienen las siguientes responsabilidades:

2.3.2.1. Respecto al formato de autorización

2.3.2.1.1. Utilizar el formato de autorización de datos personales (Anexo No. 3) al recolectar información personal, verificando siempre que se esté utilizando la versión actual.

2.3.2.1.2. Abstenerse de modificar el formato de autorización sin la autorización expresa y escrita del Oficial de Datos Personales, ya que este cuenta con los requisitos legales necesarios para obtener los datos, entre ellos, pero sin limitarse: identificación del responsable, la finalidad, los canales de quejas y reclamos, etc.

2.3.2.1.3. Solicitar la actualización del formato de Autorización siempre que las finalidades se vean limitadas, conforme al avance en los procesos y nuevos usos de tecnología e IA, que pueden generar alcances adicionales en materia del tratamiento de información personal de los grupos de interés de la Universidad.

2.3.2.2. Respecto a la autorización

2.3.2.2.1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data, a través de los canales establecidos por la Universidad y velando porque ninguna consulta o reclamo referido a datos personales quede sin ser direccionada al área a cargo de forma rápida (sin superar 48 horas), para evitar incumplimientos en los plazos de respuesta a los Titulares que pueden generar grandes sanciones.

2.3.2.2.2. Solicitar al Titular su autorización para el tratamiento de sus datos antes de hacer la recolección de datos personales, y conservar copia de la respectiva autorización. Es decir, asegurarse de que los datos obtenidos cuentan con autorización y que esta está siendo almacenada por el Área a cargo.

2.3.2.2.3. Garantizarle al Titular, la suficiente información y claridad respecto a las funcionalidades, usos y alcances de la autorización otorgada.

2.3.2.3. Respecto de las Bases de Datos y los datos personales

2.3.2.3.1. Conservar las bases de datos y la información contenida en ella, bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Ello implica evitar poner en riesgo la información por uso no autorizado de la misma, o por permitir el acceso de personas no autorizadas, o por circularla sin revisar que vaya con medidas de seguridad, y situaciones similares.

2.3.2.3.2. Actualizar la información de las bases de datos, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

2.3.2.3.3. Enviar al Oficial de Protección de Datos Personales un reporte donde informe cualquier variación sustancial de las bases de datos, indicando expresamente los puntos donde se ha presentado modificación. Se entienden cambios substanciales, cambio en la finalidad, cambio en los encargados del tratamiento, cambio en los canales de atención, cambio en la clasificación o tipos de datos personales almacenados, cambio en las medidas de seguridad de la información implementada, cambio en la política de tratamiento y cambio en la transmisión o transferencia internacional. Este reporte debe hacerse en el momento en el que ocurra el cambio.

2.3.2.4. Respectos de los encargados del tratamiento de las Bases de Datos

2.3.2.4.1. Revisar que el contratista o proveedor que se vaya a desempeñar como Encargado del Tratamiento tenga Políticas de Tratamiento de Datos Personales publicadas en su página web y que entiende la importancia de cuidar los datos y utilizarlos únicamente para la gestión contratada. Esta revisión, deberá incluir el uso de la Evaluación de impacto, su debido diligenciamiento y

socialización, sobre todo para aquellos escenarios relacionados con proyectos de innovación y tecnología.

2.3.2.4.2. Garantizar que la información que se suministre al Encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible. El Encargado es el tercero al que le confiamos alguna gestión con los datos, por ej. digitalizar, almacenar, procesar. Por lo tanto, deberá rectificar de forma inmediata la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

2.3.2.4.3. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular. Para cumplir con ello, se pueden implementar planes de seguimiento durante la vigencia del Encargo y pedir evidencia de que están cumpliendo.

2.3.2.4.4. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

2.3.2.4.5. Comunicar los canales de atención para el trámite de peticiones, quejas, reclamos o solicitudes de los titulares, que dispone la Universidad Ean para tales efectos y que encontrará en la página web en el siguiente enlace: https://universidadean.edu.co/la-universidad/canales-de-atencion-en-la-universidad-ean

2.3.2.4.6. De ser necesario, consultar mediante la mesa de servicio de tecnología de la Universidad Ean los reportes de las bases de datos que no pueda obtener como usuario funcional de los sistemas de información.

2.3.2.5. Respecto de las quejas, reclamos e incidentes de seguridad en datos personales

2.3.2.5.1. Tramitar las consultas y reclamos formulados, siempre a través del Área de la Universidad que tiene a cargo esta responsabilidad y dándole toda la prioridad ya que se trata del ejercicio de un derecho fundamental protegido por la Constitución de Colombia.

2.3.2.5.2. Cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, se deberá seguir el procedimiento establecido en el numeral 3.10 del presente Manual.

2.3.2.6. Respecto a la transmisión y transferencia de bases de datos

2.3.2.6.1. Comunicar al Oficial de Protección de Datos si terceros ajenos a la Universidad Ean pretenden acceder a la base de datos, especificando las condiciones de modo y lugar. En todo caso, deberá garantizar que esta transmisión o transferencia no se dará sin la previa y expresa aprobación del Oficial de Protección de Datos y en caso de estar relacionado el flujo de información con proyecto e implementaciones de herramientas de IA y nuevas tecnologías, se utilice la información y las respuestas obtenidas en el formato de evaluación de impacto correspondiente al proyecto en específico.

2.3.2.7. General: las demás que le informe el oficial de Protección de datos personales por escrito.

Parágrafo único. La Dirección de Transformación Organizacional notificará cualquier cambio sobre los Gestores de Datos Personales al Oficial de Protección de datos, con el fin de mantener información veraz y actualizada para el cumplimiento de la Ley.

2.3.3. Responsabilidades específicas de los Encargados de Datos Personales en la Universidad Ean: Los encargados deberán cumplir con los siguientes compromisos:

2.3.3.1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de Hábeas data.

2.3.3.2. Contar con una política de tratamiento de datos.

2.3.3.3. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

2.3.3.4. Hay que asegurar que la información que repose en las bases de datos sea veraz, completa, exacta, actualizada, comprobable y comprensible.

2.3.3.5. Actualizar la información, comunicando de forma oportuna al Responsable del tratamiento de datos, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

2.3.3.6. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Responsable del Tratamiento.

2.3.3.7. Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.

2.3.3.8. Reportar de forma inmediata a la Universidad Ean cualquier reclamación, petición o solicitud de los titulares de los datos y cualquier novedad, ajuste o nueva condición a la que esté sujeta la base de datos.

3. ADOPCIÓN DE MECANISMOS INTERNOS PARA PONER EN PRÁCTICA LA POLÍTICA

3.1. **Procedimiento de actualización de la Política:** La Universidad Ean cuenta con una política de tratamiento de datos personales y aviso de privacidad y garantiza su actualización bajo el siguiente procedimiento:

3.1.1. Elaboración Borrador: El Oficial de Protección de Datos genera un borrador de los cambios o actualizaciones que requiere la política.

3.1.2. Presentación Comité de Seguridad de la Información: El Oficial de Protección de Datos presenta en cualquiera de las sesiones mensuales en las que participa como miembro con voto y voz del Comité de Seguridad de la Información y Gestión Documental para su discusión y ajuste.

3.1.3. Recomendación de ajuste a la Rectora y al Gerente General de la necesidad de la actualización. El Oficial de Protección Datos Personales presenta al Gerente General y a la Rectora el documento con los cambios sugeridos.

3.1.4. Aprobación de los Órganos de Gobierno: la Rectora o el Gerente presentan este documento ante el Consejo Superior para su análisis y a

la Sala General para su aprobación. Su aprobación se da mediante acuerdo expedido por la Sala General.

3.1.5. Divulgación institucional de la nueva política: El oficial de protección de datos garantiza la actualización de la política en la página web y en el Registro Nacional de Bases de Datos Personales (RNBD) de la Superintendencia de Industria y Comercio - SIC. Posteriormente se divulga la política a los diferentes titulares y se solicita la autorización del tratamiento de datos según la nueva política de tratamiento de datos, en los casos de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III del Decreto 1377 de 2013 (compilado en el Decreto Único 1074 de 2015), referidos a la identificación del Responsable y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, la Universidad debe comunicar estos cambios al titular antes de o a más tardar al momento de implementar la nueva política. Además, deberá obtener del titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento.

3.2. Inventario, Registro y Actualización de las Bases de Datos ante la SIC:

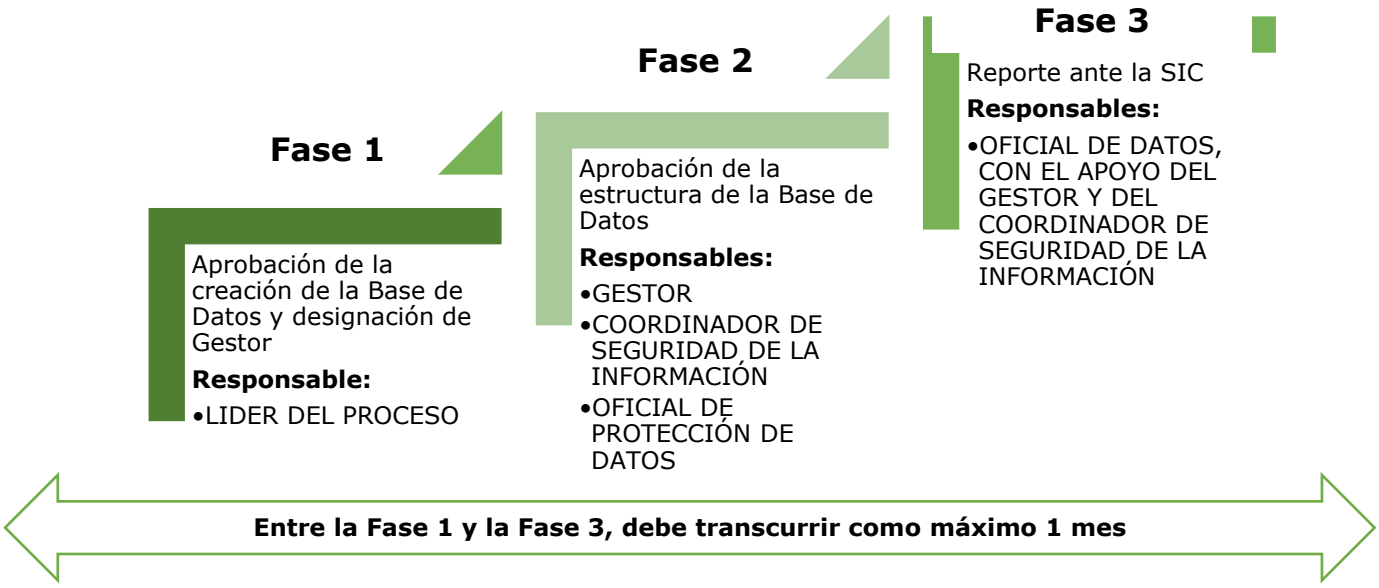
3.2.1. **Inventario de las Bases de Datos:** En el Aviso de Privacidad de la Universidad Ean que se encuentra en el siguiente enlace se relacionan las bases de datos que reportadas en el Registro Nacional de Bases de Datos Personales (RNBD) de la Superintendencia de Industria y Comercio. https://universidadean.edu.co/la-universidad/quienes-somos/orientacion-estrategica/reglamentos-universidad-ean/aviso-de-privacidad.

La Universidad realiza la inscripción o actualización de las bases de datos primarias siguiendo los lineamientos vigentes expedidos por la Superintendencia de Industria y Comercio – SIC.

Es de resaltar que la Superintendencia de Industria y Comercio ha establecido que: *"Las bases de datos que se creen con posterioridad al vencimiento de los plazos establecidos, deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación"*.

3.2.2. Procedimiento para el registro de bases de datos nuevas ante la Superintendencia de Industria y Comercio SIC: Las bases de datos que se relacionan en el aviso de privacidad son para la Universidad bases de datos primarias, las cuales se encuentran en archivos físicos o en sistemas de información y los controles necesarios para su identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición; están definidas en el documento Listado Maestro de Registros del sistema de gestión de calidad de la Universidad Ean, adicionalmente se deben gestionar de acuerdo con el Manual de Archivo de la Universidad Ean, en cuanto a la implementación, actualización y aplicación de las TRD (cuando aplique) . Así como los Gestores de Datos Personales responsables de su control y seguimiento.

La creación de una base de datos puede suponer la puesta a disposición de los titulares de un formulario que recolecte la información personal o la reorganización de la información contenida en otras bases de datos existentes. En cualquiera de los casos, el colaborador interesado en la creación de la base de datos debe seguir las siguientes etapas:



3.2.2.1. FASE 1: APROBACIÓN DE LA CREACIÓN DE LA BASE DE DATOS Y DESIGNACIÓN DE GESTOR DE DATOS PERSONALES

En esta fase, el líder del proceso debe comunicar por escrito a la Oficial de Protección de datos que es necesario crear una nueva base de datos de información personal al Oficial de Protección de Datos de la Institución, donde fundamente la necesidad de su creación y quién será nombrado como gestor de la misma.

