Cédula de Documento
Sellado

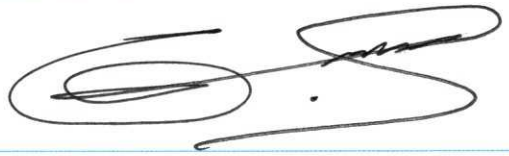
Información de Documento Sellado Digitalmente	
Entidad universitaria	Coordinación de Vinculación y Transferencia Tecnológica
Nombre del documento	CVTT-DocumentoSeguridad-DatosPersonales-20220815-vPublica.pdf
Tipo de documento	Otro
Identificador único del documento	lauRQqKMpXUAMN4pU9IKR87bl9aCC3mPQL83HFNYeP0=
Número de páginas	388
Fecha de emisión del sello	26 de agosto del 2022 a las 03:45 PM

Información de la Entidad Emisora del Sello	
Entidad universitaria	Dirección de Información y Transformación Digital CVTT

Este es un comprobante de la recepción de un documento
emitido y sellado digitalmente en la UNAM.
Esta cédula es informativa y
no forma parte del documento sellado al que hace referencia.

Documento de Seguridad de Datos Personales

Tabla de autorización

Elaboró	**Ing. Alejandro Arturo Ortega Hernández** Coordinador de Información para Vinculación Universitaria alejandro.ortega@unam.mx Tel. (55) 56585650 Ext. 236	
Elaboró	**Ricardo Albarrán Romero** Jefe del Departamento de Soporte Técnico ricardoalbarran@unam.mx Tel. (55) 5658 5650 Ext. 225	
Elaboró y revisó	**L. I. Alma Rosa García Martínez** Directora de Información y Transformación Digital y Responsable técnico de datos personales almagm@unam.mx Tel. (55) 56585650 Ext. 234	
Revisó	**Lic. Óscar Ramírez González** Jefe de la Unidad Administrativa y Responsable administrativo de datos personales oscarrag@unam.mx Tel. (55) 5658 5650 Ext. 220	
Revisó	**Mtra. Claudia Llanos Argüello** Directora Jurídica y Responsable de datos personales cllanosa@unam.mx Tel. (55) 56 58 5650 Ext. 218	
Aprobó	**Dr. Jorge Vázquez Ramos** Coordinador de Vinculación y Transferencia Tecnológica jorman@unam.mx Tel. (55) 5658 5650 Ext. 211	
	Fecha de emisión	15 de agosto de 2022
	Fecha de actualización	17 de agosto de 2022

Contenido

Introducción

El presente documento establece las medidas de seguridad y controles de carácter administrativo, físico y técnico aplicables a los Sistemas de Tratamiento de Datos Personales (STDP) que forman parte del Sistema de Gestión de Seguridad de Datos Personales (SGSDP) de la Coordinación de Vinculación y Transferencia Tecnológica (CVTT) de la UNAM, para se protejan los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y se garantice su confidencialidad, integridad y disponibilidad.

El Documento de Seguridad de Datos Personales tiene como propósito identificar los STDP, documentar las actividades realizadas para integrar el SGSDP, identificar los datos personales en posesión de la CVTT, identificar roles, funciones y responsabilidades de cada sistema y documentar las medidas de seguridad implementadas.

Objetivo

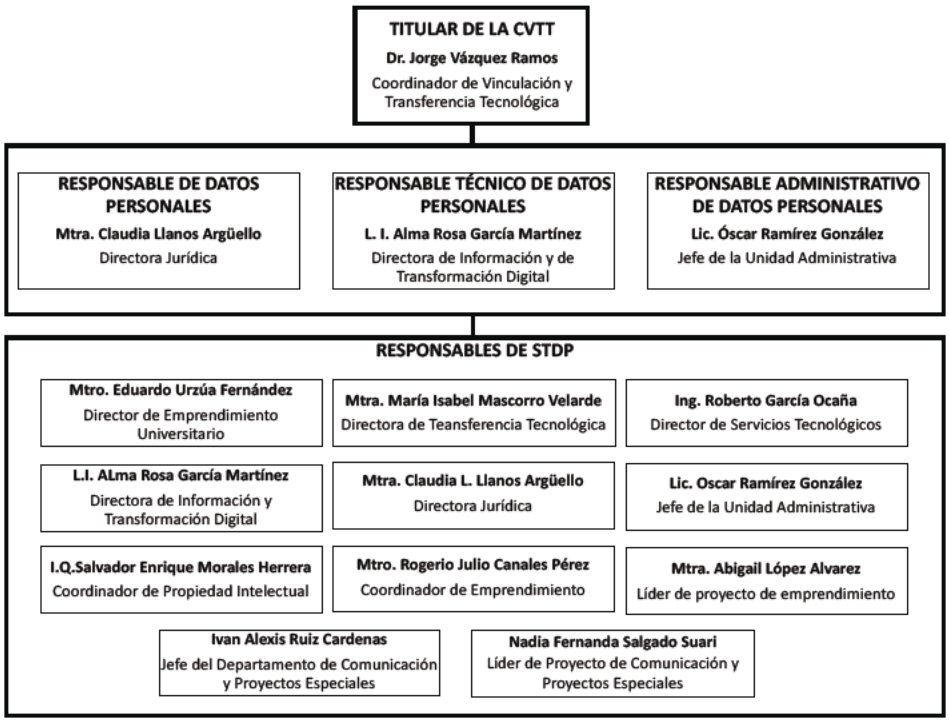
Describir las medidas de seguridad implementadas en el Sistema de Gestión de Seguridad de Datos Personales (SGSDP) para la protección de datos personales en posesión de la CVTT durante todo el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión, tomando en cuenta lo contenido en la normatividad que emita el Comité de Transparencia de la UNAM.

Alcance

El SGSDP aplica para todas las áreas de la CVTT en posesión de datos personales y datos personales sensibles.

Roles, funciones y responsabilidades

Los roles, funciones y responsabilidades dentro del SGSDP del personal que participa en el tratamiento de datos personales son los siguientes:



Titular de la CVTT

Verificar el cumplimiento del Sistema de Gestión de Seguridad de Datos Personales en todas las áreas de aplicación de la CVTT.

Responsable de seguridad de datos personales

Verificar el cumplimiento del Sistema de Gestión de Seguridad de Datos Personales en las áreas específicas de aplicación de la CVTT. Mantener actualizado el Documento de Seguridad de Datos Personales. Verificar que el SGSDP cumpla con los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México y las Normas Complementarias.

Responsable técnico de datos personales

Verificar el cumplimiento del Sistema de Gestión de Seguridad de Datos Personales en lo referente a medidas técnicas en las áreas específicas de aplicación de la CVTT. Colaborar en mantener actualizado el Documento de Seguridad de Datos Personales. Verificar que el SGSDP cumpla con los Lineamientos técnicos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México y las Normas Complementarias.

Responsable administrativo de seguridad de datos personales

Verificar el cumplimiento del Sistema de Gestión de Seguridad de Datos Personales en lo referente a medidas administrativas y físicas en las áreas específicas de aplicación de la CVTT. Colaborar en mantener actualizado el Documento de Seguridad de Datos Personales. Verificar que el SGSDP cumpla con los Lineamientos administrativos y físicos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México y las Normas Complementarias.

Responsables de STDP

Dar cumplimiento y mantener el SGSDP en sus áreas específicas de aplicación. Colaborar en la actualización continua del Documento de Seguridad de Datos Personales.

Involucrados en las actividades de tratamiento

Llevar a cabo sus actividades en los STDP de acuerdo a sus funciones y obligaciones cumpliendo con el SGSDP, los Lineamientos para la Protección de Datos Personales en Posesión de la UNAM y las Normas Complementarias.

Sistema de Gestión de Seguridad de Datos Personales

Objetivo

El objetivo del Sistema de Gestión de Seguridad de Datos Personales es establecer, mantener y revisar las medidas de seguridad y controles de carácter administrativo, físico y técnico para la protección de los datos personales que los protejan contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y garanticen su confidencialidad, integridad y disponibilidad, conforme a las Normas Complementarias que emita el Comité de Transparencia de la UNAM.

Inventario de sistemas de tratamiento de datos personales

El primer paso para establecer las medidas de seguridad es identificar los sistemas de tratamiento de datos personales en posesión de la CVTT. Para tal efecto se llevó a cabo un inventario de sistemas de tratamiento de datos personales el cual contiene la denominación específica de cada sistema, el tipo de datos personales que contiene cada uno, los responsables, encargados y usuarios de cada sistema (ver Anexo 1. Inventario de sistemas de tratamiento de datos personales).

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Para describir adecuadamente cada uno de los STDP se detalla el soporte en el que se encuentran los datos, por ejemplo, para soportes físicos podrían ser formatos, listados, documentos o expedientes, entre otros y para soportes electrónicos, hoja de cálculo o base de datos relacional, entre otros.

Se especifican, además, las características del lugar donde se resguardan los soportes, tal como:

- Para soportes físicos, se incluye una descripción con detalles sobre las características físicas de la oficina, almacén o bodega donde resguarda dichos soportes;
- Para soportes electrónicos, la descripción incluye un diagrama de la arquitectura de seguridad en el cual sea posible apreciar el flujo de datos a través de la o las redes electrónicas que interconectan los equipos (clientes, servidores, cortafuegos, unidades de almacenamiento, entre otros) del sistema de tratamiento de datos personales. Adicionalmente, se describen las medidas de seguridad física que se han implementado para la protección del centro de datos donde residen los soportes.
- En caso de que el sistema de tratamiento de datos personales ocupe ambos tipos de soportes, se presentan las descripciones correspondientes a cada uno, en términos de lo señalado en los incisos a) y b) anteriores.

(Ver Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales y Anexo 3. Diagramas de arquitectura).

ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA

Se llevó a cabo un análisis de utilizando la metodología de Análisis de Riesgo BAA , la cual fue creada por Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

La metodología se enfoca en tres factores que afectan la percepción del valor de los datos personales para un atacante:

1) **Beneficio** para el atacante. Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).
2) **Accesibilidad** para el atacante. Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero).
3) **Anonimidad** del atacante. Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente a las instalaciones de una empresa).

El objetivo de la metodología es realizar una clasificación de los datos personales en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección.

Una vez clasificación de los datos, la metodología establece define listas y patrones de control que agrupan medidas de seguridad basadas en ISO/IEC 27002 que son recomendados de protección de datos de acuerdo al entorno de riesgo existente los cuales se agrupan en seis tipos:

- CB: Patrón de control de medidas de seguridad básicas
- DMZ: Patrón para accesos desde entornos de alta anonimidad.
- CF: Patrón de Caja fuerte.

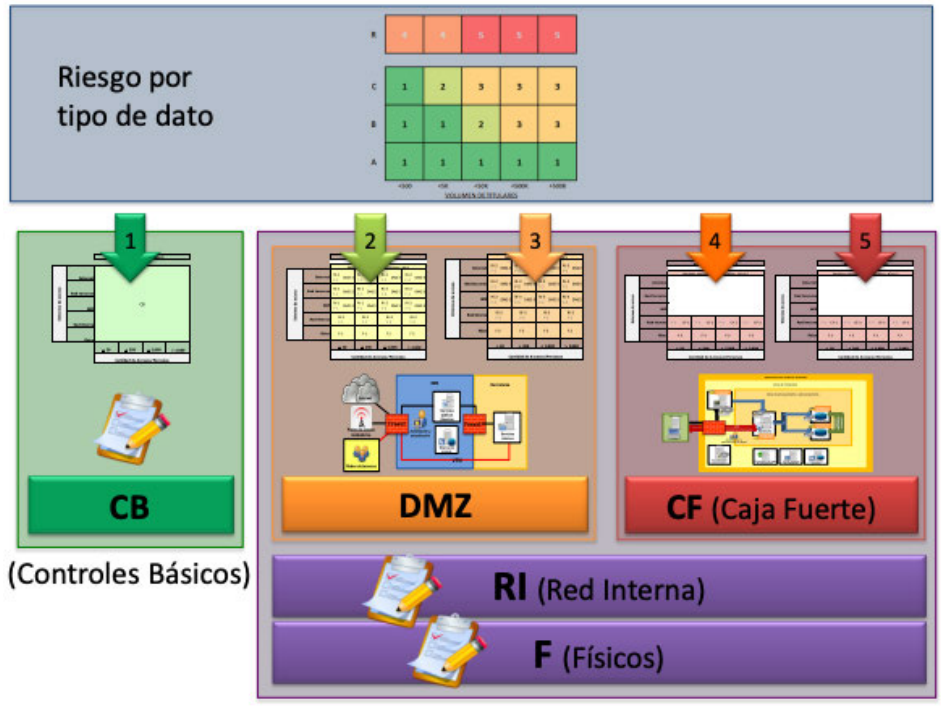
- AD: Lista de medidas administrativas.
- RI: Lista de medidas de seguridad aplicable para accesos desde la red interna.
- F: Lista de medidas de seguridad aplicable para accesos desde el entorno físico.

Con estas listas y patrones se llevó a cabo un análisis de brecha para identificar las medidas de seguridad existentes y efectivas, así como aquellas faltantes.

Para conocer el detalle de la metodología consultar el Anexo 4: Metodología de análisis de riesgo y análisis de brecha, a manera de resumen los pasos a seguir son:

1. Identificar el riesgo por tipo de dato, de acuerdo con los datos personales que se tratan (nivel de riesgo inherente).
2. Con el nivel de riesgo inherente, se procede a buscar la tabla de control que le corresponde a ese nivel, para en ella utilizar como coordenadas las otras dos variables: accesibilidad y anonimidad.
3. Utilizando el grado de accesibilidad y anonimidad, es decir, desde dónde se accede a los datos (anonimidad) y qué cantidad de accesos existen (accesibilidad), se identifica la celda correspondiente en la cual se identificarán las listas y patrones de controles que se requiere implantar.