3.2.2.2. FASE 2: APROBACIÓN DE LA ESTRUCTURA DE LA BASE DE DATOS

El gestor de la base de datos en conjunto con la Oficial de Protección de Datos Personales y el Coordinador de Seguridad de la Información deberán elaborar un documento escrito donde se acuerden como mínimo lo siguiente de la estructura de la nueva base de datos:

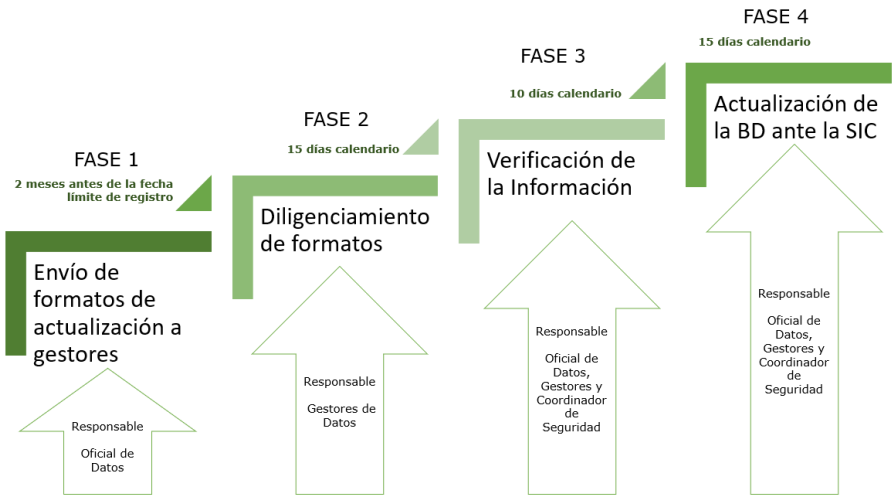
3.2.2.2.1. Datos a recolectar
3.2.2.2.2. Canales o medios de atención a los titulares
3.2.2.2.3. Ubicación
3.2.2.2.4. Encargados, si hay lugar a ello
3.2.2.2.5. Medidas de seguridad
3.2.2.2.6. Forma de obtener la autorización
3.2.2.2.7. Transferencia o transmisión si hay lugar a ello

Solo en este momento se puede crear la base de datos.

3.2.2.3. FASE 3: REPORTE ANTE LA SIC.

Dentro del mes siguiente a la creación de la base de datos, el Oficial de Protección de Datos en conjunto con el Coordinador de Seguridad de la Información reportarán la base de datos nueva en el Registro Nacional de Bases de Datos.

3.2.3. Procedimiento para la actualización anual de las bases de datos registradas ante la Superintendencia de Industria y Comercio SIC



3.2.3.1. **FASE 1**: El oficial de Protección de datos enviará: i) la información registrada ante la SIC en el Registro Nacional de Bases de Datos y; ii) El formulario para actualizarla.

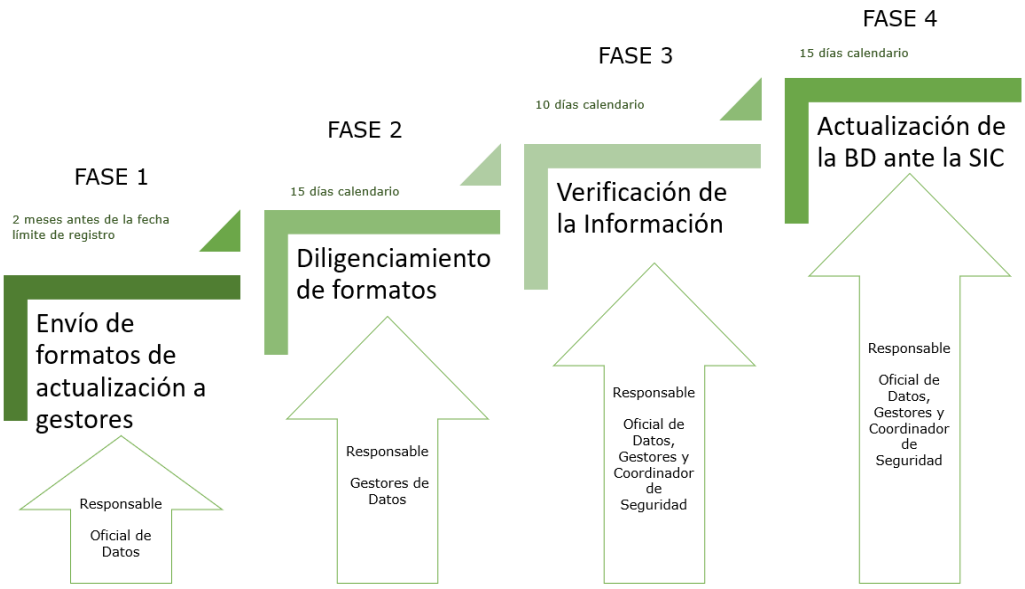
3.2.3.2. **FASE 2**: El Gestor de Datos Personales de forma diligente y responsable deberá actualizar la información en el formulario correspondiente.

3.2.3.3. **FASE 3**: El conjunto, el Oficial de Protección de Datos, el coordinador de seguridad y el gestor de datos personales responsable de la base de datos, verificaran la información contenida en el formulario, si existen vacíos o datos incompletos, el gestor de datos personales deberá resolverlos en un término de menor de tres (3) días hábiles. Si está completo sigue la siguiente fase.

3.2.3.4. **FASE 4**: Con la información completa se actualiza la base de datos ante la SIC.

3.2.4. Procedimiento para la actualización mensual de las bases de datos registradas ante la Superintendencia de Industria y Comercio SIC

Cualquier modificación sustancial de una base de datos debe reportarse por parte del Gestor de Datos Personales de forma inmediata al Oficial de Protección de Datos para la correspondiente actualización en el Registro Nacional de Bases de Datos en el sistema de la SIC, bajo el siguiente procedimiento:



3.3. Envío de correos a la comunidad Eanista

La plataforma para el envío de correos masivos será Zoom o cualquier otra que cumpla con los estándares de seguridad de la información verificados por la Universidad Ean y solo los gestores de datos personales, podrán usar la herramienta.

Los correos masivos son aquellos que pretenden llegar a toda la comunidad Eanista, cuyo contenido está relacionado con el servicio educativo que se presta, entre otros sin limitarse, al acceso a las instalaciones de la Universidad, asuntos de seguridad, acompañamiento en los

procesos de vinculación, oferta de productos y servicios y cualquiera necesaria para el cumplimiento de sus funciones académicas, administrativas y disciplinarias.
Los Gestores de Datos Personales serán los responsables de revisar que la Universidad Ean cuente con la autorización de los titulares, para el envío de este tipo de correos.

La Universidad Ean está trabajando en el mejoramiento de sus plataformas de envío para garantizar la eliminación parcial de las listas de correo.

Los titulares de estos correos podrán ejercer los derechos de eliminación, supresión, corrección y la Universidad Ean a través de los Gestores de Datos Personales procederán de conformidad.

Es importante que se considere el uso de los lineamientos de uso de correo electrónico para evitar un mal uso de esta importante herramienta, en este link puede consultarlos: Manual de Uso correo electrónico v4 (1).pdf (universidadean.edu.co)

3.4. Creación de grupos de WhatsApp o equivalentes

Para su creación es fundamental contar con la aprobación previa de la Oficial de Protección de Datos y debe considerar los siguientes criterios:

3.4.1. **Carácter excepcional:** Su creación es excepcional, ya que los miembros de la Comunidad Eanista cuenta con herramientas de mensajería instantánea administradas directamente por la Universidad Ean.

3.4.2. **Celulares corporativos:** no cree grupos de esta naturaleza en equipos móviles que no sean corporativos.

3.4.3. **Ingreso y retiro voluntario:** Los titulares deben aceptar voluntariamente su participación.

3.4.4. **Deber de información de las finalidades:** El administrador del grupo por parte de la Universidad Ean debe informar de forma previa y expresa para qué se usa el grupo y los datos que se recogen e informar de forma clara que quien desee retirarse puede hacerlo cuando lo considere, sin que su número sea guardado en las bases de datos de la Universidad Ean.

3.4.5. **No publicación de información personal:** Evite divulgar información personal de cualquier tipo propia o de terceros a los miembros del grupo y utilice los canales institucionales para ello.

3.4.6. **No requiera información innecesaria:** Si requiera información personal por este medio, utilice los canales institucionales unipersonales para tal fin.

3.4.7. **Reporte:** reporte de forma inmediata cualquier inconveniente o solicitud relacionada con datos personales al Oficial de la Universidad Ean.

3.5. Contacto de grupos de interés a través de WhatsApp o equivalentes

Se debe realizar el contacto a través de las líneas corporativas, solicitando de forma previa y expresa la autorización para el tratamiento de los datos, bajo los siguientes criterios:

3.5.1. **Celulares corporativos:** debe realizar el contacto única y exclusivamente en equipos corporativos y no personales.

3.5.2. **Autorización:** debe verificar que cuente con la autorización del titular para ser contactado por este medio.

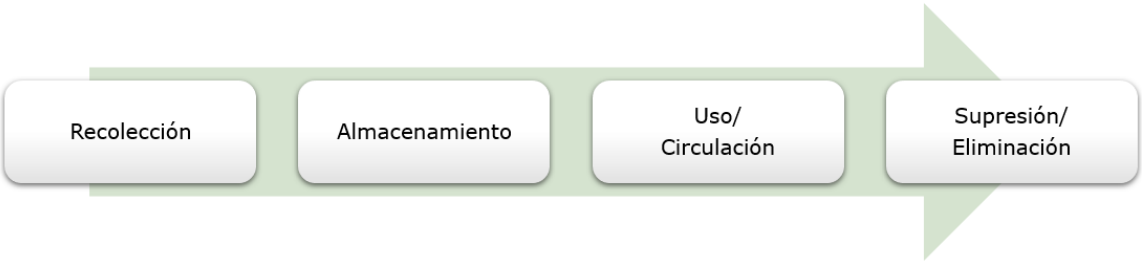
3.5.3. **Ingreso y retiro voluntario:** Los titulares deben aceptar voluntariamente la interacción en el chat.

3.5.4. **No publicación de información personal:** Evite divulgar información personal de cualquier tipo y utilice los canales institucionales para ello.

3.5.5. **No requiera información innecesaria:** Si requiere información personal por este medio, utilice los canales institucionales unipersonales para tal fin.

3.5.6. **Reporte:** reporte de forma inmediata cualquier inconveniente o solicitud relacionada con datos personales al Oficial de la Universidad Ean.

3.6. Ciclo de vida del dato y principios del tratamiento de datos personales



CICLO DE VIDA DEL DATO EN LA UNIVERSIDAD EAN	
Recolección	Los medios que utiliza la Universidad Ean para la recolección de los datos personales de los titulares son:

	a. Formularios físicos: Cuando se accede a los servicios de manera presencial, ejemplo: participación en actividades del medio universitario. b. Formularios digitales, en aplicativos o en plataformas: Cuando se accede a los servicios y estos están soportados en sistemas de información o aplicativos institucionales. c. Chat o WhatsApp: Cuando se solicita soporte o información a través de medios como establecidos en la página Web, CRM/Hydris del centro de contacto, redes sociales, teléfonos corporativos y otros. d. Grabación de voz: Cuando hay comunicación de manera telefónica. e. Cookies: Cuando se ingresa al sitio web y accede a la información contenida en está, lo que permite identificar y clasificar los intereses del usuario, de acuerdo con sus preferencias. f. Grabación de Videos: Realizados dentro del proceso de seguridad física de la Universidad, los eventos académicos e institucionales realizados internamente en la Universidad o en donde la Universidad hace presencia. En los medios mencionados anteriormente la Universidad Ean garantiza que en la recolección de los datos personales se solicite la autorización previa del titular para el tratamiento, de manera voluntaria, explícita, informada e inequívoca. Y en los casos que no se requiere la autorización de los titulares estas excepciones cumplirán según lo enunciado en la Ley 1581 de 2012 en el Artículo 10, o en los demás decretos, tales como los de emergencia sanitaria derivada por la Covid-19. Las Plataformas en las cuales la Universidad Ean tiene los datos personales registrados son las que se encuentran relacionadas en el Anexo No 4. En los casos en los que la autorización se encuentre en grabaciones telefónicas, estás quedan guardadas en el aplicativo de llamadas durante un mes para la consulta de las personas del centro de contacto. Luego pasan a un servidor interno de la Universidad, donde reposan durante el tiempo que determine la Dirección de Tecnologías de la Información y las Comunicaciones, después de este tiempo según programación del sistema de copias de respaldo pasan a cintas magnéticas para su custodia por un tercero. Por lo anterior, es necesario solicitar la eliminación de dicha copia

	cuando sea solicitado por el titular la revocación de esta y dejar en acta el registro de su eliminación.
Almacenamiento	Los medios que utiliza la Universidad para el almacenamiento de los datos personales de los titulares son: a. Servidores propios o a cargo de terceros b. Servicios en la Nube c. Archivo físico administrado por un tercero o por la Universidad Ean. d. Servidores externos a cargo de terceros. La protección y recuperación de los datos personales está a cargo del área de la Dirección de Tecnologías de la Información y las Comunicaciones quien supervisa tiene la relación contractual con los Encargados del tratamiento cuando se trata de servidores a cargo de terceros y en los casos de servidores propios su gestión se encuentra definido en el "Manual de Seguridad de la Información", disponible en www.universidadean.edu.co. Para los archivos físicos la relación contractual está a cargo del área de Gestión Documental.
Uso	Los datos personales de los titulares son utilizados en consonancia con las finalidades autorizadas por el titular y reportadas en el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio (SIC) y en cumplimiento a lo establecido en el "Aviso de Privacidad" de la Universidad Ean. En principio, los datos personales de Titulares se podrán incluir como insumo, ni compartir, en herramientas de inteligencia artificial (v.gr. Chat GPT, Bing Chat). En caso de adquirir herramientas de inteligencia artificial que coadyuven al cumplimiento de las finalidades institucionales, se observarán los principios gestores de la protección de datos personales en Colombia bajo el respeto de los derechos de los titulares y la debida diligencia de la Universidad en estos temas y las directrices dispuestas en el Anexo 7.
Circulación	La circulación de los datos personales de los titulares se hace al interior de la Universidad según las necesidades de acceso o consulta de los colaboradores a los sistemas de información y su control para el acceso

	está dado exclusivamente a la información que requiere conocer para ejercer el rol en el área al cual pertenece. Este control está a cargo del área de TIC e Innovación Tecnológica y su gestión se encuentra definido mediante los lineamientos del Manual "Roles, Obligaciones y Responsabilidades de los Líderes Técnicos, Líderes Funcionales y Usuarios" y en el procedimiento "Administración de usuarios, roles y perfiles". Igualmente hay información que se comparte con otras áreas de la Universidad de manera digital en las carpetas compartidas a través de DRIVE o OneDrive y se da acceso únicamente para visualizar los archivos sin permiso de edición o eliminación, el control depende del responsable interno asignado. Es responsabilidad del gestor de datos personales, de la información garantizar que solo pueda ser accedida por las personas que lo requieren para el desarrollo de sus actividades, partiendo del principio de acceso y circulación restringida. La Universidad Ean, igualmente suministra datos personales a: a. Entidades del Estado, en ejercicio de su función como una Entidad de Educación Superior como son: - Ministerio de Educación Nacional (SNIES, Entes de Acreditación, etc.) - Secretaria Distrital de Salud. - Migración Colombia. - Empresas de gestión pensional o parafiscales. - Alcaldía de Bogotá D.C. - Entre otras. b. Entidades que requieren información de los colaboradores como son: - Entidades financieras para el pago de nómina. - Entidades de sistema de seguridad social, pensional y parafiscales - Fiscalía General de la Nación. - DIAN y Secretaría de Hacienda. - Entre otras.

	c. Entidades que solicitan certificados de estudiantes para los procesos de selección y contratación, con la expresa autorización del titular, las cuales son entregadas al estudiante, como el titular de los datos y en el ejercicio de su derecho de acceso y consulta; o a un tercero previa autorización de este, dando cumplimiento a lo establecido en el procedimiento de Certificaciones y verificaciones académicas, disponible en el Sistema de Gestión de Calidad de la Ean. En los casos enunciados anteriormente, la circulación de los datos personales no requiere la autorización de los titulares según lo enunciado en la Ley 1581 de 2012 en el Artículo 10. La Universidad Ean no transmite datos personales que recolecta a terceros con quienes **NO** haya firmado un contrato que regule la transmisión de datos.
Supresión	La Universidad Ean realiza la supresión de los datos personales cuando se haya cumplido la finalidad por la cual fueron recolectados o en los casos que el titular de los datos solicite la eliminación de los mismos mediante el ejercicio del derecho de habeas data que se enuncia en la política de tratamiento de datos, con las excepciones derivadas de la naturaleza del servicio educativo que se presta y siempre que no medie un deber legal o contractual de conservar la información por un periodo determinado de tiempo. El proceso de Gestión Documental de la Universidad suministra las directrices que regulen la función archivística en la Ean, mediante la planeación y formulación de la política archivística que define los conceptos y criterios sobre los cuales se fundamenta la administración documental, estableciendo a nivel institucional los procedimientos y criterios para el archivo de los documentos (entre ellos los que contengan información personal) en cada uno de los procesos, para la transferencia de documentos a los archivos central e histórico y para la eliminación de los documentos según las tablas de retención documental.

	Cuando las finalidades se agoten, la Universidad Ean podrá suprimir datos personales. Para tales efectos, la Oficial de Datos Personales en conjunto con el gestor con la base de datos, requieren aprobación de esta acción al Comité de Seguridad de la Información y si la solicitud es aprobada se suprimen los datos y se deja constancia de ello en un acta.

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
Principio de necesidad y razonabilidad	Busca que los datos personales recolectados sean los necesarios para cumplir con las finalidades del tratamiento y los deberes legales.	**Recolección, Almacenamiento, Uso, Circulación y Supresión/Eliminación:** La Universidad Ean se compromete a recolectar solo los datos personales INDISPENSABLES para el desarrollo de su objeto social.	Requerir solamente los datos INDISPENSABLES para el desarrollo del objeto social de la Universidad Ean. En este sentido, no se recolectan datos personales innecesarios. Y cumplir con los compromisos establecidos en el numeral 2.3.2. de este documento.	• **Formularios de recolección de datos donde solo se requiere lo necesario para la prestación del servicio.** • **Información contenida en las bases de datos.**
Principio de legalidad	Busca que los datos se traten de conformidad con las normas que regulen la materia, es decir la Constitución Política de	**Recolección, Almacenamiento, Uso, Circulación y Supresión/Eliminación:** La	• Recolectar los datos personales, solicitando siempre la autorización para el tratamiento de estos.	• **Formulario de recolección de datos personales.** • **Aviso de Privacidad.**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
	Colombia, la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas reglamentarias.	Universidad Ean recolectará, almacenará, usará, circulará y eliminará los datos personales de los que sea responsable, de conformidad con las normas internas y externas que regulen la materia.	• Almacenar y custodiar la información de conformidad con la normativa interna y externa. • Usar los datos únicamente con las finalidades establecidas por la Institución. • Transmitir y transferir los datos solo cuando sea necesario y de acuerdo con los procedimientos determinados por la ley para este fin. • Y cumplir con los compromisos establecidos en el numeral 2.3.2. de este documento.	• **Política de Tratamiento de Datos.** • **Manual Interno de Directrices y Procedimientos – Programa Integral de Datos Personales.** • **Procedimiento de atención de solicitudes y quejas de titulares.**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
Principio de finalidad	Los datos personales recolectados están sujetos a una finalidad legítima que le es informada a los titulares.	**Recolección, Almacenamiento, Uso, Circulación y Supresión/Eliminación:** La Universidad Ean usa los datos personales recolectados con finalidades legítimas, informadas de manera clara a los titulares.	• Recolectar los datos personales únicamente para las finalidades señaladas en la Política de Tratamiento de Datos Personales y aquellas que se requieran para el logro de los objetivos del objeto social de la Institución. • Informar a los titulares las finalidades de la recolección de sus datos, en el formato de autorización que se encuentra como Anexo No 3 • Y cumplir con los compromisos establecidos	• **Documento "Aviso de privacidad", publicado en la página web y relacionada en los medios (físico o digitales) por los cuales se recolecta la información. Ver** enlace **para su consulta: https://universidadean.edu.co/la-universidad/quienes-somos/orientacion-estrategica/reglamentos-universidad-ean/aviso-de-privacidad**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
			en el numeral 2.3.2. de este documento.	• **Formato de Autorización del tratamiento de datos personales Anexo 3.**
Principio de libertad	Garantiza el tratamiento de los datos personales de los titulares cuando éste con consentimiento, previo, expreso e informado, autoriza a la Universidad, teniendo en cuenta la finalidad por la cual se obtienen.	**Recolección, Almacenamiento, Uso y, Circulación:** Quienes pretendan acceder al servicio educativo de la Universidad Ean deben autorizar el tratamiento de sus datos personales en los sistemas de información que se disponga. **Supresión/Eliminación:** El titular está en libertad de solicitar a la Universidad Ean la eliminación o supresión de	• Solicita y conserva la autorización para el tratamiento de los datos dada por el titular, la cual se obtiene mediante los diferentes medios (físico o digital) por los cuales se recolectan los datos. • Y cumplir con los compromisos establecidos en el numeral 2.3.2. de este documento.	• **Formato de Autorización del tratamiento de datos personales Anexo 3** • **Aviso de Privacidad.** • **Política de Tratamiento de Datos.** • **Manual Interno de Directrices y Procedimientos – Programa Integral de Datos Personales.**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
		sus datos. Sin embargo, esta solicitud, por la naturaleza del servicio educativo que se presta, solo será atendida de manera parcial, específicamente en la eliminación de las bases de datos que tengan fines de divulgación o promoción de los servicios de la Universidad Ean. En este sentido, los datos académicos, de salud, de conducta, en cumplimiento de un deber legal no podrán ser suprimidos o eliminados.		
Principio de veracidad o calidad	Garantiza que la información sujeta a tratamiento sea:	**Almacenamiento, Uso y, Circulación:** La Universidad	• La Universidad realiza campañas de	• **Formato de Autorización del**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
	veraz, completa, actualizada, comprobable y comprensible.	Ean registra en sus sistemas de información de forma fidedigna la historia de los titulares.	actualización de datos o por iniciativa propia del titular mediante el uso de los servicios académicos o el uso de los canales de comunicación como el correo de Habeas Data. • Los gestores de datos personales asumen la obligación de su actualización. • Y cumplir con los compromisos establecidos en el numeral 2.3.2. de este documento.	**tratamiento de datos personales Anexo 3.** • **Aviso de Privacidad.** • **Política de Tratamiento de Datos.** • **Manual Interno de Directrices y Procedimientos – Programa Integral de Datos Personales.**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
Principio de transparencia	Garantiza al titular que puede ejercer su derecho de obtener en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o dato personal que sea de su interés o titularidad.	**Recolección:** Se informa en la solicitud de autorización del tratamiento de datos, las finalidades para las cuales serán tratados los datos. **Almacenamiento, Uso y, Circulación:** La Universidad Ean responde a las solicitudes de información de los titulares d78 en los datos personales conforme ha recolectado los datos.	Direccionar de forma inmediata las solicitudes, quejas y reclamos de los titulares al correo electrónico: habeasdata@universidadean.edu.co o radicados en la Calle 71 No 9 – 84 o radicados en el teléfono 571 5936464. Si algún encargado del tratamiento de los datos recibe una consulta o reclamo del titular este debe informar de los canales existentes en la Universidad Ean.	• **Procedimiento de atención de solicitudes y quejas de titulares.**
Principio de acceso y circulación restringida.	Conserva la información bajo condiciones de seguridad necesarias para impedir su	**Recolección, Almacenamiento, Uso, Circulación y**	El acceso y la circulación de la información personal contenida en las bases de	• **Formato de Autorización del**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
	adulteración, consulta, uso o acceso no autorizado o fraudulento y no deja disponible en internet u otros medios masivos de información datos personales privados, salvo que el acceso sea controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.	**Supresión/Eliminación:** La Universidad Ean recolectará, almacenará, usará, circulará y eliminará los datos personales en sistemas de información, controlados por la Institución bajo los criterios y términos de Manual de Seguridad de la Información.	datos está en responsabilidad de los gestores de cada uno de estás (Ver tabla No 3), mediante la definición de roles y perfiles en los sistemas de información para que los colaboradores tengan sólo acceso a la información que de acuerdo con su cargo deba conocer y en medio físico el acceso a la información es asigna por el líder de cada proceso o subproceso. También se han establecido acuerdos de confidencialidad en los contratos de los	**tratamiento de datos personales Anexo 3.** • **Aviso de Privacidad.** • **Política de Tratamiento de Datos.** • **Manual Interno de Directrices y Procedimientos – Programa Integral de Datos Personales.** • **Manual de Seguridad de la Información.** • **Procedimiento de atención de solicitudes y quejas de titulares.** • **Contratos/Convenios/ Acuerdos con los**

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
			colaboradores de la Universidad, así como en los contratos de transmisión de datos personales como encargados de la información.	**encargados de datos personales.**
Principio de seguridad y Principio de confidencialidad	La información sujeta a tratamientos maneja con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad y confidencialidad de los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.		Medidas Técnicas: ✔ Reporte y seguimientos a los accidentes o incidentes de seguridad en los que pueda suceder la violación a los códigos de seguridad y existencia de riesgos en la administración de la información. ✔ Generación de backup	

PRINCIPIOS EN LA UNIVERSIDAD EAN	LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
		Medidas Humanas ✔ Cláusulas en los contratos de cada uno de los colaboradores durante el tiempo que dure su labor, en la que se compromete a conservar y mantener de manera confidencial y no revelarla a terceros cuando administren, manejen, actualicen o tengan acceso a información que se encuentren en las bases de datos. ✔ Archivos con información sensible o confidencial	

PRINCIPIOS EN LA UNIVERSIDAD EAN	LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
		deben contar con contraseña para proteger su confidencialidad. Medidas Administrativas ✔ Lineamientos de seguridad establecidos en el "Manual de seguridad de la Información". ✔ Estructuración de roles y perfiles para los sistemas de información y archivos físicos establecidos en el documento "Roles, obligaciones y responsabilidades de los líderes técnicos, líderes	

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
			funcionales y usuarios finales de los sistemas de información y aplicaciones de la Universidad EAN". ✔ Ciclo de vida de la información establecido en el Manual "Gestión Documental".	
Principio de idoneidad (especialmente aplicado a los contextos de proyectos de implementación de nuevas tecnologías e IA)	El tratamiento es capaz de alcanzar el objetivo propuesto. Por lo cual, tanto la implementación de la IA o una nueva tecnología se puede definir como una eficiencia positiva en donde, además, se podrá tratar la	Velar por la calidad del dato y cumplir con los procesos de actualización. De esta manera, se podrá mitigar el riesgo de que la información que se integre a la nueva tecnología y su automatización o que la	Seguridad de los datos, finalidades delimitadas y accesos controlados. Estructuración y uso de formatos de evaluación de impacto y de matrices de riesgo.	Las herramientas establecidas en el Anexo 7 del presente Manual sobre las directrices para el uso ético de nuevas tecnologías e IA.