Imagen 1 Resumen de metodología



El detalle del ejercicio para los STDP se puede consultar en el Anexo 5. Análisis de riesgos y análisis de brecha.

PLAN DE TRABAJO

Se elaboró un plan de trabajo que define las actividades que se llevarán a cabo para implementar los controles de seguridad identificados en el análisis de brecha como faltantes, faltantes priorizando las medidas de seguridad más relevantes con base en el riesgo detectado y la cantidad de STDP involucrados. Lo anterior, considerando los recursos asignados, el personal interno y externo al área, así como las fechas establecidas para la implementación de los controles de seguridad nuevos o faltantes.

El detalle del Plan de Trabajo se encuentra en el Anexo 6. Plan de Trabajo.

CAPACITACIÓN

El Plan de trabajo contempla actividades para la concienciación, educación y entrenamiento de seguridad de la información que tienen por objeto capacitar a los involucrados internos y externos, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos, tomando en cuenta lo siguiente:

1. Los requerimientos y actualizaciones del Sistema de Gestión de Seguridad de Datos Personales;
2. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
3. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
4. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Anexo 1

Inventario de sistemas de tratamiento de datos personales

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

COORDINACIÓN DE VINCULACIÓN Y DE TRANSFERENCIA TECNOLÓGICA

Inventario General de Sistemas de Tratamiento de Datos Personales

Fecha 15 de Agosto de 2022

ID	Nombre completo del STDP	Actualización
CCPE-01	Actualización Directorio UNAM	15/ago/2022
CCPE-02	Administración de los sitios Web de la CVTT	15/ago/2022
CCPE-03	Levantamiento y proceso de multimedia	15/ago/2022
DEU-01	Talleres de emprendimiento	15/ago/2022
DEU-02	InnovaUNAM	15/ago/2022
DEU-03	Incubación de Base Tecnológica	15/ago/2022
DEU-04	Incubación de Empresas Sociales	15/ago/2022
DEU-05	Guías para el emprendimiento profesional	15/ago/2022
DEU-06	Emprende con Santander X y la UNAM	15/ago/2022
DITD-01	Soporte TIC (equipo de cómputo, mesa)	15/ago/2022
DITD-02	Directorio Interno CVTT	15/ago/2022
DITD-03	Videoconferencia	15/ago/2022
DITD-04	Cognos UNAM	15/ago/2022
DITD-05	Gestión de convocatorias CVTT	15/ago/2022
DITD-06	Plataforma de registro de información y notificación de información de la CVTT	15/ago/2022
DITD-07	Gestión de convocatorias Consorcio UNAM TEC	15/ago/2022
DJ-01	Instrumentos consensuales	15/ago/2022
DST-01	Vinculación Interna	15/ago/2022
DST-02	Vinculacion Externa	15/ago/2022
DTT-01	Proceso Transferencia Tecnológica	15/ago/2022

Fecha 15 de Agosto de 2022

ID	Nombre completo del STDP	Actualización
DTT-02	PI	15/ago/2022
DTT-03	Contactos DTT	15/ago/2022
UA-01	Personal de estructura	15/ago/2022
UA-02	Servicios profesionales	15/ago/2022
UA-03	Proveedores	15/ago/2022

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: CCPE-01: Actualización de Directorio UNAM

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, cargo, grado, teléfono de oficina y correo electrónico.

Para que se usan los datos	Para contactarlos ya sea telefónicamente o por correo electrónico.

¿Cómo se obtienen los datos personales?	☐ Físico	
	☒ Digital	Vía correo electrónico.

Temporalidad de obtención	Permanente

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Se recibe vía correo electrónico la información para consultas en general.	• La información se ingresa o actualiza en el Sistema del Directorio UNAM. • La información puede consultarse vía Internet por el público general.	No aplica	No aplica

¿Los datos se transfieren o comparten?	☐ Comparten ☐ Transfieren	☒ No	¿Con quién?	¿Para qué?
	☐ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		No aplica	No aplica

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Nadia Fernanda Salgado Suari
Cargo:	Líder de Proyecto
Funciones:	• Recibir vía correo electrónico la información para consultas en general • La información se ingresa o actualiza en el Sistema del Directorio UNAM. • Comparten, no aplica. • Suprimir los datos del personal que ya no labora en la CVTT.
Obligaciones:	• Confidencialidad: ○ Resguardar las credenciales de acceso al Sistema del Directorio UNAM. • Integridad: ○ Manejar de manera clara y objetiva la información que se requiera para la actualización del Directorio UNAM. • Disponibilidad: ○ Mantener la información del directorio del personal de la CVTT actualizada para cuando sea requerida.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: CCPE–02: Administración de los Sitios Web de la CVTT

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, dirección de correo electrónico, numero telefónico

Para que se usan los datos	En las paginas de la CVTT existen formularios de captura para hacer llegar dudas y solicitudes de servicio de las direcciones de la coordinación.

¿Cómo se obtienen los datos personales?	☐ Físico	n/a
	☒ Digital	Captura desde los sitios web de la CVTT

Temporalidad de obtención	Permanente, se añaden a los directorios de la CCPE.

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Los datos son proporcionados por los usuarios al llenar los formularios.	Se procesan a través de la mesa de ayuda de la CVTT	La información obtenida es canalizada a distintas áreas de la CVTT según sea el caso	No se suprimen, son añadidos a un registro cuando son asignados.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Responsables de cada área dentro de la CVTT	Seguimiento de solicitudes

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Ivan Alexis Ruiz Cardenas
Cargo:	Jefe de departamento

Funciones:	• Recabar las solicitudes que ingresan desde todos los formularios de los sitios web y correo electrónico de la CVTT • Asignar y canalizar las solicitudes a las áreas que sean pertinentes
Obligaciones:	• Confidencialidad, manejar los datos personales con integridad y asignar correctamente las solicitudes a sus áreas correspondientes

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Claudia Lidia Diaz Pérez	*secretaria*	• *Recibir la información y datos de contacto recabados por los formularios de los sitios web de la CVTT* • *Dar seguimiento a las solicitudes asignadas a su cargo*	• *Tratar con integridad y confidencialidad los datos acordes a lo establecido en el aviso de privacidad de la CVTT*
Byron Ballesteros	*asistente*	• *Recibir la información y datos de contacto recabados por los formularios de los sitios web de la CVTT* • *Dar seguimiento a las solicitudes asignadas a su cargo*	• *Tratar con integridad y confidencialidad los datos acordes a lo establecido en el aviso de privacidad de la CVTT*
Angelina Canales	*Líder de proyecto*	• *Recibir la información y datos de contacto recabados por los formularios de los sitios web de la CVTT* • *Dar seguimiento a las solicitudes asignadas a su cargo*	• *Tratar con integridad y confidencialidad los datos acordes a lo establecido en el aviso de privacidad de la CVTT*
Nadia Salgado	*secretaria*	• *Recibir la información y datos de contacto recabados por los formularios de los sitios web de la CVTT* • *Dar seguimiento a las solicitudes asignadas a su cargo*	• *Tratar con integridad y confidencialidad los datos acordes a lo establecido en el aviso de privacidad de la CVTT*

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: CCPE-03: Levantamiento y proceso de multimedia

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, grado y cargos profesionales, correo electrónico, número telefónico o celular, fotografía y video.

Para que se usan los datos	Uso de datos para contacto e intercambio de material multimedia como fotografías, videos y archivos de Word, el tratamiento de datos se apega a los lineamientos expresados en el Aviso de Privacidad de la CVTT.

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	Por medio de correo electrónico o levantamiento de imágenes en campo.

Temporalidad de obtención	Permanente desde el momento en el que se levanta el material.

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Recibir por correo electrónico los datos o material necesario. Levantamiento de imágenes en campo.	Los datos se suman a los directorios y registros para su consulta, en el caso de archivos o multimedia son editados y almacenados según su uso.	Los productos resultantes del uso del material multimedia son usados sin fines de lucro para difusión en medios de comunicación convencionales y redes sociales.	No aplica, los archivos son almacenados para futuro uso y creación de material audiovisual de difusión.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Gaceta UNAM DGCS UNAM UNAM Global TV UNAM RADIO UNAM Áreas internas de la CVTT	Para uso del material audiovisual en campañas de difusión sobre la CVTT, o la actividad académica universitaria.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Ivan Alexis Ruiz Cardenas

Cargo:	Jefe de departamento
Funciones:	• Comunicación con los académicos o personas a las cuales se solicita material audiovisual o datos. • Levantamiento de imágenes en campo. • Encargado de administración y almacenamiento del material obtenido. • Edición y manipulación de material audiovisual. • Distribución de los productos realizados con el material en medios de comunicación, redes sociales y sitios web institucionales.
Obligaciones:	• Compromiso a manejar los datos y material de manera confidencial y sin fines de lucro solo para los fines institucionales de difusión y comunicación para los que son solicitados • Almacenar y poseer disponibilidad del archivo del material y los datos para los fines que convengan a la CVTT y posibles usos a futuro de dicho material

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Daniel Lagos Beltrán	Líder de Proyecto	• Edición y manipulación de material audiovisual • Publicación de los productos en redes sociales	• Compromiso a manejar los datos y material de manera confidencial y sin fines de lucro solo para los fines institucionales de difusión y comunicación para los que son solicitados • Almacenar y poseer disponibilidad del archivo del material y los datos para los fines que convengan a la CVTT y posibles usos a futuro de dicho material
Nadia Fernanda Salgado Suari	Líder de Proyecto	• Uso de información de contacto para integración a directorio y comunicación para intercambio de archivos y material	• Compromiso a manejar los datos y material de manera confidencial y sin fines de lucro solo para los fines institucionales de difusión y comunicación para los que son solicitados • Almacenar y poseer disponibilidad del archivo del material y los datos para los fines que convengan a la CVTT y posibles usos a futuro de dicho material

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-02: Talleres de emprendimiento

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, correo electrónico, universidad de procedencia, escuela o facultad, carrera, último grado de estudios.
Para que se usan los datos	Registro de participantes, envío de información relacionada con el Taller de Emprendimiento y eventos organizados por la Coordinación de Emprendimiento, así como convocatorias y eventos del ecosistema emprendedor
¿Cómo se obtienen los datos personales?	☐ Físico
	☒ Digital — Se recopilan los datos a través de un formulario [redacted]
Temporalidad de obtención	Cada vez que se abre un grupo del Taller de Emprendimiento, Taller de Emprendimiento de ase tecnológica o del Laboratorio de Innovación Social.

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
• Se solicita la información para el registro de los participantes, el conocimiento de sus proyectos y mantener comunicación.	• Se almacenan en una hoja de cálculo generada por el formulario de Google que corresponda en carpeta de Google Drive. • Se utiliza la información de contacto para envío vía correo electrónico de materiales y presentaciones referentes al Taller, para informar sobre temas logísticos relacionados con el taller e invitaciones a conferencias organizadas por al Coordinación de Emprendimiento y convocatorias del ecosistema emprendedor.	• Se envía el nombre y correo electrónico a la Coordinación del Sistema InnovaUNAM para su inclusión en el Boletín.	• No se tienen mecanismos para la destrucción de los datos.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Con la Coordinación del Sistema InnovaUNAM	Para la inclusión en la base de correos a los que les llega el Boletín InnovaUNAM

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Rogerio Julio Canales Pérez
Cargo:	Coordinador de Emprendimiento
Funciones:	• Autorizar la destrucción de la información. • Recaban, se realiza el diseño y construcción de los formularios para la recopilación de información para cada evento. • Procesan: ○ La información se almacena en hojas de cálculo en la cuenta de Drive y se realiza una copia en el Repositorio Institucional de la CVTT para su procesamiento. ○ Se utiliza la información para enviar comunicados sobre logística y operación de los talleres, materiales, invitaciones a otros eventos y actividades. • Comparten, a la Coordinación del Sistema InnovaUNAM para su inclusión en el Boletín InnovaUNAM.
Obligaciones:	• Mantener confidencialidad de datos personales: ○ Definir roles y privilegios para el acceso a los datos. • Garantizar la Integridad de datos personales, ○ Establecer cuáles son los criterios para las validaciones durante la obtención de los datos personales y verificaciones necesarias. • Asegurar disponibilidad: ○ Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU–02: SISTEMA INNOVAUNAM

Datos personales (sensibles o no) contenidos en el sistema:	Nombre del emprendedor, domicilio, perfil del emprendedor, número de cuenta o de trabajador, entidad de procedencia, carrera, teléfono local, teléfono celular, correo electrónico, registro de propiedad intelectual, domicilio fiscal, RFC, imagen en video, firma autógrafa y digital.

Para que se usan los datos	Evaluación y selección de proyectos empresariales que se postulan al Comité InnovaUNAM. Formalizar los convenios de incubación de empresas. Elaboración de estadísticas e informes Seguimiento del proceso de incubación. Capacitación y Comunicación. Documentos de soporte: **Convocatoria para presentar proyectos al Comité de selección y evaluación para ingreso al proceso de incubación en el Sistema de Incubadoras de Empresas InnovaUNAM.** **Políticas de operación del Sistema de Incubadoras de Empresas InnovaUNAM.**

¿Cómo se obtienen los datos personales?	☒ Físico	Impresión de solicitud para ingresar al Sistema de Incubadoras de Empresas InnovaUNAM
	☒ Digital	Se recopilan los datos a través de la *Plataforma de Registro para la incubación en el Sistema InnovaUNAM en el sitio* [redacted] Y a través de correo electrónico en las cuentas institucionales: [redacted]

Temporalidad de obtención	Bajo demanda. Dependiendo de las fechas establecidas en la convocatoria para realizar los comités de selección.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Se recibe información a través de la *Plataforma de Registro para la incubación en el Sistema InnovaUNAM* Y a través de correo electrónico en las cuentas institucionales	Se cargan las solicitudes y se da acceso a evaluadores mediante plataforma de evaluación, proporcionada por la DIDT, CVTT. Se cargan las Actas de los Comités en el Sistema de Firmas Electrónicas para firma de los evaluadores de la UNAM. Se cargan los expedientes y se da acceso a los	Se comparten las solicitudes con los líderes de proyecto y servidores sociales de las Incubadoras del Sistema InnovaUNAM para el seguimiento de los proyectos. Con los integrantes del comité de evaluación.	Lo expedientes y registros pueden destruirse una vez que pasaron 5 años del término del proceso de incubación. En el caso de los expedientes digitales, se borran los registros, en el caso de los documentos, se trituran según corresponda.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
	emprendedores y equipos de las incubadoras de empresas del Sistema InnovaUNAM al repositorio institucional de la CVTT y/o nube CVTT, proporcionados por la DIDT, CVTT. Se comparte la información de los expedientes con las áreas jurídicas y administrativas de la CVTT para la formalización y gestión de los procesos de incubación de empresas. Se comparte acceso a las videoconferencias de capacitación y seguimiento de los emprendedores que se realizan [redacted] con la jefa de gestión administrativa de la DEU para la difusión de los eventos en la página de InnovaUNAM: [redacted] así como el respaldo de los equipos de cómputo de la Coordinación del Sistema InnovaUNAM para que realice el respaldo [redacted] Se archiva la documentación en los expedientes correspondientes.	Con la Jefa de Área de Gestión Administrativa, para la comunicación y difusión de los eventos, así como el respaldo de la información del Sistema. Parte de la información también se comparte con el personal de las áreas jurídica y administrativa de la CVTT para la formalización y gestión de los proyectos en incubación. Con los Aliados estratégicos del sector público y privado que proporcionan recursos para los procesos de incubación se comparte la información de acuerdo con la convocatoria, reglas de operación o condiciones en que otorgan los apoyos.	

	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?

¿Los datos se transfieren o comparten?	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro	Evaluadores externos Responsables, Líderes de Proyecto y servidores sociales de las Incubadoras del Sistema InnovaUNAM Delegación Jurídica, CVTT Área Administrativa, CVTT Aliados estratégicos del sector público y privado que proporcionan recursos para la incubación.	Evaluar los proyectos. Seguimiento al proceso de incubación. Formalizar los convenios de incubación. Ejercicio de recursos para los procesos de incubación. Obtención de recursos para los procesos de incubación.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Mtro. Eduardo Urzúa Fernández
Cargo:	Director de Emprendimiento Universitario
Funciones:	Acceso a información para evaluación, selección y seguimiento de los proyectos empresariales del Sistema InnovaUNAM.
Obligaciones:	• Mantener confidencialidad de datos personales ○ Definir roles y privilegios en las plataformas de registro y selección de proyectos. ○ Tanto la Delegación Jurídica de la CVTT como las Unidades de Incubación definen los procedimientos para el tratamiento y protección de la información que les compartimos. • Garantizar la Integridad de datos personales, ○ Establecer los criterios para la validación durante la obtención de datos y verificaciones necesarias. • Asegurar disponibilidad ○ Información con acceso disponible para cuando se requiera consultar.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Mtra. Yessica González Ceja	Coordinadora del Sistema InnovaUNAM	• Recaban, ○ Recibe postulaciones para el proceso de selección de proyectos empresariales para iniciar un proceso de incubación en el Sistema InnovaUNAM mediante plataforma de registro proporcionada por la DIDT, CVTT.	• Mantener confidencialidad de datos personales ○ Autorizar nuevos usuarios a Plataforma de registro, Selección de proyectos, en el repositorio institucional de la CVTT y nube CVTT, proporcionados por la DIDT, CVTT.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		• Procesan y comparten, ○ Cargan información de las solicitudes y proporcionan acceso a evaluadores mediante plataforma de evaluación, selección y de proyectos proporcionada por la DIDT, CVTT. ○ Cargan y proporcionan acceso a los emprendedores y equipos de las incubadoras de empresas del Sistema InnovaUNAM a los expedientes de emprendedores en el repositorio institucional de la CVTT y nube CVTT, proporcionados por la DIDT, CVTT. ○ Comparten información de los expedientes con las áreas jurídicas y administrativas de la CVTT para la formalización y gestión de los procesos de incubación de empresas. ○ Archivar documentación en expedientes correspondientes. • Suprimen, ○ Los expedientes y registros pueden suprimirse cinco años después de concluido el proceso de incubación.	○ Resguarda accesos a los Sistemas, plataformas y herramientas que se utilizan en la Coordinación del Sistema InnovaUNAM. ○ Resguardar cartas de confidencialidad en los casos que se requiera. • Garantizar la Integridad de datos personales, ○ Diseñar e implementar mecanismos de seguridad técnica en el ámbito de su competencia. • Asegurar disponibilidad ○ Diseñar e implementar esquemas para mantener disponible la información cuando se requiera.
Lic. Angelina Alejandra Canales López de Nava	Jefa de Área de Gestión Administrativa de la DEU	• Recaban, ○ Solicita respaldo de los archivos alojados en los equipos de cómputo de la Coordinación del Sistema InnovaUNAM y los resguarda en un Disco Externo bajo su responsabilidad. • Procesan y comparten, ○ Descarga videos de las actividades del Sistema de la plataforma zoom, los edita y los carga a la página del Sistema InnovaUNAM: innova.unam.mx	• Mantener confidencialidad de datos personales ○ Diseñar e implementar mecanismos de seguridad técnica en el ámbito de su competencia. • Garantizar la Integridad de datos personales, ○ Diseñar e implementar mecanismos de seguridad técnica en el ámbito de su competencia. • Asegurar disponibilidad ○ Diseñar e implementar esquemas para mantener disponible la información cuando se requiera.
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Respaldos periódicos de la información almacenada en la base de datos.	• Confidencialidad: ○ Administrar privilegios de acceso. • Integridad: ○ Mantenimiento al servidor de base de datos.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		• Comparten: No aplica • Suprimen: No aplica	• Disponibilidad: ○ Asegurar el acceso a las plataformas y servicios TIC.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-03: Incubación de base tecnológica

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, imagen de credencial de alumno o trabajador e identificación oficial y firma autógrafa; así como grabaciones de videoconferencias.

Para que se usan los datos	Para registrar solicitudes de postulación al Sistema de Incubación de Empresas InnovaUNAM, para la suscripción del convenio de incubación y para fines de capacitación o seguimiento de programas de la Incubadora.

¿Cómo se obtienen los datos personales?	☒ Físico	Se almacena una copia física de los datos personales recabados digitalmente para los expedientes de ingreso al Sistema de Incubación de Empresas InnovaUNAM.
	☒ Digital	Para los expedientes de ingreso al Sistema de Incubación de Empresas InnovaUNAM, se recopilan los datos a través de la *Plataforma de Registro para la incubación en el Sistema InnovaUNAM en el sitio* [redacted] Y se reciben a través de correo electrónico en las cuentas institucionales: [redacted] Las grabaciones de videoconferencias se descargan y almacenan en las carpetas de la Incubadora de Empresas de Base Tecnológica alojadas en el Repositorio Institucional de la CVTT.

Temporalidad de obtención	Conforme lo especificado en la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Se recibe la información vía correo electrónico para el registro de los postulantes a la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM y para la integración del convenio de incubación.	Se consulta la información para seleccionar los proyectos que ingresan a incubación conforme a las Políticas Institucionales y para la integración del convenio de incubación. El almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT.	Se envían los datos de los postulantes a la Coordinación del Sistema InnovaUNAM para su inscripción en el Sistema de Incubadoras de Empresas InnovaUNAM.	La información no se suprime, se conserva en archivo permanente.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
	Los datos personales en formato físico se resguardan en [redacted]		

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Coordinación del Sistema InnovaUNAM	Inscripción en el Sistema de Incubadoras de Empresas InnovaUNAM.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Mtro. Eduardo Urzúa Fernández
Cargo:	Director de Emprendimiento Universitario
Funciones:	Supervisa la inscripción de los postulantes al Sistema de Incubadoras de Empresas InnovaUNAM, así como la suscripción del convenio de incubación.
Obligaciones:	• Mantener confidencialidad de datos personales: ○ Definir roles y privilegios para la *Plataforma de Registro para la incubación en el Sistema InnovaUNAM* • Garantizar la Integridad de datos personales: ○ Establecer cuáles son los criterios para las validaciones durante la obtención de los datos personales y verificaciones necesarias. • Asegurar disponibilidad: ○ Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Alba Inés Sánchez Vázquez	Coordinadora de la Incubadora de Empresas de Base Tecnológica InnovaUNAM Central	• Recaban. ○ Recibir la información vía correo electrónico para el registro de los postulantes a la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM y para la integración del convenio de incubación. • Procesan. ○ Consulta la información para seleccionar los proyectos que ingresan a incubación conforme a la Políticas Institucionales y para la integración del convenio de incubación. ○ Asegura el almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT. Los datos personales en formato físico se resguardan en [redacted] • Comparten. ○ Envían los datos de los postulantes a la Coordinación del Sistema InnovaUNAM para su inscripción en el Sistema de Incubadoras de Empresas InnovaUNAM. • Suprimen. ○ La información no se suprime, se conserva en archivo permanente.	• Mantener la confidencialidad de datos personales: ○ Asegurarse que todas las personas con acceso a los datos personales firmen cartas de confidencialidad correspondientes. ○ Resguardar los accesos a los expedientes físicos y digitales.
Diana Nadxelii Casas Gutiérrez	Líder de Proyecto de la Incubadora de Empresas de Base Tecnológica InnovaUNAM Central	• Recaban. ○ No aplica • Procesan. ○ Mantener el almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT. Los datos personales en formato físico se resguardan [redacted]	• Mantener la confidencialidad de datos personales: ○ Resguardar los accesos a los expedientes físicos y digitales.

[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		[redacted] • Comparten. ○ No aplica • Suprimen. ○ No aplica	
Angelina Alejandra Canales López de Nava	Jefa de Área de Gestión Administrativa	• Recaban. ○ No aplica • Procesan. ○ Mantener el almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT. • Comparten. ○ No aplica • Suprimen. ○ No aplica	• Mantener la confidencialidad de datos personales: ○ Resguardar los accesos a los expedientes digitales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-04: Incubación de empresas sociales

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, firma autógrafa, fotografía en credencial de alumno o trabajador e identificación oficial, video.

Para que se usan los datos	Para registrar solicitudes de postulación al Sistema de Incubación de Empresas InnovaUNAM y para la suscripción del convenio de incubación. Aplican la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM, así como las Políticas institucionales para proyectos empresariales en incubación dentro del sistema de incubadoras de empresas InnovaUNAM

¿Cómo se obtienen los datos personales?	☒ Físico	No se recaban en formato físico, pero se almacena una copia física de los datos personales recabados digitalmente.
	☒ Digital	Se recopilan los datos a través de la *Plataforma de Registro para la incubación en el Sistema InnovaUNAM en el sitio* [redacted] Y a través de correo electrónico en las cuentas institucionales: [redacted] Las grabaciones de videoconferencias se descargan y almacenan en el repositorio institucional de la CVTT de la Incubadora de Empresas Sociales.

Temporalidad de obtención	Conforme lo especificado en la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Se recibe la información para el registro de los postulantes a la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM y para la integración del convenio de incubación.	Se consulta la información para seleccionar los proyectos que ingresan a incubación conforme a las Políticas Institucionales y para la integración del convenio de incubación. El almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional	Se envían los datos de los postulantes a la Coordinación del Sistema InnovaUNAM para su inscripción en el Sistema de Incubadoras de Empresas InnovaUNAM.	La información no se suprime se conserva en archivo permanente.

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
	de la CVTT. Los datos personales en formato físico se resguardan en [redacted]		

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Coordinación del Sistema InnovaUNAM	Inscripción en el Sistema de Incubadoras de Empresas InnovaUNAM.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Mtro. Eduardo Urzúa Fernández
Cargo:	Director de Emprendimiento Universitario
Funciones:	Supervisa la inscripción de los postulantes al Sistema de Incubadoras de Empresas InnovaUNAM, así como la suscripción del convenio de incubación.
Obligaciones:	• Mantener confidencialidad de datos personales: ○ Definir roles y privilegios para la *Plataforma de Registro para la incubación en el Sistema InnovaUNAM* • Garantizar la Integridad de datos personales: ○ Establecer cuáles son los criterios para las validaciones durante la obtención de los datos personales y verificaciones necesarias. • Asegurar disponibilidad: ○ Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Claudia Leticia Palancares Torres	Coordinadora de la Incubadora de Empresas Sociales InnovaUNAM Social	• Recaban ○ Recibir la información para el registro de los postulantes a la Convocatoria del Sistema de Incubadoras de Empresas InnovaUNAM y para la integración del convenio de incubación. • Procesan ○ Consulta la información para seleccionar los proyectos que ingresan a incubación conforme a la Políticas Institucionales y para la integración del convenio de incubación. ○ Asegura el almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT. Los datos personales en formato físico se resguardan en [redacted] • Comparten ○ Envían los datos de los postulantes a la Coordinación del Sistema InnovaUNAM para su inscripción en el Sistema de Incubadoras de Empresas InnovaUNAM. • Suprimen ○ La información no se suprime se conserva en archivo permanente.	• Mantener la confidencialidad de datos personales: ○ Asegurarse que todas las personas con acceso a los datos personales firmen cartas de confidencialidad correspondientes. ○ Resguardar los accesos a los expedientes físicos y digitales.
Edgar Ángeles Ramírez	Líder de Proyecto de la Incubadora de Empresas Sociales InnovaUNAM Social	• Recaban ○ No aplica • Procesan ○ Mantener el almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT. Los datos personales en formato físico se resguardan en	• Mantener la confidencialidad de datos personales: ○ Resguardar los accesos a los expedientes físicos y digitales.