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
	información personal en su mejor calidad y bajo una esfera idónea, sin decir que no puedan existir potenciales riesgos o situaciones por manejar, siempre que no superen los estándares de riesgo que la Institución tenga establecidos y en la evaluación de impacto se puedan prever herramientas para prevenir y mitigar riesgos.	herramienta de IA sea alimentada y surta su proceso de aprendizaje, bajo datos actuales y pertinentes.	Entendimiento técnico de los pros y los contras de la tecnología que está siendo evaluada. Toma de decisiones, informadas, abiertas a las áreas responsables y transparentes para la Institución en general, habiendo socializado los riesgos asumidos y los que pueden venir, y las posibilidades de mejoras en eficiencias y calidad de los servicios.	
Principio de necesidad (especialmente aplicado a los contextos de proyectos de	No existe otra medida más moderada en cuanto al impacto de las operaciones de tratamiento en la protección	Velar por la calidad del dato y cumplir con los procesos de actualización. De esta manera, se podrá mitigar el		

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
implementación de nuevas tecnologías e IA)	de datos personales e igual de eficaz para conseguir tal objetivo De esta manera, lo que se busca es utilizar los datos personales que realmente sean necesarios para la finalidad que se está buscando y al mismo tiempo, poder soportar que la herramienta de IA o la nueva tecnología si logra resolver la necesidad puntual que la Universidad esté buscando, luego de haber hecho el ejercicio de identificar y repasar qué tipo de herramientas ya se tienen y si podrían ser extensibles a la necesidad puntual o no.	riesgo de que la información que se integre a la nueva tecnología y su automatización o que la herramienta de IA sea alimentada y surta su proceso de aprendizaje, bajo datos actuales y pertinentes.	Informar, notificar y actualizar a los Titulares respecto al uso de nuevas tecnologías y de ser necesario, solicitar nuevas autorizaciones. Monitorear el cumplimiento de las obligaciones de los diferentes roles de las áreas involucradas, respecto a que se estén utilizando las herramientas e instrumentos de evaluación y los formatos en su versión más actualizada. Establecer lineamientos y documentos claros y antes de	

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
			su implementación verificar con las personas involucradas en su utilización que los comprendan, para que, en caso de necesitarlo, escalen cualquier pregunta o un nuevo asunto identificado que deba ser atendido de manera particular o si amerita la actualización del documento, contrato, notificación entre otros. Revisar a nivel interno, qué herramientas ya se tienen y si potencialmente pudiesen atender la necesidad por la cual se pretende implementar	
Principio de razonabilidad (especialmente aplicado a los contextos de proyectos de implementación de nuevas tecnologías e IA)	El tratamiento debe estar orientado a cumplir finalidades constitucionales. Por tanto, la implementación de una herramienta de IA o de nueva tecnología debe resolver y mitigar los riesgos que obstaculicen el cumplimiento de las finalidades del tratamiento y paralelamente, la protección de los derechos del Titular.	Velar por la calidad del dato y cumplir con los procesos de actualización. De esta manera, se podrá mitigar el riesgo de que la información que se integre a la nueva tecnología y su automatización o que la herramienta de IA sea alimentada y surta su proceso de aprendizaje, bajo datos actuales y pertinentes. De esta manera se podrá protegen el derecho de habeas data y los ejercicios propios del Titular conforme a la Ley 1581 de 2012.		

PRINCIPIOS EN LA UNIVERSIDAD EAN		LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
Principio de proporcionalidad en sentido estricto (especialmente aplicado a los contextos de proyectos de implementación de nuevas tecnologías e IA)	**Las ventajas obtenidas como consecuencia de la restricción del derecho a la protección de datos no deberán ser superadas por las desventajas de afectar el derecho al Habeas Data. De esta manera, las decisiones de implementación y uso de herramientas de IA o nuevas tecnologías no** deberían **romper o cortar con las estrategias de cumplimiento que la Institución ya tiene implementadas y que hacen parte de la gestión del tratamiento y la**	**Velar por la calidad del dato y cumplir con los procesos de actualización. De esta manera, se podrá mitigar el riesgo de que la información que se integre a la nueva tecnología y su automatización o que la herramienta de IA sea alimentada y surta su proceso de aprendizaje, bajo datos actuales y pertinentes. De esta manera se podrá protegen el derecho de habeas data** y los **ejercicios propios del Titular conforme a la Ley 1581 de 2012.**	una nueva IA o tecnología. Este ejercicio le dará fundamento al examen de necesidad, idoneidad y razonabilidad que siempre debe realizarse, para la toma de decisiones y para explotar al máximo herramientas que muchas veces pueden operar para atender la necesidad planteada y así no tener que incurrir en contrataciones, impactos, costos y riesgos mayores y/o desconocidos. Posibilidad de usar procesos de anonimización y/o encriptación, en caso de que este tipo de medidas técnicas	

PRINCIPIOS EN LA UNIVERSIDAD EAN	LA REALIDAD DE LOS PRINCIPIOS EN EL CICLO DE VIDA DEL DATO	RESPONSABILIDADES ESPECÍFICAS DE LOS GESTORES DE DATOS PERSONALES, ENCARGADOS Y DE LA UNIVERSIDAD EAN.	EVIDENCIAS DE CUMPLIMIENTO
	seguridad de los datos personales que se tratan. En todo caso, todo proyecto nuevo puede traer riesgos, no se pretende que no existan, sino que se puedan atender y mitigar, teniendo en cuenta las herramientas y las buenas prácticas que la se tienen para proteger los datos personales que se recolectan y se tratan, conforme a la naturaleza y tipo de relación contractual entre la Universidad Ean y el Titular.		ayuden a mitigar riesgos e impactos negativos.	

3.7. Datos Sensibles y Datos de niños, niñas y adolescentes en la Universidad Ean: Por el desarrollo del objeto social la Universidad recolecta datos personales sensibles de los titulares y datos de niños, niñas (menores de 12 años de edad) y adolescentes (entre 12 y 18 años de edad) con las siguientes finalidades:

3.7.1. Datos sensibles de los titulares como:

3.7.1.1. Datos de personas en situación de discapacidad, con la finalidad de facilitar el acceso dentro de las instalaciones de la Universidad y permitir la prestación del servicio académico.

3.7.1.2. Datos étnicos y de sexo biológico y género identitario, con la finalidad de garantizar el libre desarrollo de la personalidad, permitir el acceso a descuentos, demás beneficios de la Universidad Ean para este grupo poblacional y reportes antes las autoridades correspondientes, tales como, Ministerio de Educación, Secretaría de Educación, Secretaría de Salud, etc.

3.7.1.3. Datos relacionados con la salud física y sicológica, con la finalidad de tramitar incapacidades de los colaboradores, solicitudes de ausencia de los estudiantes a través de incapacidades, cumplimiento del sistema de seguridad y salud en el trabajo, la prestación de los servicios que ofrece la Universidad Ean en salud física y sicológica y toda la información necesaria para contener situaciones relacionadas con este asunto.

3.7.1.4. Datos biométricos como: la huella y/o captura de foto de la cara con reconocimiento facial con la finalidad de la carnetización de la comunidad Eanista y difusión de eventos de carácter institucional y académico mediante el registro fotográfico y video. Los videos de vigilancia y grabación de voz con el propósito de garantizar la seguridad de las personas, los bienes e instalaciones y trazabilidad de sus procesos académicos y/o administrativos.

Se aclara que en las grabaciones de las clases virtuales de la Universidad Ean no se usan técnicas biométricas de reconocimiento.

3.7.2. Datos de niños, niñas y adolescentes: Los datos personales que recolecta la Universidad de niños, niñas y adolescentes tienen la finalidad de garantizar el derecho a la educación, la formación integral y el bienestar de los estudiantes y de los hijos menores o adolescentes de los docentes, visitantes o colaboradores. La recolección de estos datos se realiza en los siguientes casos:

3.7.2.1. Proceso de inscripción y admisión a los programas académicos que imparte la Universidad.

3.7.2.2. Servicios académicos, administrativos y culturales que ofrece la Universidad.

3.7.2.3. Afiliación al sistema de seguridad social, caja de compensación familiar y seguro de vida.

3.7.2.4. Actividades de bienestar que beneficia a los menores de edad o adolescentes.

3.7.2.5. Toma de fotografías y videos en eventos cuando expresamente sea autorizado por sus padres o tutores legales.

3.7.2.6. Ingreso a las instalaciones de la Universidad.

Para estos datos se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes y para garantizar su derecho a la educación en el caso de los menores adultos, estos podrán otorgar directamente la autorización en los términos y condiciones establecidos en la Política de Tratamiento de Datos de la Universidad Ean.

Es posible que, en ciertas circunstancias, la Universidad se encuentre frente a un conflicto o choque entre los derechos de los representantes legales de los menores (ejercicio de patria potestad, deber de protección y bienestar) y los derechos de los menores (educación, libre desarrollo de la personalidad y datos personales). Para dirimir estos conflictos el primer lineamiento es actuar protegiendo el interés superior del menor.

✔ Cuando se trata de asuntos relacionados con su expediente académico: La Guía para el Tratamiento de Datos Personales para el sector de la educación pública y privada de la Superintendencia de Industria y Comercio - SIC señala que los centros educativos deben informar y garantizar al alumno y a sus padres, representantes o acudientes autorizados, el acceso al expediente académico, así como el derecho de requerir la actualización, rectificación o eliminación de la información allí contenida.

✔ Cuando se trata de asuntos relacionados con actividades de bienestar: Se debe propender para que la información responda al interés superior del menor sin violar su intimidad ni otros derechos como el del libre desarrollo de la personalidad y

garantizando siempre su derecho a la vida e integridad. Así, podría proporcionarse información referida a si el estudiante ha accedido o no a servicios de psicología o bienestar universitario, pero salvaguardando su derecho a la intimidad, específicamente sus detalles. Cuando la consulta vaya mucho más allá de la generalidad, sería necesario hacer una ponderación sobre la finalidad para la cual se pretendería acceder a esa información, es decir, si exponer el detalle de la información garantiza o protege los derechos del menor o no.

✔No existe una fórmula única, ya que dependerá del análisis de cada caso, así que se requiere consultar al Oficial de Datos ante cualquier reto.

3.8. Reporte de Reclamos de Titulares ante la SIC: El reporte se hará de acuerdo con los siguientes criterios:

3.8.1. Solicitudes: Cuando el titular pide que se suprima, actualice, rectifique y demás acciones relacionadas con sus datos y estas son atendidas de conformidad, por la Universidad Ean.

3.8.2. Reclamos: Cuando el titular realizó una segunda solicitud, haciendo notar que la primera no fue atendida integralmente por la Universidad Ean. Con lo anterior, se define que serán reportados a la SIC, los reclamos presentados por los titulares en los términos contenidos en el presente documento, bajo los códigos contenidos en el Manual de Usuario de la Superintendencia de Industria y Comercio.

3.9. Hechos relacionados con datos personales de la Universidad Ean

3.9.1. Definición: En la Universidad Ean, un hecho relacionado con datos personales es todo aquel en el que se evidencia un incumplimiento de los procedimientos de la Institución frente a los datos personales, que no amenaza ni tiene un impacto superior que comprometa las operaciones de la misma o los datos personales que esta custodia.

3.9.2. Reporte: Se seguirá el siguiente procedimiento:

3.9.2.1. Notificación al Oficial de Protección de Datos: cualquier persona que conozca de un hecho relacionado con datos personales, notificará al Oficial de Datos Personales.

3.9.2.2. Evaluación: La Oficial de Datos Personales, definirá, con base en la evidencia aportada si la situación expuesta en un hecho que involucra datos personales o un incidente de seguridad.

3.9.2.3. Plan de mitigación o mejora: Si se concluye que se trata de un hecho que involucra datos personales, se analiza el caso y se plantean las acciones preventivas y correctivas que correspondan, y se lleva el caso al Comité de Seguridad de la Información y Gestión Documental.

3.10. Incidentes de Seguridad que involucren datos personales

3.10.1. Definición: En la Universidad Ean un incidente de seguridad en datos personales es un hecho o serie de sucesos de seguridad donde se materializa un riesgo que atenta contra la Confidencialidad, y/o Integridad y/o Disponibilidad de los datos personales y que tiene(n) una probabilidad significativa de comprometer las operaciones de la Universidad y amenazar la seguridad de los datos personales.

3.10.2. Reporte del incidente de seguridad: Se seguirá el siguiente procedimiento:

3.10.2.1. Notificación del incidente de datos personales: cualquier persona que conozca de una situación que pueda considerarse como un incidente de datos personales deberá reportarlo por escrito al correo electrónico habeasdata@universidadean.edu.co o en la mesa de servicios de tecnología o cualquier medio habilitado. También puede ser reportado directamente por la Oficial de Datos Personales, luego de que se analice que un hecho relacionado con datos personales se clasifica como incidente de seguridad.