[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		[redacted] • Comparten ○ No aplica • Suprimen ○ No aplica	
Angelina Alejandra Canales López de Nava	Jefa de Área de Gestión Administrativa	• Recaban ○ No aplica • Procesan ○ Mantener el almacenamiento de los datos personales en formato digital se realiza en el repositorio institucional de la CVTT. • Comparten ○ No aplica • Suprimen ○ No aplica	• Mantener la confidencialidad de datos personales: ○ Resguardar los accesos a los expedientes digitales.
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban ○ No aplica • Procesan ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten ○ No aplica • Suprimen ○ No aplica	• Confidencialidad: ○ Administrar privilegios de acceso. • Integridad: ○ Mantenimiento al servidor de base de datos. • Disponibilidad: ○ Asegurar el acceso a las plataformas y servicios TIC.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU–05: GUÍAS PARA EL EMPRENDIMIENTO PROFESIONAL

Datos personales (sensibles o no) contenidos en el sistema:	Nombre, Apellidos, correo electrónico, ciudad, país, edad, nivel educativo, área de conocimiento, progreso del curso.

Para que se usan los datos	• Seguimiento del progreso del curso. • Emitir constancia de término sin validez oficial. • Generar estadísticas de cuántos usuarios han tenido las guías de negocio.

¿Cómo se obtienen los datos personales?	☐ Físico	
	☒ Digital	Se recopilan los datos a través de la *plataforma de las Guías para el emprendimiento profesional*

Temporalidad de obtención	Conforme van llegando nuevos usuarios incrementa el número.

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Los usuarios se autoregistran en la plataforma.	La plataforma registra el progreso de cada participante conforme su avance. Al concretar las guías y bajo solicitud del participante la plataforma emite constancias. Periodicamente se descarga la información registrada en una hoja de cálculo para obtener conteo de los usuarios y generar indicadores.	No se comparten.	No se suprimen.

¿Los datos se transfieren o comparten?	☐ Comparte ☐ Transfiere	☐ No	¿Con quién?	¿Para qué?
	☐ CVTT ☐ Áreas Universitarias		No aplica	No aplica
	☐ Gobierno federal ☐ Gobierno local			

	☐ Personas físicas ☐ Personas morales ☐ Otro		

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Nombre:	Abigail López Alvarez
Cargo:	Líder de Proyecto de la Incubadora de Empresas de Base Tecnológica
Funciones:	• Ingresos de proyectos de incubación • Seguimiento de proceso de incubación • Asesorías y consultorías • Gestión de pago a consultores • Informes de indicadores de la incubadora
Obligaciones:	• Mantener confidencialidad de datos personales: ○ Firmar carta de confidencialidad dado que se tienen datos de los emprendedores

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento[2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica ○ Suprimen: No aplica	• Confidencialidad: ○ Administrar privilegios de acceso. • Integridad: ○ Mantenimiento al servidor de base de datos. • Disponibilidad: ○ Asegurar el acceso a las plataformas y servicios TIC.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-06: Emprende con Santander X y la UNAM

Datos personales (sensibles o no) contenidos en el sistema:	Plataforma de Emprende con Santander X y la UNAM: Correo electrónico, nombre, apellidos, ciudad, país. Mesa de ayuda: Nombre, correo electrónico

Para que se usan los datos	• Identificar al usuario dentro de la plataforma • Dar seguimiento del progreso del usuario. • Generar estadísticas de cuántos usuarios han terminado los cursos asignados. • Seguimiento de incidentes relacionados con el uso de la plataforma.

¿Cómo se obtienen los datos personales?	☐ Físico	
	☒ Digital	Se recopilan los datos a través de la *plataforma de Emprende con Santander X y la UNAM*: [redacted] Se recopilan los datos a través de la *mesa de ayuda:* [redacted]

Temporalidad de obtención	Conforme van llegando nuevos usuarios incrementa el número.

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Los participantes se auto registran en la plataforma.	La plataforma registra el progreso de cada participante conforme su avance.	La información a compartir incluye usuarios inscritos, sus avances, diagnósticos de conocimientos y encuestas de satisfacción en los cursos en la plataforma	No se suprimen

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☐ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☒ Personas morales ☐ Otro		BANCO SANTANDER (MÉXICO) SOCIEDAD ANÓNIMA, INSTITUCIÓN DE BANCA MÚLTIPLE, GRUPO FINANCIERO SANTANDER MÉXICO	Para permitir avanzar en etapas y/o formar parte de alguno de los diferentes programas de becas que ofrece la división de "SANTANDER UNIVERSIDADES"

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**

Responsable de seguridad de datos personales:	L.I Alma Rosa García Martínez
Cargo:	Directora de Información y Transformación Digital
Funciones:	• Recaban: ○ Diseño de formulario para el registro de participantes • Procesan ○ Se consultan los datos registrados en la plataforma para apoyos técnicos o consultas de estadísticas. • Comparten ○ Se da acceso al enlace de Santander para realizar consulta de los datos en la plataforma. • Suprimen ○ Sí es el caso se elimina el registro por medio de la plataforma.
Obligaciones:	• Confidencialidad: ○ Autorizar accesos, definir roles y privilegios para el uso de la plataforma. • Integridad: ○ Definir las reglas para validación de la información • Disponibilidad: ○ Establecer los periodos en los que debe estar disponible la información

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Ariadna Hernández Zamora	Gerente Plan de Apoyo a la Educación Superior Santander Universidades	• Recaban, no aplica • Procesan, ○ Recibir los registros de los usuarios de la plataforma para verificar que se encuentren en algunos de los programas apoyados por Santander. ○ Conocer el nivel de avance y/o conclusión de los inscritos. • Comparten, no aplica • Suprimen, no aplica	• Confidencialidad: ○ No compartir información con personal no autorizado para las funciones correspondientes • Integridad, no aplica • Disponibilidad, no aplica

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan:	• Confidencialidad: Administrando los privilegios de acceso. • Integridad: Mantenimiento al servidor de base de datos.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

		○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica • Suprimen: No aplica	• Disponibilidad: Asegurar el acceso a la plataforma y la mesa de ayuda desde internet.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-01: Soporte TIC

Datos personales (sensibles o no) contenidos en el sistema:	Personal perteneciente a la CVTT: Nombre, Primer apellido, Segundo apellido, Correo electrónico.

Para que se usan los datos	Los datos recabados se utilizan para llevar a cabo el inventario del equipo de computo que le es asignado o desasignado a cada persona que presta sus servicios en la Coordinación, así como dar seguimiento de tickets generados a través de la mesa de Ayuda [redacted]

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	• Hoja de cálculo: [redacted] • Plataforma de Gestión de servicios [redacted]

Temporalidad de obtención	Por evento

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Se solicita al jefe de personal los datos de los empleados y personal externo activo que preste sus servicios en la CVTT.	Registro en la hoja de cálculo con los datos asociados a los equipos de cómputo. Registro en la plataforma con los datos asociados a los equipos de cómputo.	No aplica	En caso de que el personal interno o externo deje de prestar sus servicios en la CVTT.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☒ No	¿Con quién?	¿Para qué?
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		No aplica	No aplica

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	L.I. Alma Rosa García Martínez
Cargo:	Directora de Información y Transformación Digital

Funciones:	• Recaban: No aplica • Procesan: No aplica • Comparten: No aplica • Suprimen: Evaluar y autorizar la eliminación de los datos
Obligaciones:	• Confidencialidad: Definir roles y privilegios para el uso de los datos. • Integridad: Definir las reglas para validación de la información. • Disponibilidad: Establecer los periodos en los que debe estar disponible la información.

Encargados			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Ricardo Albarrán Romero	Jefe del Departamento de Soporte Técnico	• Recaban ○ Se solicita al jefe de personal los datos de los empleados y personal externo activo que preste sus servicios en la CVTT. • Procesan ○ Registro en la hoja de cálculo con los datos asociados a los equipos de cómputo. • Procesan ○ Registro en la plataforma GLPI con los datos asociados a los equipos de cómputo. • Comparten ○ No aplica • Suprimen ○ En caso de que el personal interno o externo deje de prestar sus servicios en la CVTT.	• Confidencialidad ○ No aplica • Integridad ○ Únicamente se ingresa información previamente verificada. • Disponibilidad ○ No aplica
Laura Lechuga Rodríguez	Servicio profesional de la DITD	• Recaban ○ No aplica • Procesan ○ Registro en la plataforma [redacted] con los datos asociados a los equipos de cómputo. • Comparten ○ No aplica • Suprimen ○ No aplica	• Confidencialidad ○ No aplica • Integridad ○ Únicamente se ingresa información previamente verificada. • Disponibilidad No aplica
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban ○ No aplica • Procesan ○ Registro en la plataforma [redacted] con los datos asociados a los equipos de cómputo. ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten ○ No aplica	• Confidencialidad: ○ Administrar privilegios de acceso. • Integridad: ○ Mantenimiento al servidor de base de datos. • Disponibilidad ○ Asegurar el acceso a las plataformas y servicios TIC.

		• Suprimen ○ No aplica	

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-02: DIRECTORIO INTERNO CVTT

Datos de Identificación	• Comunidad Universitaria: Nombre, teléfono celular. • Externos: Nombre, correo electrónico, teléfono celular.
Datos Laborales	• Comunidad Universitaria: Puesto, correo electrónico institucional, teléfono institucional. • Externos: No aplica

Para que se usan los datos	Los datos que se recaban se utilizan con fines informativos dentro de la Coordinación de Vinculación de Transferencia Tecnológica.

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	• Hoja de cálculo: [redacted]

Temporalidad de obtención	• Por evento

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
Al ingreso de trabajadores o de personal externo que preste sus servicios en las áreas de la Coordinación se les solicita dicha información para ser integrada al Directorio.	• El jefe de personal avisa del ingreso del trabajador o personal externo. • Se solicitan los datos para ser agregarlos a la hoja de cálculo.	Se comparten con las asistentes administrativas de cada una de las áreas de la Coordinación para su difusión.	No aplica

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		• Coordinación de Vinculación y Transferencia Tecnológica • Dirección de Transferencia de Tecnología • Coordinación de Propiedad Intelectual • Dirección de Servicios Tecnológicos	El objetivo es que el personal de la Coordinación de Vinculación y Transferencia Tecnológica este informado sobre los datos de contacto de las personas que prestan sus servicios en cualquier área.

		• Dirección de Incubadoras y Parques Tecnológicos • Coordinación de Proyectos Especiales • Delegación Jurídica • Unidad Administrativa • Delegación Administrativa	

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	L.I Alma Rosa García Martínez
Cargo:	Directora de Proyectos Especiales
Funciones:	• Recaban: No aplica • Procesan: No aplica • Comparten: No aplica • Suprimen: Evaluar y autorizar la eliminación de los datos
Obligaciones:	• Confidencialidad: Definir roles y privilegios para el uso de los datos. • Integridad: Definir las reglas para validación de la información. • Disponibilidad: Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica	No aplica	• Recaban: No aplica • Procesan: No aplica • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: No aplica • Integridad: No aplica • Disponibilidad: No aplica

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Laura Nayeli Lechuga Rodríguez	Servicios Profesionales	• Recaban: Se contacta al personal o persona externa de recién ingreso y se le solicitan los datos en mención. • Procesan: Se agregan o modifican los datos en la hoja de cálculo. • Comparten: Se comparten con las asistentes administrativas de cada una de las áreas de la Coordinación. • Suprimen: No aplica	• Confidencialidad: No aplica. • Integridad: Únicamente se ingresa información previamente verificada. • Disponibilidad: No aplica

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-03: VIDEOCONFERENCIA

Datos de Identificación:	• Comunidad Universitaria: Nombre, correo electrónico. • Externo: Nombre, correo electrónico. NOTA: Cabe aclarar que por cada evento se podrá solicitar datos adicionales según se requiera.
Datos Laborales	• Comunidad Universitaria: Correo electrónico institucional. • Externo: No aplica NOTA: Cabe aclarar que por cada evento se podrá solicitar datos adicionales según se requiera.

Para que se usan los datos	Para administración de los invitados a las videoconferencias.

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	• Sitio web de la plataforma de videoconferencia

Temporalidad de obtención	• Por evento

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
La comunidad universitaria o personal externo mediante el llenado de un formulario en la página Web de Appointlet. Durante la sesión Zoom almacena la los datos del usuario, así como lo proyectado en sus cámaras Web.	La página Web de [redacted] almacena los datos en sus sistemas. En [redacted], los datos sirven para realizar reportes. En [redacted] los videos se procesan para su descarga.	Se comparte el listado de asistentes.	No aplica

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Con el responsable del evento solicitado.	Control de asistentes.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	L.I. Alma Rosa García Martínez
Cargo:	Directora de Proyectos Especiales
Funciones:	• Recaban: No aplica • Procesan: No aplica • Comparten: No aplica • Suprimen: Evaluar y autorizar la eliminación de los datos
Obligaciones:	• Confidencialidad: Definir roles y privilegios para el uso del sistema. • Integridad: Definir las reglas para validación de la información. • Disponibilidad: Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Ing. Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: Se realizaron consultas para llevar el control de los asistentes. • Comparten: Se comparte el listado de asistentes al responsable del evento. • Suprimen: No aplica	• Confidencialidad: Únicamente el encargado tiene acceso. • Integridad: No aplica. • Disponibilidad: No aplica.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica	No aplica	No aplica	No aplica

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-04: COGNOS UNAM 2.0

Datos de Identificación	• Comunidad Universitaria: Nombre, teléfono particular, correo electrónico, RFC, CURP, fecha de nacimiento, nacionalidad, fotografía. • Externos: Nombre, correo electrónico, RFC, CURP, fecha de nacimiento.
Datos Laborales	• Comunidad Universitaria: Puesto, correo electrónico institucional, teléfono institucional, número de empleado. • Externos: Puesto.