3.10.2.2. Recepción de la solicitud y análisis del incidente: el Oficial de Protección de Datos o el Coordinador de Seguridad de la Información de la Universidad Ean reciben la solicitud, la analizan y de ser necesario toman medidas inmediatas para proteger los derechos que se vean amenazados.

3.10.2.3. Reporte al Comité de Seguridad de la Información y Gestión Documental de la Universidad Ean: Se lleva el análisis de la situación, las medidas previas de protección y se sugiere una línea de acción para aprobación del Comité. De ser necesario se eleva el caso al Comité de Ética. El análisis del incidente debe tener como mínimo:

3.10.2.3.1. Análisis de la situación y clase de datos comprometidos.

3.10.2.3.2. Categoría de titulares afectados.

3.10.2.3.3. Fecha y hora del incidente y/o del descubrimiento de este.

3.10.2.3.4. Indagaciones preliminares iniciadas por la Institución.

3.10.2.3.5. Medidas Correctivas.

3.10.2.3.6. Responsable individualizado de manejo del incidente en la Universidad Ean.

3.10.2.3.7. Evaluación del nivel de riesgo derivado del incidente.

3.10.2.3.8. La inclusión de detalles a que haya lugar.

3.10.2.3.9. La estrategia para prevenir futuros incidentes.

3.10.2.3.10. El comité de seguridad de la información podrá apoyarse en el análisis forense que se haga del caso para determinar las medidas a implementar.

3.10.2.4. Implementación de las medidas: El Oficial de Protección de Datos hace seguimiento a la línea de acción aprobada en el Comité, específicamente a la implementación de las medidas e informa a dicho Comité para el cierre de este incidente. Una de las medidas deberá ser la comunicación escrita que debe enviarse a los titulares de la información, cuando se considere necesario. Así mismo, se dejará trazabilidad de todas las acciones que se tomen en torno a la atención del incidente y se documentarán las lecciones aprendidas.

3.10.2.5. Respuesta al solicitante: La Universidad Ean informa al solicitante de las medidas adoptadas.

3.10.2.6. Reporte a la SIC: Se reporta el incidente de acuerdo con las directrices de la SIC, dentro de los quince (15) días hábiles siguientes al momento en que se detecte o sea reportado el hecho al Oficial de Protección de Datos.

Parágrafo primero: En todos estos registros debe evaluarse la conveniencia de anonimizar los datos de los titulares para seguridad y manejo de la información.

Parágrafo segundo: los pasos establecidos en los numerales 3.8.1.2.1. al 3.8.2.5. deberán realizarse en un término máximo de 15 días hábiles bajo las guías y directrices que imparta la [1]SIC.

[1] Tener en cuenta la guía de la SIC que se encuentra en el siguiente link https://issuu.com/quioscosic/docs/guia_gestion_incidentes_dic21_2020 o la que esté vigente.

Parágrafo tercero: El incidente se cerrará cuando se ejecuten todas las acciones relacionadas con el mismo.

3.11. Gestión del tratamiento en la transmisión y transferencias de datos

CARACTERÍSTICA	TRANSMISIÓN	EVIDENCIA
Tratamiento de datos	La Universidad determina cuál será el tratamiento de los datos personales por parte del encargado.	Mediante objeto del contrato, convenio, acuerdo de voluntades, o descripción establecida en la Orden de Compra, en la que el contratista actúe por cuenta de la Universidad en el tratamiento de los datos personales
Formalidad	Las partes deben celebrar contrato de transmisión de datos personales o acuerdo de transmisión	Contrato que regule la transmisión de datos personales firmado por el representante legal del proveedor y la Universidad Ean. También es posible incluir cláusulas relacionadas con la transmisión y/o anexos a los contratos.
Autorización del titular	La transmisión de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requiere que sea informado al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.	

Cuando el gestor tenga dudas sobre los roles de las partes en el contrato (responsables o encargados), deben consultarlo con el Oficial de Protección de Datos para saber si se trata de una transmisión o una transferencia.

3.11.1. Requisitos para la transferencia

CARACTERÍSTICA	TRANSFERENCIA	EVIDENCIA
Tratamiento de datos	La Universidad y el tercero son responsables de las bases de datos y ambos los tratan de manera independiente bajo su propia política de tratamiento.	Mediante: Objeto del contrato, convenio, acuerdo de voluntades, o descripción establecida en la Orden de Compra, en la que el contratista en calidad de responsable.
Formalidad	Las partes deben celebrar contrato de transferencia de datos personales. A falta de contrato, las siguientes reglas: Verificar que haya autorización previa de los titulares para la transferencia de sus datos personales. Transferir datos solo a países que proporcionen niveles adecuados de protección de acuerdo con los establecidos por la SIC. Hacer las gestiones necesarias de conformidad con los lineamientos de la SIC en el evento en que la transferencia se realice a países que no tienen adecuado nivel de protección de datos personales de acuerdo con la SIC.	Contrato que regule la transferencia de datos personales firmado por el representante legal del proveedor y la Universidad Ean.
Autorización del titular	La transferencia de datos personales que se efectúen entre un responsable y un responsable requiere contar	

con el consentimiento del Titular.

Cuando el gestor tenga dudas sobre los roles de las partes en el contrato (responsables o encargados), deben consultarlo con el Oficial de Protección de Datos para saber si se trata de una transmisión o una transferencia.

Para más información de una transferencia segura de datos en la Universidad Ean consulte por favor el Anexo No 5, diligencie el formulario y contacte a la Oficial de Datos previo a la decisión de transferencia.

3.12. Auditorías y Administración de Riesgos

3.12.1. Auditorías internas y externas: La Universidad Ean planifica anualmente la realización de auditorías internas o externas. Los resultados de estas auditorías hacen parte del plan de mejoramiento de sistema de datos personales en la Universidad Ean, junto con la revisión de riesgos identificados, seguimiento a procesos y/o como resultado de la atención de incidentes presentados.

El resultado de las auditorias, se registran en las actas del Comité de Seguridad de la Información y Gestión Documental y en el Comité de Auditoría de la Universidad Ean, donde se deja constancia de las acciones adoptadas, se revisan algunas situaciones particulares, se discute y concreta la implementación articulada de las estrategias, se reciben recomendaciones y se informa del curso de las acciones de mejora del sistema.

Estas auditorías deberán incluir las propias a la administración del riesgo por el uso e implementación de nuevas tecnologías y/o herramientas de IA, conforme a las herramientas dispuestas en el Anexo 7.

3.12.2. Administración de los riesgos: La Universidad Ean ha establecido a través del Sistema de Gestión de la Calidad y Seguridad de la Información la metodología de gestión de riesgos, estableciendo lineamientos en el formato denominado "matriz de riesgo", con el fin de determinar la identificación y manejo de los riesgos asociados al tratamiento de datos personales con el propósito de evaluar y/o anticipar nivel de cumplimiento de las normas de protección de datos personales. La administración de los riesgos para la protección de datos está a cargo de la Universidad Ean y de los gestores de

datos personales, en cada una de las etapas del ciclo de vida de los datos. El proceso de monitoreo de los riesgos identificados está a cargo del Oficial de Protección de Datos y tiene como finalidad realizar seguimiento constante para velar porque las medidas que se han establecido sean efectivas.

Por lo anterior, la revisión y periodicidad de evaluación de los controles asignados a los riesgos, **se realiza de manera anual para asegurar que estén funcionando en forma oportuna, efectiva y eficiente**, así como asegurar que los riesgos residuales se encuentran en los niveles de aceptación.

En todo caso, se evaluarán los riesgos identificados ante cualquier cambio significativo en las actividades de tratamiento que pueda derivar en la aparición de nuevos riesgos o en la implementación de proyectos que involucren datos personales, incluidos los derivados de usos o implementaciones de nuevas tecnologías y herramientas de IA, de conformidad con el Anexo 7.

4. PROCESOS INTERNOS DETALLADOS PARA LA ATENCIÓN Y CONSULTA DE QUEJAS Y RECLAMOS DE LOS TITULARES

La Universidad Ean tiene unos canales de atención específicos para habeas data, a través del correo electrónico, sin embargo, si otra área recibe una petición, queja o reclamo de esta naturaleza, tiene la obligación de redireccionarla al correo de habeas data, en un término máximo de dos (2) días hábiles, después de recibida.

*El término máximo para atender la petición, queja o reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término, se informa al titular los motivos de la demora y la **fecha** en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.*

4.1. **Radicar solicitud:** el Titular de los datos radica una solicitud mediante un escrito dirigido a la Universidad Ean a través del correo postal remitido a la dirección: Calle 71 No 9 – 84 o mediante el correo electrónico: habeasdata@universidadean.edu.co, indicando en el asunto cuál es el derecho que quiere ejercer con los siguientes datos:

4.1.1. Nombre y apellidos del Titular.

4.1.2. Número y tipo de identificación. Se podrá pedir copia de la cédula para verificar la autenticación cuando no se envía desde el correo electrónico registrado en la Universidad Ean.

4.1.3. Petición en que se concrete el derecho que se quiere ejercer.

4.1.4. Dirección para notificaciones, fecha y firma del solicitante, en los casos que sea mediante escrito.

4.1.5. Documentos acreditativos de la petición formulada, cuando corresponda.

4.1.6. En los casos que la solicitud la realicé un tercero este debe presentar documento de representación, en caso de que actuase como apoderado o carta de autorización del titular, reconocimiento de firma y junto con la fotocopia del documento de identidad del titular y la persona autorizada.

4.2. **Tramite inicial de la solicitud:** El oficial de protección de datos personales recibe las solicitudes y las transmite a los gestores para garantizar el derecho de habeas data efectivamente en las bases de datos que corresponda.

4.3. **Solicitudes incompletas:** Si al recibir un reclamo éste está incompleto, el Oficial de Protección de Datos, lo comunicará al titular dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane la información faltante. El Oficial de Protección de Datos será notificado del requerimiento con el fin de realizar seguimiento a la atención de este. Si transcurridos dos (2) meses desde la fecha del requerimiento, sin que el titular presente la información requerida, se entenderá que ha desistido del reclamo.

4.4. **Revisión interna de los gestores de la Solicitud:** Los gestores de datos personales revisan la solicitud y la hacen efectiva, dentro de los (2) días hábiles siguientes a la recepción de la solicitud responde de fondo a la petición a la Oficial de Protección de Datos Personales, enviando la constancia de las acciones o la información requerida.

Petición	Responsabilidad de los Gestores
Actualización / Corrección/ Rectificar	Actualiza, corrige o rectifica la información en la base de datos y envía

	a la Oficial de Protección de Datos la prueba de dicha acción.
Supresión / Eliminación/ Revocación	Es importante tener en cuenta que el derecho de cancelación no es absoluto y la Universidad puede negar el ejercicio de este en los siguientes casos: ✔ La solicitud de supresión de la información no procederá cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos, este es el caso de la información educativa, académica y de la historia de los estudiantes en la Universidad Ean. ✔ La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas o académicas. ✔ Los datos sean necesarios para proteger los intereses jurídicamente tutelados del Titular, para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el Titular.
Prueba de la autorización	Se envía la prueba a la oficial de protección de datos.
Informar finalidades	Se envía las finalidades al oficial de protección de datos
Acceder a los datos personales	Se envía la información a oficial de protección de datos

4.5. **Respuesta al Titular**: La Oficial de Protección de Datos Personales responde de fondo la solicitud del titular en un término no mayor a 15 días hábiles.

5. ANEXOS A ESTE PROGRAMA

Anexo No 1: Definiciones
Anexo No 2: Gestores
Anexo No 3: Formato de autorización
Anexo No 4: Plataformas tecnológicas de la Universidad
Anexo No 5: Lineamientos para transferencia internacional en la Universidad Ean
Anexo No 6: Guía de evaluación de impacto datos personales
Anexo No 7: Directrices para la implementación de Nuevas tecnologías e Inteligencia Artificial (IA)

6. HISTORIAL DE VERSIONES DE ESTE DOCUMENTO

Versión	Fecha de aprobación
Primera	2019
Segunda	2022
Tercera	Septiembre de 2022
Cuarta	13 de diciembre de 2022
Quinta	12 de abril de 2023
Sexta	23 de agosto de 2023
Séptima	22 de noviembre de 2023
Octava	24 de abril de 2024
Novena	27 de noviembre de 2024

ANEXO No 1

DEFINICIONES

Las definiciones que se relacionan están en concordancia con la normatividad vigente en materia de protección de datos personales y contextualización la operación de este Manual en la Institución:

1. **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

2. **Dato personal:** Es cualquier pieza de información que por sí misma o en asocio con otra información puede llegar a identificar a una persona. Existen cuatro tipos de datos personales:

2.1. Dato público: Es el dato que no es semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a Reserva. En el dato público no se requiere obtener el consentimiento de su titular para su tratamiento, mientras que, si es privado o semiprivado, se requerirá siempre obtener la autorización previa expresa e informada del titular para su tratamiento.

2.2. Dato semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa al titular y a cierto sector o grupo de personas o a la sociedad en general. Ejemplos: datos financieros y crediticios, dirección, teléfono, correo electrónico.

2.3. Dato privado: Es el dato que solo es relevante para su titular. Ejemplo: fotografías, videos, datos relacionados con su estilo de vida.

2.4. Dato sensible: Es aquel que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación. Ejemplos: origen racial o étnico, orientación política, convicciones religiosas o filosóficas, la pertenencia a

sindicatos, organizaciones sociales, de derechos humanos, partido político, así como los datos relativos a la salud, vida sexual, y los datos biométricos.