Para que se usan los datos	Los datos que se recaban se utilizan con fines informativos, así como para la administración de usuarios del sistema.

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	• Sitio web: [redacted]

Temporalidad de obtención	• Permanente

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
La comunidad universitaria o personal externo mediante el llenado de un formulario solicita el acceso al sistema.	• Llega la solicitud al correo del administrador. • Validan la información. • Crea la cuenta del usuario.	No aplica	No aplica

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☒ No	¿Con quién?	¿Para qué?
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		No aplica	No aplica

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**

Responsable de seguridad de datos personales:	L.I Alma Rosa García Martínez
Cargo:	Directora de Proyectos Especiales
Funciones:	• Recaban: No aplica • Procesan: No aplica • Comparten: No aplica • Suprimen: Evaluar y autorizar la eliminación de los datos
Obligaciones:	• Confidencialidad: Definir roles y privilegios para el uso del sistema. • Integridad: Definir las reglas para validación de la información. • Disponibilidad: Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Ing. María Yolanda Nigó González	Servicios Profesionales	• Recaban: No aplica • Procesan: Cambio de datos personales por datos de prueba en ambientes de pruebas y desarrollo. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: Aseguramiento de datos personales para no ser usados en ambientes de pruebas y desarrollo. • Integridad: No aplica • Disponibilidad: No aplica
Laura Nayeli Lechuga Rodríguez	Servicios Profesionales	• Recaban: Se obtiene los datos de identificación y laborales de los nuevos titulares asignados. • Procesan: Se ingresan y modifican los datos al sistema mediante el llenado del formulario (provee). • Comparten: No aplica • Suprimen: Se eliminan los registros en caso de ser necesario a través del sistema.	• Confidencialidad: No aplica. • Integridad: Se ingresa información al sistema previamente validada. • Disponibilidad: No aplica

Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica
		• Procesan:
		  ○ Respaldos periódicos de la información almacenada en la base de datos.
		• Comparten: No aplica
		• Suprimen: No aplica
			• Confidencialidad:
			  ○ Administrar privilegios de acceso.
			• Integridad:
			  ○ Mantenimiento al servidor de base de datos.
			• Disponibilidad:
			  ○ Asegurar el acceso a las plataformas y servicios TIC.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD–05: GESTIÓN DE CONVOCATORIAS CVTT

Datos personales (sensibles o no) contenidos en el sistema:	La gestión de convocatorias contiene datos personales no sensibles los cuales y pertenecen a miembros de la comunidad universitaria y personas externas. El sistema puede contener los siguientes datos: • Correo electrónico, Nombres, Apellidos, Tratamiento, Teléfono fijo, Teléfono celular En caso de que pertenezca a la comunidad el sistema además puede contiene los siguientes datos dependiendo de la convocatoria: • Tipo de áreas de conocimiento, Tipo de entidad o dependencia. En caso de que sean integrantes de equipos que postulan propuestas el sistema además puede contiene los siguientes datos dependiendo de la convocatoria: • Género, Relación actual del responsable con la UNAM, Escuela, facultad o entidad universitaria de procedencia, Área de formación, Identificación oficial, Último grado de estudios. En caso de que sean evaluadores el sistema contiene los siguientes datos dependiendo de la convocatoria: • Evaluaciones de proyectos.

Para que se usan los datos	• Enviar invitaciones para confirmación o notificación de las convocatorias. • Registrar propuestas de las convocatorias • Evaluar las propuestas de las convocatorias • Seguimiento de avances de los proyectos

¿Cómo se obtienen los datos personales?	☐ Físico	
	☒ Digital	Plataforma para postulación de proyectos: [redacted] Plataforma de evaluación de proyectos: [redacted] Nube de la CVTT: [redacted] Plataforma de la mesa de ayuda: [redacted] Plataforma de sello digital universitario: [redacted]

Temporalidad de obtención	Conforme lo indicado en cada convocatoria

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
• Recepción de propuestas que se postulan a Convocatorias. • Grabaciones de webinar sobre convocatorias. • Recepción de solicitudes de información. • Registro de calificaciones de rúbrica por los evaluadores.	• Publicación en [redacted] de webinars sobre convocatorias. • Atención de solicitudes de información. • Extracción de la Plataforma para postulación de Proyecto. • Transformación de datos y carga a Plataforma de evaluación de proyectos. Generar resultados de evaluación de propuestas. • Notificar vía correo electrónico sobre eventos, reuniones y nuevas convocatorias. • Respaldar información.	• Evaluadores para registrar calificaciones de la rúbrica correspondiente. • Responsable de cada convocatoria.	La información no se suprime, se conserva en archivo permanente.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ Interior CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		• Con los evaluadores asignados a cada convocatoria. • Con el responsable de cada convocatoria.	• Para registrar calificaciones de la rúbrica. • Para consulta de resultados.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	L.I Alma Rosa García Martínez
Cargo:	Directora de Información y Transformación Digital
Funciones:	• Recabar: ○ Diseño de instrumentos para el registro de propuestas. ○ Seguimiento a registro de propuestas postuladas. • Procesan: ○ Extracción, transformación y carga de propuestas postuladas al sistema de evaluación. • Comparten: ○ Generación de enlaces para compartir información en nube de la CVTT. • Suprimen: No aplica
Obligaciones:	• Confidencialidad: ○ Autorización de accesos, definir roles y privilegios para el uso del sistema a plataformas para postulación de Proyecto, evaluación de proyectos, nube de la CVTT y mesa de ayuda.

	○ Solicitud de accesos a plataforma de Sello Digital Universitario. ○ Resguardar credenciales de acceso a plataformas. • Integridad: ○ Definir las reglas para validación de la información. • Disponibilidad: Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Alba Inés Sánchez Vázquez Diana Nadxelii Casas Gutiérrez María Isabel Mascorro Velarde Claudia Lidia Díaz Pérez Yessica E. González Ceja	Coordinadora de la Incubadora de Empresas de Base Tecnológica InnovaUNAM Líder de Proyecto Incubación Directora de Transferencia de Tecnología Servicio Profesional de la DTT Coordinadora del Sistema de Incubadoras de Empresas InnovaUNAM	• Recaban: No aplica • Procesan: ○ Alta de evaluadores ○ Asignar propuestas por evaluar a cada Evaluador ○ Enviar notificación y recordatorios de propuestas por evaluar. ○ Seguimiento de avance de evaluaciones. ○ Diseñar estrategias y toma de decisiones de la convocatoria. ○ Generar documentos relacionados con la convocatoria • Comparten: ○ Con áreas internas de la CVTT. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. • No compartir información con personal no autorizado para las funciones correspondientes.
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Carga de documentos de propuestas postuladas al sistema de evaluación. ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: Administrando los privilegios de acceso. • Integridad: Mantenimiento al servidor de base de datos. • Disponibilidad: Asegurar que el sistema siempre este en línea.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Ricardo Albarrán Romero Laura Lechuga Rodríguez	Jefe del Departamento de Soporte Técnico Servicio profesional de la DITD	• Recaban: ○ Seguimiento a registro de propuestas postuladas. ○ Diseño de instrumentos para el registro de propuestas y a eventos. ○ Seguimiento a registro eventos (webinars y sesiones informativas) ○ Grabación de eventos. • Procesan: ○ Generación de reportes sobre asistencia a eventos.	• Confidencialidad: ○ Resguardar los accesos a las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD–06: PLATAFORMA DE REGISTRO DE INFORMACIÓN Y NOTIFICACIÓN DE INFORMACIÓN DE LA CVTT

Datos personales (sensibles o no) contenidos en el sistema:	La plataforma de registro de información y notificación de información de la CVTT contiene datos personales no sensibles los cuales y pertenecen a miembros de la comunidad universitaria y personas externas. El sistema puede contener los siguientes datos: • Correo electrónico, Nombres, Apellidos, Tratamiento, Teléfono fijo, Teléfono celular En caso de que pertenezca a la comunidad el sistema además puede contiene los siguientes datos dependiendo de la convocatoria: • Tipo de áreas de conocimiento, Tipo de entidad o dependencia. En caso de que sean integrantes de equipos que postulan propuestas el sistema además puede contiene los siguientes datos dependiendo de la convocatoria: • Género, Relación actual del responsable con la UNAM, Escuela, facultad o entidad universitaria de procedencia, Área de formación, Identificación oficial, Último grado de estudios. En caso de que sean evaluadores el sistema contiene los siguientes datos dependiendo de la convocatoria: • Evaluaciones de proyectos.

Para que se usan los datos	• Enviar invitaciones para confirmación o notificación de registros e información de la CVTT • Recabar información de los registros de la CVTT • Evaluar las propuestas de los registros de proyectos • Seguimiento de avances de los proyectos

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	Plataforma de registro y notificación de información de la CVTT: [redacted]

Temporalidad de obtención	Conforme lo indicado en cada convocatoria

¿Cuál es el tratamiento de los datos?			
Recaban	Procesan	Comparten	Suprimen
• Recepción de información de los registros.	• Publicación en [redacted] de webinars sobre eventos. • Atención de solicitudes de información.	• Responsable de cada registro.	La información no se suprime, se conserva en archivo permanente.

	• Extracción de información de los registros. • Notificar vía correo electrónico sobre eventos y reuniones. • Respaldar información.		

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ Interior CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		DEU de la CVTT DTT de la CVTT CCPE de la CVTT DST de la CVTT	Para que el responsable de cada registro pueda obtener información.

Responsable STDP:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	L.I Alma Rosa García Martínez
Cargo:	Directora de Información y Transformación Digital
Funciones:	• Recabar: ○ Diseño de instrumentos para el registro de propuestas. ○ Seguimiento a registro de propuestas postuladas. • Procesan: ○ Extracción de la información de registros y notificaciones de la CVTT. • Comparten: ○ Generación de enlaces para compartir información en nube de la CVTT. • Suprimen: No aplica
Obligaciones:	• Confidencialidad: ○ Autorización de accesos, definir roles y privilegios para el uso de la plataforma de registro y notificación de información de la CVTT ○ Resguardar credenciales de acceso a plataforma. • Integridad: ○ Definir las reglas para validación de la información. • Disponibilidad: Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: Administrando los privilegios de acceso. • Integridad: Mantenimiento al servidor de base de datos. • Disponibilidad: Asegurar que el sistema siempre este en línea.
Ricardo Albarrán Romero Laura Lechuga Rodríguez	Jefe del Departamento de Soporte Técnico Servicio profesional de la DITD	• Recaban: ○ Seguimiento a registro y envío de notificaciones. ○ Diseño de instrumentos para el registro y notificación de información de la CVTT. • Procesan: ○ Generación de reportes sobre confirmación y asistencia a eventos. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos a las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Beatriz Barros Ruíz Julio Cesar Cosbert Vázquez César Alejandro León Pineda Alba Inés Sánchez Vázquez Abigail López Álvarez Diana Nadxelii Casas Gutiérrez Angelina Alejandra	Coordinadora de Apoyo a la Vinculación Coordinador de Transferencia Tecnológica de Proyectos de las Ciencias de la Vida y de la Salud Coordinador de Transferencia Tecnológica de Proyectos de Química, Ingenierías y Materiales Coordinadora de la Incubadora de Empresas de Base Tecnológica InnovaUNAM Líder de Proyecto de Emprendimiento Líder de Proyecto Incubación Jefa de Área de Gestión Administrativa	• Recaban: No aplica • Procesan: ○ Consultan información de reportes sobre confirmaciones y asistencia a eventos. ○ Consultan información registrada en el instrumento por los usuarios. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos a las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Canales López de Nava Alcira Barrera Núñez	 Coordinadora de Comunicación y Proyectos Especiales		
María Mercedes Navarrete Jiménez Byron Ballesteros Argueta Nadia Fernanda Salgado Suari	Coordinadora de Vinculación Servicio profesional de la DST Líder de Proyecto de Logística y Relaciones Publicas	• Recaban: No aplica • Procesan: ○ Consultan información de reportes sobre asistencia a eventos. ○ Editan y agregan registros a la base central de participantes. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos a las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-07: Gestión de Convocatorias Consorcio UNAM TEC

Datos personales (sensibles o no) contenidos en el sistema:	• Integrantes de equipos que postulan propuestas a las convocatorias del Cosorcio UNAM-TEC, los cuales son miembros de la comunidad de la UNAM y del TEC : Nombre, Primer apellido, Segundo apellido, Correo electrónico, Número celular de contacto, Institución de adscripción, Entidad de adscripción, Último grado de estudios, Tipo de comunidad, Comprobante de pertenencia a su institución, Rol que desempeña el postulante en el proyecto, Actividad principal dentro del equipo de trabajo, Fotografía en identificación, firma autógrafa, video, datos de proyecto postulado, resultado de postulacion. • Personal de organizaciones externas que tienen interes en la transferencia de la tecnología generada por la propuesta: Nombre completo, correo electrónico, organización a la que pertenece, puesto, firma autógrafa. • Evaluadores de las tecnologías, puede ser personal UNAM, del TEC o Externos: Nombre completo, correo electrónico, evaluaciones de proyectos.