3. **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

4. **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

5. **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

6. **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

7. **Encargado del Tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del Tratamiento.

8. **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos

9. **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento. Para la Universidad Ean los titulares son: Estudiantes, Colaboradores, Egresados; y sus familiares, proveedores, contratistas y visitantes.

10. **Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como: la recolección, almacenamiento, uso, circulación o supresión.

11. **Manual Interno de Políticas y Procedimientos – Programa Integral de Gestión de Datos Personales:** Es una herramienta fundamental que da cuenta del compromiso del responsable del tratamiento, al tiempo que es una medida eficaz para evitar cualquier infracción a la política de datos personales.

12. **Evaluación de Impacto:** Herramienta interna que permite una identificación oportuna de los riesgos y generar una trazabilidad material del análisis de los mismos y de potenciales interferencias que puede generar el tratamiento de datos personales, como también el uso de nuevas tecnologías e IA, respecto a los buenos estándares de privacidad y protección de datos personales.

13. **Inteligencia Artificial:** "El CONPES 39754 define la inteligencia artificial como **"(...) un campo de la informática dedicado a resolver problemas cognitivos** comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos".

14. **Privacidad desde el diseño y por defecto:** Es considerada una medida proactiva para, proteger de principio a fin todos los procesos que se relacionen con el tratamiento de datos personales. De esta manera, se garantiza que, tanto los procesos de recolección como el tratamiento mismo y el monitoreo y actualización para la protección de los datos personales, están soportados en herramientas preventivas y transversales que ayudan a prevenir riesgos en esta materia.

ANEXO NO 2

GESTORES

Gestor	Cargo	Proceso	Base de Datos
Mauricio Pardo Rojas	Coordinador II	Contratación y Nómina	Colaboradores
Sandra Rocío Valbuena Castillo	Coordinador II	Registro Académico	Estudiantes
Omaira Yiceth Ramírez Rojas	Coordinador I	Admisiones	Estudiantes
Martha Lucía Prieto Monroy	Coordinador II	Graduados	Graduados
Luis Alexander Zamora	Asistente Técnico	Gestión Documental	Control de Acceso
Jaier Yoary Torres Solis	Profesional I	Bienestar Universitario	Salud Física y Psicológica
Martha Lucía Prieto Monroy	Coordinadora	Graduados	Prácticas Profesionales
Diana Dusley Pinilla León	Coordinador I	Extensión y Proyección Social	Educación Continuada y Extensión
Paola Andrea Bastidas Ramírez	Profesional I	Extensión y Proyección Social	Educación Continuada y Extensión
Jacqueline Calderón Rojas	Coordinador I	Biblioteca - Centro de Recursos para Aprendizaje y la Investigación	Biblioteca
Leidy Paola Fonseca Caro	Coordinador II	Centro de Contacto	Interesados y Aspirantes
Rolf Alexander Ríos Neusa	Coordinador II	Gestión de Proveedores	Proveedores y Contratista
Lucy Guerrero	Gerente	Gerencia de Internacionalización y Relaciones Institucionales	Internacionalización y Relaciones Institucionales
Abelino Hernández Hernández	Coordinador I	Servicios al Estudiante	PQRS
María Ximena Moreno	Profesional II	Assessment Center y Aseguramiento de la Calidad Académica	Proceso Evaluativo de Estudiantes

María Ximena Moreno	Profesional II	Assessment Center y Aseguramiento de la Calidad Académica	Certificaciones
Sandra Patricia Casas Castaño	Director	Dirección de Experiencia Estudiantil	Permanencia Estudiantil
Paola Andrea Franco	Gerente	Instituto para el Emprendimiento Sostenible	Impacta Emprendimiento Sostenible
Juan Manuel Cely	Director	Ean X	Ean X
Lyda Amparo Santos Bustos	Directora	Recursos Financieros	Ean a tu alcance 40/60
Nelson Eduardo Bonilla Ramírez	Coordinador II	Infraestructura y Planta Física	Videovigilancia

ANEXO No 3

FORMATO DE AUTORIZACIÓN DEL TRATAMIENTO DE DATOS PERSONALES

A. Este es el texto al que deben remitir todas las autorizaciones:

AUTORIZACIÓN TRATAMIENTO DE DATOS PERSONAL EN LA U. EAN

Hola:

Queremos contarte que la Universidad Ean, en su calidad de institución de educación superior sin ánimo de lucro con personería jurídica, otorgada mediante Resolución No. 2898 del 16 de mayo de 1969 del Ministerio de Justicia, reconocida académicamente como Universidad por medio de la Resolución 2470 del 30 de mayo de 2006, identificada con NIT. 860.026.058-1, con domicilio principal en la dirección: Calle 71 No. 9 – 84 de la ciudad de Bogotá D.C. y número telefónico 601 – 593 64 64, bajo el desarrollo habitual de sus actividades, actúa como **Responsable del Tratamiento de los Datos Personales**, de conformidad con la Ley 1581 de 2012 el Decreto 1074 de 2015, las Circulares expedidas por la Superintendencia de Industria y Comercio que se puedan relacionar con el Tratamiento de Datos Personales (Ej. Circular 002 y 003 del 21 y el 22 de agosto de 2024, respectivamente), como cualquier norma o regulación que modifique y/o adicione a las anteriores y de conformidad con la Política para el Tratamiento de Datos Personales, disponible en (incluir).

Conforme a lo anterior, necesitamos recabar tu Autorización de forma previa a la entrega de la información personal que te estamos solicitando para las siguientes **finalidades:**

PARA TODOS LOS TITULARES

PARA DARTE ACCESO A LAS INSTALACIONES

Para esto debes proporcionar algunos Datos Personales de identificación y contacto, que pueden incluir tu imagen, huella y análisis biométrico que permite el seguimiento y control de tu acceso a las instalaciones y servicios que presta la Universidad Ean. Entendemos que estos últimos son Datos Sensibles, sin embargo, son indispensables para esta finalidad.

Recuerda que, en caso de requerir comunicarnos contigo, únicamente utilizamos los Datos Personales que hemos solicitado y los suministrados por ti.

PARA CUMPLIR CON LAS FUNCIONES DE SEGURIDAD DE LA UNIVERSIDAD

Contamos con un sistema de videovigilancia (plenamente identificado) que monitorea y puede captar tus imágenes con el objetivo de preservar la seguridad y facilitar el cumplimiento de las funciones académicas, administrativas y disciplinarias de la Institución.

PARA TU PARTICIPACIÓN EN REUNIONES DE TRABAJO Y/O ACADÉMICAS

Es importante que conozcas que algunas actividades académicas, formativas, laborales o de servicios en las que participes pueden ser grabadas por la Universidad Ean y se te podría solicitar el encendido de tu cámara, cuando exista una finalidad admisible.

De igual manera, la Institución es consciente de que las grabaciones y el uso de tu imagen, corresponde al Tratamiento de datos biométricos, los cuales clasifican como de naturaleza sensible, por lo cual serán Tratados con especial cuidado y medidas reforzadas de seguridad.

SI ERES ASPIRANTE, INTERESADO, ESTUDIANTE, REPRESENTANTE LEGAL DE UN ESTUDIANTE, DOCENTE, EMPLEADO (COLABORADOR), PROVEEDOR O CONTRATISTA
[Imagen de Estudiantes, empleados y directivos]

PARA ACOMPAÑARTE EN TU PROCESO DE VINCULACIÓN Y/O EN EL RELACIONAMIENTO QUE TENGAS CON LA UNIVERSIDAD EAN

En este proceso recabamos información personal para adelantar tu vinculación y desarrollar las actividades propias de tu relación contractual con la Universidad, llevar a cabo la prestación de los servicios actuales y futuros ofrecidos por la Institución, darte a conocer las alianzas nacionales e internacionales y convenios que tenemos disponibles para tu desarrollo, divulgar los beneficios, descuentos, becas y programas de financiación a los que te puedes postular, así como verificar tu información académica, financiera, administrativa, judicial y demás que sea necesaria para prestarte nuestros servicios. Ten en cuenta que, para esta finalidad, la Universidad Ean podrá adoptar herramientas tecnológicas para el cumplimiento cabal de nuestras obligaciones.

PARA COMUNICARNOS CONTIGO Y MANTENERTE INFORMADO

Usaremos tus Datos Personales para informarte, enviarte comunicaciones y actualizaciones respecto de tu relación contractual con la Universidad Ean, la prestación de los servicios actuales y futuros, sus términos y condiciones, las actividades de acompañamiento a la comunidad Eanista, las alianzas y convenios nacionales e internacionales que tengamos disponibles para tu desarrollo, los servicios de carácter comercial y publicitario propios o de nuestros aliados, los beneficios, descuentos y becas a los que te puedas postular y programas de bienestar de los que puedas ser parte, así como cambios que puedan presentarse en los servicios de la Universidad.

Al ser una Institución académica vanguardista y propositiva, también necesitamos contactarte para poder informarte, actualizarte y si es el caso, solicitar nuevas Autorizaciones, conforme al uso de nuevas tecnologías que nos permiten prestar mejor nuestros servicios.

Así las cosas, te garantizamos desde la calidad de Responsable del Tratamiento, que cumpliremos con los principios de transparencia, seguridad, calidad de la información, idoneidad, razonabilidad y necesidad, para que la implementación de la tecnología sea bajo las mejores prácticas y conforme a las finalidades éticas correspondientes.

PARA CONOCER TUS NECESIDADES ESPECÍFICAS Y PRESENTARTE OFERTAS Y BENEFICIOS

Para acompañarte en tu relacionamiento con la Universidad, es importante conocer tu opinión y condiciones particulares. Esta información será Tratada con las siguientes finalidades específicas:

a. Conocer la percepción que tienes sobre servicios de la U y la calidad de los mismos.
b. Entender tu afinidad y/o tus preferencias con los programas y servicios de la U y los de sus aliados.
c. Realizar transferencia y/o transmisión de tus Datos Personales tanto a nivel nacional como internacional, atendiendo a tu interés y cumpliendo con los compromisos de Ley.
d. Desarrollar las actividades administrativas necesarias para el relacionamiento con la Universidad Ean, incluyendo emisión de facturación, cobros y pagos, entre otras.
e. Actualizar tu información y la de quienes hayan servido de garantes o codeudores, así como emitir certificaciones.
f. Recabar y salvaguardar tu estado académico, administrativo, disciplinario y/o financiero en la Universidad Ean y tu historial académico/profesional previo, junto con la documentación personal que entregues en el proceso de vinculación a la Institución.

g. Acompañar a los miembros de la comunidad Eanista a través de programas de bienestar de atención psicosocial, actividades deportivas, culturales, de salud, entre otras.

h. Acompañar y ejecutar las acciones disponibles por la Universidad Ean para retener talento y para promover el éxito académico.

i. Informar a terceros (por ejemplo, familiares o acudientes) sobre situaciones relevantes del desarrollo de la relación académica, proponer y gestionar planes de acompañamiento, suministro de información de financiación y pagos.

PARA FACILITAR EL DESARROLLO DE LAS FUNCIONES ACADÉMICAS, ADMINISTRATIVAS Y DISCIPLINARIAS

Algunas actividades académicas y formativas en las que participes pueden ser grabadas a través de las plataformas tecnológicas dispuestas por la Universidad Ean. Así mismo, algunas pruebas virtuales podrán desarrollarse con el apoyo de tecnología que permite registrar el comportamiento del estudiante y su desempeño en las mismas, por lo cual se requerirá de tus registros de imagen y/o de audio, los cuales podrían llegar a tener la naturaleza de sensible, si se aplican técnicas biométricas.

Queremos RECORDARTE que:

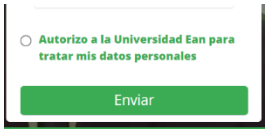
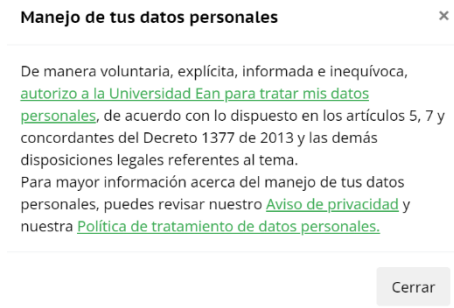
✓ Para acompañar tu formación integral o vínculo con la Universidad podrá ser necesario Tratar Datos Personales relativos a tu historial deportivo, intereses culturales, a tu salud y condición física y sicológica.

✓ Si eres mayor de 12 años y menor de 18 años, tienes la calidad de MENOR ADULTO y por ello tú puedes otorgar directamente la Autorización para informarte sobre el portafolio de programas académicos de la Institución y para garantizarte el acceso y prestación del servicio educativo. En este sentido, la Universidad Ean protegerá tus Datos Personales y sólo los usará para que puedas adelantar tu proceso formativo y hagas efectivo tu derecho a la educación protegido por la Constitución.

✓ Puedes ejercer los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre el Tratamiento de los Datos Personales, mediante escrito dirigido a la UNIVERSIDAD EAN, identificada con NIT 860.026.058 – 1 y teléfono (571) 5936464 a la dirección de correo electrónico habeasdata@universidadean.edu.co, indicando en el asunto el derecho que deseas ejercer, o mediante correo ordinario a la dirección: Calle 79 # 11 – 45, Bogotá, D.C. En caso de que el ejercicio de tus derechos esté relacionado con el uso o tratamiento de tus datos bajo una tecnología o herramienta de IA en específico, te pedimos por favor hacer tu solicitud identificando la tecnología correspondiente.