Para que se usan los datos	• Registrar propuestas a convocatorias del Consorcio UNAM-TEC • Evaluar propuestas a convocatorias del Consorcio UNAM-TEC • Adquirir recursos para las propuestas selecionadas • Seguimiento a avances de proyectos

¿Cómo se obtienen los datos personales?	☐ Físico	No aplica
	☒ Digital	• Plataforma para postulación de Proyecto: [redacted] • Plataforma de evaluación de proyectos: [redacted] • Nube de la CVTT: [redacted] • Plataforma de mesa de ayuda [redacted] • Plataforma de Sello Digital Universitario: [redacted]

Temporalidad de obtención	Conforme lo especificado en las Convocatorias del Consorcio UNAM TEC.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
• Recepción de propuestas que se postulan a Convocatorias. • Grabaciones de webinar sobre convocatorias.	• Publicación en youtube de webinars sobre convocatorias. • Atención de solicitudes de información.	• Evaluadores para registrar calificaciones de la rúbrica correspondiente. • Personal de la UA de la CVTT para la adquisición de	La información no se suprime, se conserva en archivo permanente.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
• Recepción de solicitudes de información, apoyo para generación de binómios de colaboración. • Registro de calificaciones de rúbrica por los evaluadores. • Solicitudes de recursos para proyectos aprobados.	• Apoyo para conformación de binomios. • Extración de la Plataforma para postulación de Proyecto. • Transformación de datos y carga a Plataforma de evaluación de proyectos. • Generar resultados de evaluación de propuestas. • Generar de documentos auxiliares para el Comité Técnico del Consorcio para la toma de decisiones sobre selección y aprobación de proyectos. • Notificar vía correo electrónico sobre eventos, reuniones y nuevas convocatorias. • Respaldar información.	recursos para los proyectos aprobados. • Personal de la DJ de la CVTT para Gestión de instrumentos consensuales. • Personal del TEC para la adquisición de recursos para los proyectos aprobados. • Personal del TEC para diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI.	

¿Los datos se transfieren o comparten?	☒ Comparten ☒ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ Interior CVTT		UA de la CVTT	Adquisición de recursos
	☒ Áreas Universitarias		DJ de la CVTT	Gestión de Instrumentos Consensuales
	☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas			
	☒ Personas morales ☐ Otro		TEC	Adquisición de recursos Diseño de estrategias y toma de decisiones

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de Sistema de Tratamiento de datos personales:	L.I Alma Rosa García Martínez
Cargo:	Directora de Información y Transformación Digital
Funciones:	• Recabar: ○ Diseño de instrumentos para el registro de propuestas. ○ Seguimiento a registro de propuestas postuladas. • Procesan: ○ Extracción, transformación y carga de propuestas postuladas al sistema de evaluación. • Comparten: ○ Generación de enlaces para compartir información en nube de la CVTT.

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
	• Suprimen: ○ No aplica
Obligaciones:	• Confidencialidad: ○ Autorización de accesos, definir roles y privilegios para el uso del sistema a plataformas para postulación de Proyecto, evaluación de proyectos, nube de la CVTT y mesa de ayuda. ○ Solicitud de accesos a plataforma de Sello Digital Universitario. ○ Resguardar credenciales de acceso a plataformas. • Integridad: ○ Definir las reglas para validación de la información. • Disponibilidad: ○ Establecer los periodos en los que debe estar disponible la información.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Arturo Santos García	Director de Transferencia de tecnología del TEC	• Recaban: No aplica • Procesan: ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI. ○ Evaluación de propuestas. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Jorge Abel Avendaño	Director de Comercialización y Transferencia Tecnológica del TEC y Coordinador General del Consorcio por parte del TEC.	• Recaban: No aplica • Procesan: ○ Apoyo para conformación de binomios. ○ Adquisición de recursos para los proyectos aprobados. ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI. ○ Evaluación de propuestas. ○ Generar de documentos auxiliares para el Comité Técnico del Consorcio para la toma de decisiones sobre selección y aprobación de proyectos. ○ Notificar vía correo electrónico sobre eventos, reuniones y nuevas convocatorias. • Comparten: ○ Con áreas internas del TEC responsables de adquisiciones, protección PI y acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ Solicitar accesos a la información para colaboradores del TEC. ○ Asegurarse que todas las personas con acceso a los datos personales firmen cartas de confidencialidad correspondientes. ○ No compartir información con personal no autorizado para las funciones correspondientes.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Benito Sotelo Villa	Gerente de relaciones institucionales y con Gobierno del TEC y Secretario Técnico del Consorcio por parte del TEC	• Recaban: No aplica • Procesan: ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI. ○ Evaluación de propuestas. ○ Generar de documentos auxiliares para el Comité Técnico del Consorcio para la toma de decisiones sobre selección y aprobación de proyectos. • Comparten: ○ Con áreas internas del TEC responsables de adquisiciones, protección PI y acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Pedro Castillo Novoa	Relaciones Corporativas	• Recaban: No aplica • Procesan: ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI. ○ Evaluación de propuestas. • Comparten: ○ Con áreas internas del TEC responsables acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Hazael Pinto Piña	Especialista en Comercialización de Tecnologías	• Recaban: ○ Consulta de propuestas postuladas. • Procesan: ○ Apoyo para conformación de binomios. ○ Adquisición de recursos para los proyectos aprobados. ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI. ○ Evaluación de propuestas. ○ Generar de documentos auxiliares para el Comité Técnico del Consorcio para la toma de decisiones sobre selección y aprobación de proyectos.	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ Solicitar accesos a la información para colaboradores del TEC. ○ Asegurarse que todas las personas con acceso a los datos personales firmen cartas de confidencialidad correspondientes. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		○ Notificar vía correo electrónico sobre eventos, reuniones y nuevas convocatorias. • Comparten: ○ Con áreas internas del TEC responsables de adquisiciones, protección PI y acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	
Nidya Balbina Solis Hernández María Helena Sánchez Tual	Especialistas en protección de Propiedad Intelectual del TEC	• Recaban: No aplica • Procesan: ○ Evaluación de propuestas. ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos y protección de PI. • Comparten: ○ Con áreas internas del TEC responsables protección PI y acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Delfina María Guedimin Bojorquez	Especialista en Transferencia Tecnológica del TEC	• Recaban: No aplica • Procesan: ○ Evaluación de propuestas. ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos y Transferencia Tecnológica. • Comparten: ○ Con áreas internas del TEC responsables Transferencia Tecnológica y acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Jorge Manuel Vázquez Ramos	Coordinador de Vinculación y Transferencia Tecnológica	• Recaban: No aplica • Procesan: ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI, transferencia. ○ Evaluación de propuestas. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Eduardo Urzúa Fernández	Director de Emprendimiento Universitario y Coordinador General del Consorcio por parte de la UNAM	• Recaban: No aplica • Procesan: ○ Apoyo para conformación de binomios. ○ Adquisición de recursos para los proyectos aprobados. ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI. ○ Evaluación de propuestas. • Comparten: ○ Con áreas internas de la UNAM responsables de adquisiciones y acuerdos del Consorcio a cargo de la UNAM. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ Solicitar accesos a la información para colaboradores de la UNAM. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Alba Inés Sánchez Vázquez	Coordinadora de la Incubadora de Empresas de Base Tecnológica InnovaUNAM y Secretario Técnico del Consorcio por parte de la UNAM	• Recaban: ○ Seguimiento a registro de propuestas postuladas. • Procesan: ○ Apoyo para conformación de binomios. ○ Alta de evaluadores. ○ Asignación de propuestas por evaluar a cada Evaluador. ○ Notificación y recordatorios de propuestas por evaluar. ○ Seguimiento de avance de evaluaciones. ○ Evaluación de propuestas. ○ Generar de documentos auxiliares para el Comité Técnico del Consorcio para la toma de decisiones sobre selección y aprobación de proyectos. ○ Adquisición de recursos para los proyectos aprobados. ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, aprobaciones de recursos, protección de PI, transferencia. ○ Notificar vía correo electrónico sobre eventos, reuniones y nuevas convocatorias. ○ Grabaciones de sesiones informativas. • Comparten: ○ Con áreas internas de la UNAM responsables de adquisiciones,	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ Gestionar acceso a la información para colaboradores de la UNAM. ○ Asegurarse que todas las personas con acceso a los datos personales firmen cartas de confidencialidad correspondientes. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		protección PI, gestión de instrumentos consensuales y acuerdos del Consorcio a cargo de la UNAM. • Suprimen: No aplica	
María Isabel Mascorro Velarde Julio César Cosbert César Alejandro León Pineda Claudia Lidia Díaz Pérez	Directora de Transferencia de Tecnología Coordinador de Transferencia Tecnológica de Proyectos de las Ciencias de la Vida y de la Salud Coordinador de Transferencia Tecnológica de Proyectos de Química, Ingenierías y de Materiales Asistente de la DTT	• Recaban: No aplica • Procesan: ○ Evaluación de proyectos ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de seguimiento de proyectos, protección de PI y Transferencia. • Comparten: ○ Con áreas internas de la responsables protección PI, gestión de instrumentos consensuales y acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Salvador Enrique Morales Herrera Sara Marlene Ugalde Matehuala Luis Rodríguez Salazar Patricia Camacho Santillan	Coordinador de Propiedad Intelectual Coordinadora de Gestión de Propiedad Intelectual Coordinador de Seguimiento y Atención de las Acciones Oficiales Asistente Ejecutiva Coordinación PI	• Recaban: No aplica • Procesan: ○ Evaluación de proyectos ○ Diseño de estrategias y toma de decisiones del Consorcio en materia de protección de PI. • Comparten: ○ Con áreas UNAM responsables de protección PI y de acuerdos del Consorcio a cargo del TEC. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Claudia Llanos Argüello	Directora Jurídica	• Recaban: No aplica • Procesan: ○ Diseño de estrategias y toma de decisiones del Consorcio. • Comparten: ○ Con áreas UNAM responsables para la gestión de instrumentos consensuales. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Diana Casas Gutiérrez	Líder de Proyecto Sistema de Incubadoras de Empresas InnovaUNAM	• Recaban: No aplica • Procesan: ○ Generar de documentos auxiliares para el Comité Técnico del Consorcio para la toma de decisiones sobre selección y aprobación de proyectos. ○ Adquisición de recursos para los proyectos aprobados. ○ Notificar vía correo electrónico sobre eventos, reuniones y nuevas convocatorias. • Comparten: ○ Con áreas internas de la CVTT responsables de adquisiciones, protección PI, gestión de instrumentos consensuales y acuerdos del Consorcio a cargo de la UNAM. • Suprimen: No aplica	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Alcira Barrera Núñez Angelina Alejandra Canales López de Nava	Coordinadora de Comunicación y Proyectos Especiales Jefa de Área de Gestión Administrativa de la DEU	• Consulta de información.	• Confidencialidad: ○ Resguardar los accesos las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.
Alejandro Canela Alejandro Carlos Farias Zúñiga Andrés Ferrara Carlos Aguirre Acosta Carlos Medina Ayala César Gutiérrez Pérez César Fernando González Monterrubio Edgar Eli Vergara Enrique de Hoyos Guajardo Enrique Galindo	Evaluadores	• Procesan: ○ Evaluación de proyectos	• Confidencialidad: ○ Resguardar los accesos a las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Enrique Zamacona Ernesto Rivera Gabriela Matzallani Gómez Alvarado Héctor Valle Mesto Jaime Reyes Robles Jesús Seañez Jorge Luis Martínez Rodríguez José Bortoni Juan Carlos Martínez Karla Serrano González Leopoldo Ruiz Luis Gastélum Marco Antonio Castellanos Marco Antonio Huerta María Yolanda Delgadillo Saldaña Marlen González Nestor Quintero Octavio Tonatiuh Ramírez Reivich Porfirio Caballero Mata Ramsés Galaz Ricardo Lozada Rolando Cortés Vázquez			
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Carga de documentos de propuestas postuladas al sistema de evaluación.	• Confidencialidad: Administrando los privilegios de acceso. • Integridad: Mantenimiento al servidor de base de datos.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica • Suprimen: No aplica	• Disponibilidad: Asegurar que el sistema siempre este en línea.
Ricardo Albarrán Romero Laura Lechuga Rodríguez	Jefe del Departamento de Soporte Técnico Servicio profesional de la DITD	• Recaban: ○ Seguimiento a registro de propuestas postuladas. ○ Diseño de instrumentos para el registro de propuestas y a eventos. ○ Seguimiento a registro eventos (webinars y sesiones informativas) ○ Grabación de eventos. • Procesan: ○ Generación de reportes sobre asistencia a eventos.	• Confidencialidad: ○ Resguardar los accesos a las plataformas. ○ No compartir información con personal no autorizado para las funciones correspondientes.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DJ–01: Instrumentos Consensuales

Datos personales (sensibles o no) contenidos en el sistema:	• Nombre completo • Correo Electrónico • Dirección • Firma autógrafa • Fotografía de la persona • Representación legal

Para que se usan los datos	Elaboración y trámite de instrumentos consensuales.

¿Cómo se obtienen los datos personales?	☒ Físico	Del proyecto de instrumento consensual que entrega el área solicitante • Proyecto de Convenio • Identificación oficial • Poder notarial • Acta constitutiva de empresas • Comprobante de domicilio
	☒ Digital	Del proyecto de instrumento consensual que entrega el área solicitante • Proyecto del intrumento consensual. • Identificación oficial • Poder notarial • Acta constitutiva de empresas Comprobante de domicilio

Temporalidad de obtención	Permanente

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
• Recibe el proyecto instrumento consensual y los documentos legales.	• Se coteja la información del instrumento consensual contra los documentos legales y se realizan las correcciones necesarias. • Se crea un expediente físico con la información del asunto.	• Se envía a la Oficina de la Abogacía General el instrumento consensual y los documentos legales para su validación y registro. • Se envía a la Dirección General de Patrimonio Universitario el instrumento consensual para su autorización.	• No aplica

	• Se crea un expediente digital con la información del asunto.	• Se entrega el instrumento consensual validado al área solicitante para firma y/o entrega de dicho instrumento.	

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☐ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Dirección General de Asuntos Jurídicos de la OAG de la UNAM Dirección General de Estudios de Legislación Universitaria de la OAG de la UNAM Dirección General de Patrimonio Universitario	Validación, firma y/o entrega del instrumento consensual

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Mtra. Claudia L. Llanos Argüello
Cargo:	Directora Jurídica
Funciones:	• Recibir el proyecto del instrumento consensual y la documentación legal. • Verifica la información • Se comparte el instrumento consensual a las áreas universitarias para su validación, firma y/o entrega de dicho instrumento
Obligaciones:	• Mantener la confidencialidad de los datos personales inmersos en el instrumento consensual y la documentación legal., no compartiéndola a terceros • Resguardar el expediente del instrumento consensual en la oficina de la Dirección jurídica. • Dar acceso a la información de los expedientes a su resguardo en caso de ser autorizado.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Lic. Claudia Patricia González Villegas	Jefe de Departamento	• Recibir el proyecto del instrumento consensual y la documentación legal • Revisar y cotejar la información • Compartir el instrumento consensual a las áreas universitarias para su validación, firma y/o entrega de dicho instrumento	• Mantener la confidencialidad de los datos personales inmersos en el instrumento consensual, no compartiéndola a terceros no autorizados. • Mantener la información de los expedientes de los instrumentos consensuales actualizada y resguardada en la oficina de la Dirección Jurídica.

[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: DIRECCIÓN DE SERVICIOS TECNOLÓGICOS

ID: DST–01: Vinculación Interna

Datos personales (sensibles o no) contenidos en el sistema:	Nombre completo, cargo, correo electrónico institucional, teléfono institucional y teléfono celular,

Para que se usan los datos	Se utiliza la información para la comunicación permanente con los responsables de vinculación de cada entidad o dependencia. Vía correo electrónico institucional se hacer llegar información sobre: • Eventos organizados por la Coordinación para los responsables de vinculación: (encuentros y actividades de capacitación. • Difusión de convocatorias y eventos, como es el caso de ferias, seminarios, cursos, entre otros. • Solicitudes de Servicios Tecnológicos . Esta actividad responde al procedimiento de vinculación interna establecido en el Sistema de Gestión de Calidad, de la Dirección de Servicios Tecnológicos bajo la norma ISO 9901 2015.

¿Cómo se obtienen los datos personales?	☒ Físico	En actividades presenciales a través del registro en las listas de asistencia que se elaboran para los eventos organizados por la Coordinación para los vinculadores (encuentro y las actividades de capacitación). Mediante oficio para la designación de representantes de vinculación ante el Comité de Vinculación Universitaria y de Transferencia de la UNAM.
	☒ Digital	En activiades virtuales a través del registro digital en la plataforma de videoconferencia. A través de correo electrónico institucional que se envía a los vinculadores solicitando la información para actualizar el directorio de vinculadores universitarios.

Temporabilidad de obtención	Permanente

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Se envía correo institucional solicitando la información para actualizar el directorio de vinculadores universitarios.	La información proporcionada se registra en el "DIRECTORIO DE REPRESENTANTES DE VINCULACIÓN" en un archivo de Excel y en la [redacted]	La información de datos personales de los responsables de vinculación se comparte con las DITD y la CCPE, para el envío de comunicados y envío de	No aplica

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Se obtiene a través del registro en las listas de asistencia de los eventos organizados por la Coordinación. Mediante oficio para la designación de representantes de vinculación ante el Comité de Vinculación Universitaria y de Transferencia de la UNAM.	[redacted] Este directorio se consulta de manera constante para mantener comunicación con el responsable de vinculación de cada entidad y dependencia universitaria. El registro en [redacted] se utiliza para el envío de comunicados y recopilación de invormación. Es una base de datos que se actualiza de manera periódica, modificando el directorio con la información proporcionada mediante los mecanismos especificados.	instrumentos para recopilar invormación.	

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Con la DITD y la CCPE de la CVTT. Con otras áreas de la CVTT y los responsables de vinculación de las diferentes entidades y dependencias universitarias.	Para el envío de comunicados y envío de instrumentos para recopilar información Para fines de vinculación y atención al desarrollo de un proyecto conjunto.

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Nombre:	ROBERTO GARCÍA OCAÑA
Cargo:	DIRECTOR DE SERVICIOS TECNOLÓGICOS
Funciones:	• Autorizar al personal de la dirección a su cargo, el acceso a la información de datos personales. • Compartir de manera específica la información para los fines de vinculación universitaria
Obligaciones:	• Guardar confidencialidad de la información de datos personales de los vinculadores • Garantizar la integridad de los datos personales de los vinculadores

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
NO APLICA			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
MARIA MERCEDES NAVARRETE JIMÉNEZ	COORDINADOR DE SERVICIOS TECNOLÓGICOS VINCULACIÓN CON ENTIDADES Y DEPENDENCIAS DE LA UNAM	• Recabar la información de datos personales a través del correo institucional, oficios de designación o por la información recabada en las listas de asistencia • Procesar la información de datos personales en un archivo [redacted] Este archivo se encuentra en Repoositorio Institucional de la CVTT. • Compartir, vía correo electrónico institucional y de manera específica, la información de datos personales de los representantes de vinculación y otras áreas de la CVTT.	• Guardar confidencialidad de la información proporcionada por los vinculadores. • Garantizar la integridad de los datos personales de los vinculadores.
CARLOS MOLES	COORDINADOR DE SERVICIOS TECNOLÓGICOS VINCULACIÓN CON LOS SECTORES DE LA SOCIEDAD EMPRESARIAL Y GOBIERNO	• Recabar la información de datos personales a través del correo institucional. • Compartir, vía correo electrónico institucional y de manera específica, la información de datos personales de los representantes de vinculación y otras áreas de la CVTT.	• Guardar confidencialidad de la información proporcionada por los vinculadores. • Garantizar la integridad de los datos personales de los vinculadores.
BEATRIZ BARROS	COORDINADOR DE PROYECTOS DE INNOVACIÓN TECNOLÓGICA	• Recabar la información de datos personales a través del correo institucional. • Compartir, vía correo electrónico institucional y de manera específica, la información de datos personales de los representantes de	• Guardar confidencialidad de la información proporcionada por los vinculadores. • Garantizar la integridad de los datos personales de los vinculadores.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Usuarios del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento[2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		vinculación y otras áreas de la CVTT.	
BYRON BALLESTEROS	HONORARIOS SOPORTE TÉCNICO EN TIC	• Recabar la información de datos personales a través del correo institucional o por la información recabada en las listas de asistencia • Procesar la información de datos personales en un archivo [redacted] Este archivo se encuentra en Repoositorio Institucional de la CVTT. Integrar la información de datos personales en [redacted].	• Guardar confidencialidad de la información proporcionada por los vinculadores. • Garantizar la integridad de los datos personales de los vinculadores.
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Administrar privilegios de acceso. • Integridad: ○ Mantenimiento al servidor de base de datos. • Disponibilidad: ○ Asegurar el acceso a las plataformas y servicios TIC.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: DIRECCIÓN DE SERVICIOS TECNOLÓGICOS

ID: DST–02: Vinculación Externa

Datos personales (sensibles o no) contenidos en el sistema:	Nombre de la empresa, domicilio, página web, nombre completo del contacto, cargo, teléfono celular y correo electrónico. Documentos probatorios: Poder notarial, Acta constitutiva, Comprobante domicilio, Identificación oficial.

Para que se usan los datos	Se utiliza la información para el registro, atención y seguimiento de la solicitud de servicios tecnológicos, así como la formalización de instrumentos jurídicos. Esta actividad responde al procedimiento de vinculación interna establecido en el Sistema de Gestión de Calidad, de la Dirección de Servicios Tecnológicos bajo la norma ISO 9901 2015.

¿Cómo se obtienen los datos personales?	☐ Físico	NO APLICA
	☒ Digital	A través de: Correo que envía el usuario a un correo electrónico institucional y donde envía anexo, el formato de solicitud de servicios con la información correspondiente. Formulario [redacted]

Temporabilidad de obtención	permanente

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Se envía un correo electrónico institucional al usuario y se anexa el formato de solicitud de servicios tecnológicos. El usuario responde al correo institucional enviado anexo el formato con la información correspondiente. O bien el usuario accediendo desde el sitio enlace.unam.mx llena el Formulario de Google.	Los formatos de solicitud de servicio se almacenan en el Repositorio Institucional de la CVTT y en los equipos de cómputo de los colaboradores de la CVTT. La información proporcionada por el usuario se registra en la base de datos [redacted] La información proporcionada se consulta	Vía correo electrónico institucional, se comparte la información con el responsable de vinculación, el investigador y/o académico, de la entidad o dependencia, que puede atender la solicitud. Para la formalización de los instrumentos jurícos se entrega de manera física y digital a la DJ de la CVTT los documentos probatorios	Se archiva en la base de datos [redacted] y se conserva por dos años.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
	para dar atención y seguimiento a la solicitud.	necesarios y el preliminar del Convenio.	

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Con el responsable de vinculación, el investigador y/o académico, de la entidad o dependencia, que puede atender la solicitud de servicios. Con la DJ de la CVTT.	Para que la entidad o dependencia pueda atender y dar seguimiento a la solicitud de servicios. Para la formalización de instrumentos jurídicos.

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Nombre:	ROBERTO GARCÍA OCAÑA
Cargo:	DIRECTOR DE SERVICIOS TECNOLÓGICOS
Funciones:	• Dar autorización para el manejo de la información. • Compartir de manera específica la información para los fines de vinculación universitaria
Obligaciones:	• Guardar confidencialidad de la información de datos personales de los usuarios de servicios tecnológicos. • Garantizar la integridad de los datos personales manejados.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
NO APLICA			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
CARLOS MOLES	COORDINADOR DE SERVICIOS TECNOLÓGICOS VINCULACIÓN CON LOS SECTORES DE LA SOCIEDAD EMPRESARIAL Y GOBIERNO	• Recabar la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios • Procesar la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios para	• Guardar confidencialidad de la información de datos personales proporcionada por el usuario. • Garantizar la integridad de la información de datos personales proporcionada por el usuario. • Garantizar la disponibilidad de la información al

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		registrarla en la base de datos [redacted] • Compartir la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios con el responsable de vinculación, el investigador y/o académico de la entidad o dependencia universitaria correspondiente. • Respalda la información proporcionada por el usuario de la base de datos [redacted] cada dos años.	administrar la cuenta [redacted] y realizando los respaldos correspondientes.
BEATRIZ BARROS	COORDINADOR DE PROYECTOS DE INNOVACIÓN TECNOLÓGICA	• Procesar la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios para registrarla en la base de datos [redacted]	• Guardar confidencialidad de la información de datos personales proporcionada por el usuario. • Garantizar la integridad de la información de datos personales proporcionada por el usuario.
MARIA MERCEDES NAVARRETE J.	COORDINADOR DE SERVICIOS TECNOLÓGICOS VINCULACIÓN CON ENTIDADES Y DEPENDENCIAS DE LA UNAM	• Recabar la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios • Compartir la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios con el responsable de vinculación, el investigador y/o académico de la entidad o dependencia universitaria correspondiente.	• Guardar confidencialidad de la información de datos personales proporcionada por el usuario. • Garantizar la integridad de la información de datos personales proporcionada por el usuario.
BYRON BALLESTEROS.	SOPORTE TÉCNICO EN TIC	• Recabar la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios y a traves del formulario de Google. • Procesar la información de datos personales proporcionados por el usuario en el formato de solicitud de servicios para	• Guardar confidencialidad de la información de datos personales proporcionada por el usuario. • Garantizar la integridad de la información de datos personales proporcionada por el usuario.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		registrarla en la base de datos [redacted]	

Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica
		• Procesan:
		  ○ Respaldos periódicos de la información almacenada en la base de datos.
		• Comparten: No aplica
		• Suprimen: No aplica
			• Confidencialidad:
			  ○ Administrar privilegios de acceso.
			• Integridad:
			  ○ Mantenimiento al servidor de base de datos.
			• Disponibilidad:
			  ○ Asegurar el acceso a las plataformas y servicios TIC.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DTT – 01: Proceso Transferencia Tecnológica

Datos personales (sensibles o no) contenidos en el sistema:	Puede dar tratamiento a datos personales de colaboradores de la UNAM y organizaciones externas. Los datos que se pueden recopilar son: nombre completo, cargo, correo electrónico institucional, teléfono institucional y en algunos casos teléfono celular, comprobante de domicilio, identificación personal , fira autógrafa, datos fiscales.

Para que se usan los datos	Formalización de Convenios de Colaboración para la Transferencia de Tecnología y/o de Confidencialidad para compartir información que permita la la negociación de acuerdos de transferencias.

¿Cómo se obtienen los datos personales?	☒ Físico	Entrega directa de documentos probatorios con información de datos personas
	☒ Digital	Correo electrónico enviado por el interesado.