✓ En caso de querer conocer más sobre nuestras directrices en materia de Tratamiento y protección de Datos Personales te invitamos a conocer nuestra Política para el Tratamiento de Datos Personales y nuestro Aviso de Privacidad.

B. Si pretende recolectar información por vías electrónicas o digitales puede hacer uso del siguiente esquema para obtener la autorización:

De manera previa a la recolección de la información, debe requerirse la autorización, así:	
Cuando el titular de clic en el anterior texto de autorizo a la Universidad Ean para tratar mis datos personales, debe aparecer el siguiente texto:	
Los apartes resaltados en verde en el texto anterior, es decir autorización debe remitir al texto enunciado en el literal A. de este Anexo, así mismo, el titular debe poder tener acceso a la autorización y a la política de tratamiento de la Universidad Ean.	

ANEXO No 4

PLATAFORMAS

EMPRESA	PLATAFORMA/SOFTWARE
EAN / SERVIDOR INTERNO	
MICROSOFT	One Drive
CONSULTORÍA ORGANIZACIONAL	SAP
ITIS SUPPORT S.A.S.	On Base
TIAL SAS	Archivo Físico
CREHANA	Evaluación Y Desarrollo
KI INVERSIONES	Miremos
COLMEDICOS	Exámenes Ocupacionales
INSTRUCTURE	Canvas
BGH WEBEX	WEBEX
PROQUEST COLOMBIA SAS	ALEPH
EDTECH SOLUCIONES DE COLOMBIA S.A.S.	Credity
MERCADOPAGO	Eanx Pasarela de pagos
ALIANZA SUPERIOR S.A.S.	Griky
TELEDISCA	Call Center
LEARNWORLDS	Agencia Digital EanX
GOOGLE	Google Drive
THOMAS SIGNE	Diplomas
ZOOM	CRM
QS UNISOLUTION GMBH	Move On
LOGAN IT SOLUTIONS SAS	Medical Record
INTELINOVA SOFTWARE SL	Training Gym
W-TECH S.A.S.	Proctorizer
ZKTECO COLOMBIA	Zk – Control de Acceso
CERTIKA	Eanx Certificaciones

ANEXO No 5

LINEAMIENTOS PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES DE LA UNIVERSIDAD EAN A TERCEROS FUERA DE COLOMBIA

Nombre del Gestor	
Fecha	

INTRODUCCIÓN

El presente documento busca brindar los lineamientos para regular las actividades relacionadas con la transferencia de Datos Personales de la UNIVERSIDAD EAN a terceros, principalmente otras universidades, fuera de Colombia, considerando el marco legal colombiano de Protección de Datos y como parte del Programa Integral de Gestión de Datos Personales de la Universidad.

Estos lineamientos contribuirán a estandarizar algunas prácticas y procedimientos para lograr el objetivo último de cumplir de manera íntegra y permanente con la ley de Protección de Datos, así como brindar garantías suficientes a los Titulares en el tratamiento de sus Datos Personales, fortaleciendo los elementos para el cumplimiento del principio de responsabilidad demostrada.

Asimismo, también se incluyen algunos lineamientos para la identificación de riesgos asociados a la Transferencia internacional de Datos Personales con terceros.

¿A QUIENES VAN DIRIGIDOS ESTOS LINEAMIENTOS?

Estos lineamientos están concebidos para facilitar la comprensión y adecuada aplicación del marco legal colombiano de Protección de Datos y de los procedimientos internos de la Universidad EAN, especialmente para aquellos que pretendan realizar transferencias internacionales de datos de la Universidad EAN a terceros ubicados fuera de Colombia.

¿CUÁL ES EL MARCO LEGAL?

El marco legal colombiano de Protección de Datos está compuesto principalmente por la Ley 1581/2012 y sus decretos reglamentarios (Decreto 1074/2015).

Asimismo, la Autoridad colombiana de Protección de Datos (Superintendencia de Industria y Comercio – SIC) ha emitido lineamientos específicos relacionados con el principio de responsabilidad en la transferencia internacional de Datos Personales, los cuales también son tomados en cuenta.

CUESTIONARIO DE EVALUACIÓN

La Universidad EAN en este documento, llevará el registro de los aspectos de esta evaluación de riesgo de la transferencia y debe ser firmada por el Oficial de Datos, el Gestor de la Base de Datos y el Coordinador de Seguridad de la Información.

De acuerdo con el marco legal aplicable, los lineamientos de la SIC y los procedimientos internos de la Universidad EAN para el tratamiento de Datos Personales, la Universidad, a través del gestor, debe evaluar el riesgo de la transferencia internacional a terceros verificando lo siguiente:

¿A quién se transferirían los datos? A qué persona jurídica se transferirán los Datos Personales, para que el destinatario actúe como Responsable del Tratamiento de los Datos Personales.

RTA/

¿A dónde se transferirán los datos? ¿La persona jurídica está ubicada en un país considerado por la SIC con estándares adecuados de protección de Datos Personales?

La SIC ha declarado que los siguientes son países con niveles adecuados de protección: Alemania, Australia, Austria, Bélgica, Bulgaria, Chipre, Croacia, Costa Rica, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos de América, Estonia, Finlandia, Francia, Grecia, Holanda, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, México, Noruega, Perú, Polonia, Portugal, Reino Unido, República de Corea, República Checa, Rumania, Serbia, Suecia, y los países que han sido declarados con el nivel de protección adecuado por la Comisión Europea (Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Feroe, Andorra, Israel, Uruguay y Nueva Zelanda).

RTA/

¿Qué tipo de Datos Personales se transferirán? Semiprivado, privado, sensible

RTA/

¿La Universidad EAN cuenta con autorización del Titular para transferir sus Datos Personales? La Universidad EAN deberá asegurarse de que los Titulares cuyos datos serán

transferidos hayan dado su consentimiento para la transferencia internacional de sus Datos Personales. La Universidad EAN deberá poder acreditar el medio y fecha en que el Titular brindó la autorización correspondiente.

RTA/

¿Cómo se transferirán los datos? Dependiendo de la cantidad de datos y los tipos de Datos Personales involucrados (según la sección 4.3), la Universidad EAN transferirá los datos (directamente o a través de un Encargado) por medios seguros, por ejemplo, mediante el envío de archivos cifrados o carpetas con contraseña para abierto, y con acceso limitado del personal del destinatario.

RTA/

¿Para qué fines se transfieren los datos? La Universidad EAN definirá y limitará los fines de la transferencia, ya que, si bien el destinatario actuará como Controlador al igual que la Universidad EAN, los usos de los Datos Personales por parte del destinatario deberán ser coherentes con los usos autorizados por el Titular.

RTA/

¿Por cuánto tiempo? El destinatario deberá hacer uso de los Datos Personales por un período de tiempo determinado o mientras no se haya agotado la finalidad, el cual no podrá exceder del plazo por el cual el Titular dio su consentimiento a la Universidad EAN.

RTA/

¿Pueden existir transferencias ulteriores de Datos Personales? Es clave evaluar si el destinatario tiene previsto realizar transferencias posteriores de los Datos Personales a terceros (es decir, otras empresas o universidades) y dónde están ubicadas estas empresas. La Universidad EAN trabajará bajo estándares de mejores esfuerzos para garantizar que los Datos Personales que recolecte serán resguardados y procesados de manera segura, incluso después de haber sido transferidos al primer destinatario.

RTA/

¿Cuáles son las Personas o área de contacto del tercero que recibirá la información? Tanto la Universidad EAN como el destinatario deberán designar una persona o área de contacto encargada de cada transferencia (o grupo de transferencias si se realizan periódicamente) de Datos Personales.
RTA/
¿Después de esta evaluación de riesgos se considera necesario hacer la transferencia?
RTA **SI** **NO**

Si la respuesta anterior, fue positiva, se debe continuar con el siguiente formulario de lo contrario no, donde se plantean algunas cuestiones adicionales que deben acordarse para asegurar una transferencia adecuada y garantizar la integridad, confidencialidad y seguridad de los Datos Personales incluso después de la transferencia.

Privilegios de acceso a la información: en virtud del principio de confidencialidad, la Universidad EAN y el destinatario deberán informar qué áreas de cada parte tendrán acceso a los Datos Personales objeto de la transferencia, y determinar si es conveniente establecer mayores privilegios (cifrado, contraseñas de archivos y carpetas, etc.) para salvaguardar los datos que se comparten entre las empresas. En todo caso, debe ser absolutamente claro quién entrega y quién recibe la información y el medio.	RTA/
Preguntas y reclamos de los Titulares de los Datos: los Titulares de los Datos pueden plantear preguntas o reclamos en relación con el procesamiento de los Datos Personales objeto de la transferencia. Tales consultas y/o	RTA/

reclamos pueden estar relacionados con el tratamiento que realiza la Universidad EAN y/o el destinatario de los datos en su rol de Responsable. Adicionalmente y si es posible, se procurará acordar lo siguiente entre las partes: • Un procedimiento interno y tiempos para comunicar dichas consultas y/o reclamos en forma oportuna y eficiente entre las empresas; • Acordar qué parte estará obligada a dar respuesta al Titular de los datos; y • Acordar un canal y área/persona que será responsable de recibir y procesar estas comunicaciones dentro de cada parte.	
Incidentes de seguridad relacionados con los Datos Personales: la Universidad EAN y el destinatario procurarán comunicarse oportunamente entre ellos cualquier violación de datos que involucre los Datos Personales objeto de transferencia. Lo anterior es importante para contribuir a cumplir con la obligación de la Universidad EAN de reportar los incidentes de datos personales a la SIC dentro de los 15 días hábiles siguientes al conocimiento de la ocurrencia de la violación de datos, así como en cuanto a la necesidad de evaluar si la Universidad EAN deberá informar los Titulares de la ocurrencia de la violación de datos.	RTA/
Seguimiento de transferencias ulteriores: durante el tiempo en el que el destinatario	RTA/

actúe bajo el mismo consentimiento otorgado por el Titular a la Universidad EAN, ésta deberá entender y ser notificada de las transferencias posteriores que pretenda y/o realice el destinatario de los Datos Personales, para garantizar que dichas transferencias posteriores se realicen a países con niveles adecuados de protección y de una manera que asegure la protección de los Datos personales de los Interesados. La Universidad EAN deberá consultar periódicamente (anualmente) si el destinatario ha realizado o tiene previsto realizar alguna transferencia posterior de los Datos Personales.	
Trazabilidad e indicadores de seguimiento: la Universidad EAN deberá llevar un registro de su responsabilidad demostrada en la elaboración y seguimiento de la transferencia. Llevar un registro de las transferencias también es un buen medio para generar indicadores sobre el volumen de transferencias, países receptores, identificación de brechas de datos, reclamos relacionados con la transferencia, entre otros.	RTA/
Política de Tratamiento de Datos: *Adjuntar la Política de Tratamiento de Datos de la entidad o institución con la que se considera realizar la transferencia de información.*	

EL oficial de Datos en conjunto con el gestor enviará una carta de recomendación al tercero que recibirá los datos con la información más relevante que demuestre el compromiso de la Universidad Ean en una adecuada gestión de los datos.

En constancia firman

GESTOR DE LA BASE DE DATOS

OFICIAL DE DATOS PERSONALES

COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN

ANEXO No 6

EVALUACIÓN DE IMPACTO DE PRIVACIDAD

Universidad Ean

V3 21 de octubre de 2024

Esta evaluación es un instrumento de aproximación previa, a la implementación de un proyecto de mejora o innovación o implementación de nuevas tecnologías y herramientas de Inteligencia Artificial (IA) en la Universidad Ean, a través del cual, se analizará el impacto que esas potenciales nuevas herramientas a implementar, podrían traer en los procesos actuales relacionados con el Tratamiento de datos personales de la Institución y determinar medidas que mitiguen los riesgos previsibles y en todo caso, la Universidad pueda tomar decisiones bajo principios de necesidad, razonabilidad y transparencia si los nuevos proyectos sobre la mesa tiene una viabilidad eficiente o tal vez no. Para más información puede consultar la Guía de Oficial de Protección de Datos de la SIC de 2023.

El Oficial de Protección de Datos, el supervisor o solicitante del contrato y/o proyecto y el Coordinador de Seguridad de la Información de la Universidad Ean, son los responsables de diligenciar este formulario, siempre y cuando se trate de una relación jurídica y/o comercial donde se traten los datos personales.

El uso y redacción de este instrumento deben estar alineados con el cumplimiento de los artículos 15 y 20 de la Constitución Política; los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012 (por la cual se dictan disposiciones generales para la Protección de Datos Personales) (en adelante LEPD); y el artículo 13 del Decreto 1377 de 2013 (Hoy compilado en el Decreto 1074 del 2015), por el cual se reglamenta parcialmente la Ley anterior. Así mismo, en lo referente a datos de carácter financiero y crediticio estará sujeta a la Ley 1266 de 2008. De igual manera, la Universidad Ean, se acoge a las iniciativas regulatorias pertinentes para el uso e implementación de este instrumento, por parte de la Superintendencia de Industria y Comercio, incluyendo las Circulares relacionadas con la protección de datos personales y el flujo de los mismos, como pueden ser, pero sin limitarse la Circular 002 y 003 del 21 y 22 de agosto de 2024, como también las cartillas y material no vinculante como puede ser la guía para el cumplimiento del principio responsabilidad demostrada.

De igual manera, la valoración y evaluación del impacto deberá tener en cuenta los siguientes conceptos y principios que soportan el quehacer de la Universidad conforme a las buenas prácticas

relacionadas con la protección de Datos Personales y estándares de seguridad, dentro de un contexto de uso de nuevas tecnologías e IA frente a dichos Tratamientos:

- **Principio de idoneidad:** El tratamiento es capaz de alcanzar el objetivo propuesto.
- **Principio de necesidad:** No existe otra medida más moderada en cuanto al impacto de las operaciones de tratamiento en la protección de datos personales e igual de eficaz para conseguir tal objetivo.
- **Principio de razonabilidad:** El tratamiento debe estar orientado a cumplir finalidades constitucionales.
- **Principio de proporcionalidad en sentido estricto:** Las ventajas obtenidas como consecuencia de la restricción del derecho a la protección de datos no deberán ser superadas por las desventajas de afectar el derecho al Habeas Data.

Inteligencia Artificial: "El CONPES 39754 define la inteligencia artificial como "(...) un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos".

Privacidad por diseño: Privacidad por diseño el conjunto de medidas que permitan actuar de manera preventiva y que se insertan desde el inicio del procesamiento de datos y/o del proyecto de inteligencia artificial.

Privacidad por defecto: Es una estrategia globalmente conocida para atender las obligaciones derivadas del tratamiento y protección de datos personales, bajo la premisa general de que el tratamiento de datos sea el mínimo posible y justo el necesario, salvaguardando bajo herramientas de carácter más restrictivo la privacidad de los Titulares.

Este formato de evaluación estará vigente durante toda la relación jurídica, **siempre y cuando las condiciones del tratamiento de datos no varíen**, si estas llegan a cambiar, será necesario elaborar otra evaluación de impacto.

Evaluación

1- **¿Cuál es el objeto del contrato?** **Compra de 225 licencias para la plataforma Platzi para cursos de idiomas en la ruta de bilingüismo de profesores**

2- **Por favor relacione claramente la identificación del contratista:**

Nombre: PLATZI SAS
Identificación: 900.594.524-0

3- **¿El proyecto/contrato involucra datos personales de lo que trata la Universidad Ean?**

SI ☒ **NO☐**

4- **El tercero/contratista tiene política de Protección de datos o seguridad de la información, si marca si, por favor adjuntarla.**

SI ☒ **NO☐**

5- **¿Esos datos personales son de menores de edad o sensibles o población vulnerable?**

SI ☐ **NO☒**

Si la respuesta es SI. Especifique los datos que se trataran:
Menores de edad, grupos étnicos, población en situación de discapacidad y víctimas del conflicto armado, personas privadas de la libertad, mujeres cabeza de hogar, reintegrados y adulto mayor.

6- **¿Los datos serán sometidos a análisis biométricos?**

SI ☐ **NO☒**

7- **Para determinar si este tratamiento es a gran escala responda las siguientes preguntas:**

7.1. Número de personas impactadas: *75*

7.2. Duración del tratamiento *1 año*

8- **¿El proyecto implica actividades de videovigilancia de los titulares, a través de métodos de geolocalización?**

SI ☐ **NO☒**

9- **¿El proyecto/contrato contempla medidas intrusivas?** [*Se entiende como medidas intrusivas aquellas actividades o procesamientos o herramientas de investigación o búsqueda que compilan información personal de los titulares sin el conocimiento de estos y que puede afectar los derechos fundamentales, por ejemplo: comunicaciones privadas.*]

SI ☐ **NO☒**

Si la respuesta es SI. Especifique las medidas intrusivas:

Explique y enumere las medidas

10- **¿Este proyecto/contrato elaborará perfiles de los titulares?**

SI ☐ **NO☒**

Si la respuesta es SI. Especifique los perfiles:

Explique y enumere los perfiles

11- **Se pretende usar los datos personales para fines exceptuados por la ley**

SI ☐ **NO☒**

Si la respuesta es SI. Especifique qué otros fines:

Explique los fines

12- **¿Se compartirán datos personales con terceros, diferentes al contratista, es decir este hará transferencias ulteriores?**

SI ☒ **NO☐**

Si la respuesta es SI, especifique con quien y qué garantías de protección, seguridad y estabilidad en materia de la calidad de los datos ofrecen.

Podrá realizar transmisiones o transferencias entre su casa matriz, filiales, subsidiarias, sucursales y grupo empresarial.

13. **¿El proveedor utiliza cifrado obligatorio para proteger la información de identificación personal?**

SI ☐ **NO☒**

14. **¿Se implementan controles de cifrado para la transmisión de este tipo de información?**

SI ☐ **NO☒**

15. **¿Este proyecto/contrato supone la transferencia internacional de datos?**

SI ☐ **NO☐**

Si la respuesta es SI. Especifique a qué países (Recuerde que, para transferencias internacionales, debe revisar el Manual de Directrices y Procedimientos):

Escriba el nombre de los países

Conclusiones

Riesgos encontrados *Detalle los riesgos que se encuentran en esta operación*
Controles **Firmar un documento en donde se establezcan las consideraciones relacionadas con datos personales, cuando los titulares entregan su información en la Plataforma Platzi.** *Detalle los controles y su estrategia de mitigación, con responsabilidades claras, fechas y entregables de ser necesario*

En constancia se suscribe en la *Seleccione la fecha de elaboración*

Firma: Oficial de Protección de Datos

Firma: Coordinador de Seguridad de la Información

Firma: Supervisor o solicitante del proyecto o contrato

ANEXO No 7:

DIRECTRICES PARA LA IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS E INTELIGENCIA ARTIFICIAL (IA)

Los avances en la tecnología y los nuevos retos que trae consigo la Inteligencia Artificial (IA) hacen que el sector educativo no pueda ser indiferente a sus desafíos. Es por esto que, la Universidad EAN ha identificado la necesidad de tener un entendimiento previo, pero sobre todo actualizado y en constante evolución, como también unos acuerdos y directrices de buenas prácticas y usos no restrictivos pero si guiados hacia un bien común, que le permitan tanto a la Institución como a los grupos de interés, relacionarse con la implementación de nuevas herramientas tecnológicas y/o de IA, de manera informada, con buenos criterios preventivos y con optimismo consciente.

En el presente anexo, se establecen las directrices para tener en cuenta, cuando los proyectos de innovación e implementación de nuevas tecnologías e IA traigan, impactos a los procedimientos y a los estándares de protección de datos personales, que la Institución ya tiene implementados, respecto a sus bases de datos y, en general, al tratamiento de datos personales, bajo su rol de Responsable del tratamiento.

Entendiendo que el uso ético y razonable de la IA y las nuevas tecnologías debe mirarse con flexibilidad y adaptación, para que nuestros docentes, áreas administrativas y estudiantes aprovechen las eficiencias de la tecnología, desde la posibilidad de recibir una educación más personalizada y con herramientas y criterios para los desafíos del futuro, y la automatización de procesos que permitan abrir más espacios para desarrollar nuevos proyectos administrativos y de investigación.

A continuación, se establen los principios normativos y las buenas prácticas que no se pueden perder de vista en esta materia, las necesidades puntuales a atender frente a la posibilidad de entrada de nuevas tecnologías y herramientas de IA a las operaciones habituales de la Universidad, y algunas herramientas que podrán utilizarse y personalizarse, para cada proyecto o necesidad de una nueva herramienta tecnológica, como un ejercicio de trazabilidad y responsabilidad demostrada, capaz de ir evaluando el caso a caso, entendiendo que cada nueva herramienta y sus alcances tienen sus propias características y particularidades.

¿Qué normas y principios no podemos perder de vista?

- Cumplir las normas locales sobre tratamiento de datos personales, incluidas, pero sin limitarse a la Ley 1581 de 2012 el Decreto 1074 de 2015, las Circulares 002 y 003 de agosto de 2024, expedidas por la Superintendencia de Industria y Comercio, y cualquier otra norma que adicione y/o modifique el marco regulatorio.

- También hay que considerar los estudios y conceptos de organizaciones mundiales, regionales y locales (UNESCO, Banco Mundial, OMPI, Autoridades de la Unión Europea, entre otras) que generan trazabilidad sobre cómo establecer usos éticos de las nuevas tecnologías y la IA, sobre todo cuando afectan a la protección de datos personales.

- Respecto a los principios que no se debe perder de vista para la lectura y materialización de este Anexo, se resaltan los principios de Transparencia, de Idoneidad, Proporcionalidad, Necesidad y Razonabilidad que han sido explicados dentro del capítulo/ Tabla de los Principios aplicables al tratamiento de datos personales en la Universidad Ean, del presente Manual de procedimientos y que se estarán atendiendo con el ejercicio de identificación de necesidades a atender en esta materia, las recomendaciones a continuación y las herramientas desagregadas que se proponen para la materialización de las directrices del presente Anexo.

¿Qué necesidades tenemos y qué recomendaciones debemos tener en cuenta?

- Implementación de la privacidad bajo diseño y por defecto, con el fin de continuar con las buenas prácticas que ya se han implementado en la materia y poder reforzar las estrategias y herramientas del programa de gestión de datos personales, cuando de la entrada de nueva tecnologías y/o IA se trate, mediante ejercicios de acompañamiento permanente, directrices preventivas o que por lo menos contengan el impacto negativo de la funcionalidad y permite tener información y herramientas para la trazabilidad, evolución y monitoreo del uso de la tecnología escogida, para así poder custodiar el proceso de principio a fin, bajo un contexto de análisis puntual de cada proyecto o cada potencial entrada de una nueva tecnología.
- Diferenciar el grupo de interés o las personas de la Comunidad Eanista que usen o implementen IA. De esta manera se podrán evaluar los impactos conforme a las decisiones de las áreas operativas, la perspectiva de nuestros docentes y fomentar la investigación ética en el campo de la IA por parte de los estudiantes.

- Reconocer los derechos de los titulares de datos personales, que se puedan ver impactados por el uso de nuevas tecnologías y/o IA. Específicamente, los titulares tienen derecho a recibir la información suficiente y de manera transparente, de la IA, sus alcances y características, siempre que logre probar el impacto causado por el uso de la nueva tecnología.

Los titulares también tienen derecho a no aceptar tratamientos automatizados de sus datos personales como también conocer los fundamentos éticos que llevaron al Responsable del tratamiento, a utilizar una nueva tecnología que tiene nuevos alcances los cuales debe ser previamente informados y autorizados por ellos.

- Hacer explícitos los principios y valores que guiarán el uso de herramientas de IA a todas las áreas involucradas .
- Es necesario establecer estándares de calidad para la recolección de los datos que nutrirán las herramientas de IA, Lo anterior para cumplir con el principio de calidad de la información y poder aportar como valor agregado y como ejemplo de buenas prácticas a los procesos de machine learning e IA generativa, dentro del sector de la educación.
- Efectuar estudios de impacto de privacidad y de seguridad.
- Necesidad de una visión flexible y con nuevos niveles de adaptabilidad. La Institución y los grupos de interés de la Comunidad Eanista, siempre deberán recordar la necesidad de adaptación confirme a los nuevos desafíos que surjan en materia de cumplimiento y operación de la IA y las nuevas tecnologías, como parte de las tareas relacionadas con la constante actualización sobre la materia.

¿qué herramientas debemos estructurar y aplicar?

- Contratos/Convenios/Acuerdos con los encargados de datos personales.
- Utilizar los formatos de Evaluaciones de Impacto y matrices de riesgo que ayuden a identificar y monitorear los niveles adecuados de seguridad de la información personal y la prevención de impacto negativo al tratamiento de datos personales de terceros.
- Espacios de socialización y actualización.
- Ejercicios de investigación y actualización de directrices aceptadas en el sector y Capacitaciones al respecto.
- Aterrizar espacios de retroalimentación periódica, sobre la IA o nueva tecnología implementada, posterior a un tiempo razonable de haberla puesto en funcionamiento.
- Segmentación de los grupos de interés de la Universidad, frente a cada proyecto de nuevas implementaciones tecnológicas, para determinar cuáles serían los titulares potencialmente impactados y qué tipo de información personal estaría involucrada, entendiendo que no todas las herramientas tienen usos transversales o 360 dentro de la Institución.
- Plan de auditoría y evaluación de si la IA o nueva tecnología usada, cumple con los principios aquí dispuestos y con generar valores agregados en materia de eficiencia y servicios de la Universidad.

- Contratación y/o colaboración con expertos en materia de política pública y procesos de implementación de buenas prácticas al respecto, para soportar la responsabilidad de la Universidad de mantenerse en constante actualización al respecto.
- Utilizar herramientas de anonimización en los proyectos que sea posible y así se disminuyen los riesgos o el impacto relacionado al tratamiento de datos personales y sus exigencias técnicas y legales.
- Fomentar la colaboración con otras universidades y organizaciones para compartir conocimientos y experiencias en el ámbito de la IA.
- Reconocer que las directrices deberán ser actualizadas periódicamente para adaptarse a los rápidos avances en el campo de la IA.
- Utilizar la IA como una herramienta complementaria a la enseñanza tradicional.
- Promover el desarrollo de habilidades críticas y creativas en los estudiantes.
- Garantizar que la IA no sustituya la interacción humana entre profesores y estudiantes.
- Asegurar que la investigación con IA cumpla con los principios anteriormente mencionados.

FIN DEL DOCUMENTO