Temporabilidad de obtención	Bajo solicitud

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
A través de correos electrónicos o en formato físico entregado al personal de la DTT.	Se abre un expediente fisico y digital par cada aproceso de transferecnia tecnológica. Se registran los datos recibidos en la “CARTERA DE PROYECTOS”, que se encuentra resguardada en el repositorio institucional de la CVTT. Para la consulta, se ingresa a las computadoras de los integrantes de la DTT, las cuales cuentan con contraseñas.	La información de datos personales se comparte de forma física y digital con la DJ de la CVTT, área responsable de la gestión jurídica de Convenios de Colaboración.	No aplica.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
	En caso de los expedientes físicos, estos se encuentran en [redacted]		

¿Los datos se transfieren o comparten?			¿Con quién?	¿Para qué?
	☒ Comparten ☐ Transfieren	☐ No	1. DJ de la CVTT.	Para revisión, registros y firma de convenios de colaboración.
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro			

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Nombre:	Mtra. María Isabel Mascorro Velarde
Cargo:	Directora de Transferencia de Tecnología
Funciones:	• Recabar información para identificar y promover proyectos universitarios y de personas que participan en convocatorias. • Procesar la información de proyectos universitarios para promoción con las empresas y de personas que participan en convocatorias. • Compartir información con personal adscrito a la CVTT.
Obligaciones:	• Confidencialidad: guardar la privacidad de los datos personales. • Integridad: asegurar la información mediante claves, contraseñas y barreras físicas. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
NO APLICA			

Involucrados en las actividades de tratamiento[2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Julio César Cosbert Vásquez	Coordinador de Transferencia de Tecnología de Proyectos para la Salud.	• Recabar la información específica de los proyectos que se tienen asignados.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Usuarios del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		• Procesar la información específica de los proyectos que se tienen asignados. • Compartir la información específica de los proyectos que se tienen asignados al interior y con otras áreas de la CVTT. • Suprimir en coordinación con la persona responsable la información sensible.	de la información y proteger los expedientes utilizados en el trabajo. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.
César Alejandro León Pineda	Coordinador de Transferencia de Tecnología.	• Recabar la información específica de los proyectos que se tienen asignados. • Procesar la información específica de los proyectos que se tienen asignados. • Compartir la información específica de los proyectos que se tienen asignados al interior y con otras áreas de la CVTT. • Suprimir en coordinación con la persona responsable la información sensible.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo de la información y proteger los expedientes utilizados en el trabajo. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.
Claudia Lidia Díaz Pérez	Asistente de Dirección de Transferencia de Tecnología.	• Recabar la información específica de los proyectos que se tienen asignados. • Procesar la información específica de los proyectos que se tienen asignados. • Compartir la información específica de los proyectos que se tienen asignados al interior y con otras áreas de la CVTT.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo de la información y proteger los expedientes utilizados en el trabajo. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.
Alejandro Arturo Ortega Hernández	Coordinador de Información para Vinculación Universitaria	• Recaban: No aplica • Procesan: ○ Respaldos periódicos de la información almacenada en la base de datos. • Comparten: No aplica • Suprimen: No aplica	• Confidencialidad: ○ Administrar privilegios de acceso. • Integridad: ○ Mantenimiento al servidor de base de datos. • Disponibilidad: ○ Asegurar el acceso a las plataformas y servicios TIC.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DTT – 02: PI

Datos personales (sensibles o no) contenidos en el sistema:	Para inventores, diseñadores, autores y obtentores, para trámites de propiedad intelectual cuyo titular es la UNAM se solicita: • Nombre completo • Fecha y lugar de nacimiento • Correo electrónico • Teléfono • Domicilio • RFC • Entidad/dependencia a la que pertenece • Firma autógrafa

Para que se usan los datos	Los datos personales son requeridos para comenzar trámite de solicitudes en materia de propiedad intelectual, de conformidad con las siguientes legislaciones. • Ley Federal de Protección a la Propiedad Industrial - LFPPI • Reglamento de la Ley de la Propiedad Industrial • Acuerdo que Establece las Reglas para la Presentación de Solicitudes ante el Instituto Mexicano de la Propiedad Industrial • Ley Federal del Derecho de Autor - LFDA • Reglamento de la Ley Federal del Derecho de Autor • Ley Federal de Variedades Vegetales - LFVV • Reglamento de la Ley Federal de Variedades Vegetales • Tratado de Cooperación en materia de Patentes - PCT • Reglamento del Tratado de Cooperación en materia de Patentes • Instrucciones Administrativas del Tratado de Cooperación en materia de Patentes

¿Cómo se obtienen los datos personales?	☒ Físico	• Datos generales de los autores o colaboradores que son requeridos por el Instituto Nacional del Derecho de Autor (INDAUTOR) para el trámite de registro legal de una obra. • Documento de Cesión de Derechos
	☒ Digital	• Datos generales de los autores o colaboradores que son requeridos por el Instituto Nacional del Derecho de Autor (INDAUTOR) para el trámite de registro legal de una obra. • Documento de Cesión de Derechos

Temporalidad de obtención	Los datos se recopilan de manera permanente cada vez que se solicita a esta Coordinación una solicitud de protección de algún desarrollo que surge del quehacer universitario.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Se solicita la información para la generación de un expediente de solicitud de protección.	Se verifica la información y es utilizada para conformar un expediente físico y/o digital sobre su asunto.	Se solicita de manera formal, mediante oficio ante la DGAJ, la presentación de la solicitud de protección. Dicha presentación incluye el expediente generado que incluye datos personales.	Existe destrucción de la información cuando la documentación presenta errores o inconsistencias.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☒ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Dirección General de Asuntos Jurídicos (DGAJ)	La DGAJ en su carácter de apoderado de los asuntos de la UNAM en materia de Propiedad Intelectual necesita los datos para generar el expediente de entrada ante IMPI, SNICS e INDAUTOR. Para comenzar el trámite de protección legal de un desarrollo de conformidad con el marco normativo en materia de Propiedad Intelectual.

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Salvador Enrique Morales Herrera
Cargo:	Coordinador de Propiedad Intelectual
Funciones:	• Recaba, Se solicita y reciben los datos personales como parte de la información necesaria para la generación de un expediente de solicitud de protección • Procesa, Se verifica la información y es utilizada para conformar un expediente sobre el asunto del cual se solicitará protección. El expediente físico y/o digital incluye los datos personales; . • Comparte, Se solicita de manera formal, mediante oficio ante la DGAJ, la presentación de la solicitud de protección. Dicha presentación incluye el expediente generado que incluye datos personales. Para el caso de solicitudes en materia de Propiedad Industrial todos los expedientes son publicados de conformidad con la LFPPI • Suprime, Destrucción de documentación que incluye datos personales cuando dicha documentación es incorrecta o caduca
Obligaciones:	• Mantener confidencialidad de datos personales: ○ Definir personas que tienen acceso a los expedientes previo a la presentación de la solicitud • Garantizar la Integridad de datos personales mediante el resguardo de expedientes • Firma de carta de confidencialidad

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Patricia Camacho Santillán	**Asistente Ejecutiva**	• Recaba, Se solicita y reciben los datos personales como parte de la información necesaria para la generación de un expediente de solicitud de protección • Procesa, Se verifica la información y es utilizada para conformar un expediente sobre el asunto del cual se solicitará protección. El expediente físico y/o digital incluye los datos personales; . • Comparte, No aplica • Suprime, Destrucción de documentación que incluye datos personales cuando dicha documentación es incorrecta o caduca	• Mantener confidencialidad de datos personales: • Garantizar la Integridad de datos personales mediante el resguardo de expedientes • Firma de carta de confidencialidad

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Sara Marlene Ugalde Matehuala	**Coordinadora de Gestión de Propiedad Intelectual**	• Recaba, Se solicita y reciben los datos personales como parte de la información necesaria para respuesta a requerimientos por parte de la autoridad • Procesa, Se verifica la información y es utilizada para conformar un expediente de respuesta de forma ante la autoridad. El expediente de respuesta físico y/o digital incluye los datos personales; • Comparte, Se solicita de manera formal, mediante oficio ante la DGAJ, la presentación de la respuesta a requerimientos formales. Dicha respuesta incluye el expediente con datos personales. • Suprime, Destrucción de documentación que incluye datos	• Mantener confidencialidad de datos personales: • Garantizar la Integridad de datos personales mediante el resguardo de expedientes, • Firma de carta de confidencialidad

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		personales cuando dicha documentación es incorrecta o caduca	
Luis Rodríguez Salazar	**Coordinador de Seguimiento y Atención de las Acciones Oficiales**	• Recaba, Se solicita y reciben los datos personales como parte de la información necesaria para respuesta a requerimientos por parte de la autoridad • Procesa, Se verifica la información y es utilizada para conformar un expediente de respuesta de forma ante la autoridad. El expediente de respuesta físico y/o digital incluye los datos personales; • Comparte, Se solicita de manera formal, mediante oficio ante la DGAJ, la presentación de la respuesta a requerimientos formales. Dicha respuesta incluye el expediente con datos personales. • Suprime, Destrucción de documentación que incluye datos personales cuando dicha documentación es incorrecta o caduca	• Mantener confidencialidad de datos personales: • Garantizar la Integridad de datos personales mediante el resguardo de expedientes, • Firma de carta de confidencialidad

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DTT–03: CONTACTOS DTT

Datos personales (sensibles o no) contenidos en el sistema:	El directorio de contactos para la DTT se integra con datos de personas de: 1. UNAM 2. Empresariales 3. Otras universidades y centros de investigación De cada persona se recaba: nombre, priemer apellido y segundo apellido, cargo, correo electrónico institucional, teléfono institucional y en algunos casos el teléfono celular.

Para que se usan los datos	Intercambiar información sobre desarrollos tecnológicos, agendar reuniones, invitaciones a participar en convocatorias, concursos y promoción de tecnologías a nivel nacional e internacional.

¿Cómo se obtienen los datos personales?	☒ Físico	Entrevistas presenciales Tarjetas de presentación Vía telefónica
	☒ Digital	Consulta a sitios web coorporativos Consulta a redes sociales profesionales

Temporabilidad de obtención	Permanente

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
A través de: • Entrevistas presenciales • Tarjetas de presentación • Vía telefónica • Consulta a sitios web corporativos Consulta a redes sociales profesionales	La información se captura o actualiza en el directorio de contactos. En todos los casos se verifica la incorporación del contacto vía correo electrónico con el titular de los datos.	La información de datos personales se comparte al interior de la CVTT bajo requerimiento con otras áreas de la CVTT.	Eliminación de datos sólo en los casos que el contacto lo solicité o bien se cuente con información sobre el cese de funciones como contacto de transferencia técnológica.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién? 1. CCPE de la CVTT.	¿Para qué? Para promover información sobre desarrollos universitarios, invitación a eventos.
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro			

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Nombre:	Mtra. María Isabel Mascorro Velarde
Cargo:	Directora de Transferencia de Tecnología
Funciones:	• Recabar información para identificar y promover proyectos universitarios y de personas que participan en convocatorias. • Procesar la información de proyectos universitarios para promoción con las empresas y de personas que participan en convocatorias. • Compartir información con personal adscrito a la dirección y de la CVTT, empresas, investigadores y funcionarios universitarios y otras áreas. • Elaborar medidas de seguridad para la supresión de datos desactualizados.
Obligaciones:	• Confidencialidad: guardar la privacidad de los datos personales. • Integridad: asegurar la información mediante claves y contraseñas. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
NO APLICA			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Julio César Cosbert Vásquez	Coordinador de Transferencia de Tecnología de Proyectos para la Salud.	• Recabar la información específica de los proyectos que se tienen asignados. • Procesar la información específica de los proyectos que se tienen asignados. • Compartir la información específica de los proyectos que se tienen asignados al interior y con otras áreas de la CVTT. • Suprimir en coordinación con la persona responsable la información sensible.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo de la información y proteger los expedientes utilizados en el trabajo. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.
César Alejandro León Pineda	Coordinador de Transferencia de Tecnología.	• Recabar la información específica de los proyectos que se tienen asignados. • Procesar la información específica de los proyectos que se tienen asignados. • Compartir la información específica de los proyectos que se tienen asignados al interior y con otras áreas de la CVTT. • Suprimir en coordinación con la persona responsable la información sensible.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo de la información y proteger los expedientes utilizados en el trabajo. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Usuarios del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Claudia Lidia Díaz Pérez	Asistente de Dirección de Transferencia de Tecnología.	• Recabar la información específica de los proyectos que se tienen asignados. • Procesar la información específica de los proyectos que se tienen asignados. • Compartir la información específica de los proyectos que se tienen asignados al interior y con otras áreas de la CVTT. • Suprimir en coordinación con la persona responsable la información sensible.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo de la información y proteger los expedientes utilizados en el trabajo. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: UA-01 Personal de Estructura

Objetivo del sistema	Elaborar altas, bajas, reingresos, actualizaciones, entre otros movimientos del personal contratado por estructura de la CVTT.

Datos personales (sensibles o no) contenidos en los expedientes:	Nombre, apellidos, domicilio, número de cuenta para pagos, RFC, CURP, teléfono personal.

Para que se usan los datos	Para dar de alta personal por estructura de nuevo ingreso en la Coordinación de Vinculación y Transferencia Tecnológica en el sistema integral de personal de la UNAM (SIP), el cual solicita en algunos de sus campos que se escaneen diversos documentos de los antes descritos.

¿Cómo se obtienen los datos personales?	☒ Físico	Documentos en original ✓ Acta de nacimiento actualizada ✓ Solicitud de Empleo ✓ Currículo Vitae actualizado firmado Fotocopias de la siguiente documentación: ✓ Constancia de último Grado Estudios, Título o grado académico ✓ Comprobante de Domicilio (Recibo de pago de agua, teléfono, con código postal, máximo 3 meses) ✓ 1 Fotografía tamaño infantil a color con Fondo Blanco ✓ Registro Federal de Contribuyentes RFC (Cédula Fiscal) ✓ Constancia de situación fiscal ✓ CURP proporcionados por la SHCP ✓ Identificación Oficial Vigente con Fotografía (IFE o Pasaporte) ✓ Estado de Cuenta Bancario Se solicitan a los interesados por contratar, mediante solicitud por escrito que se les entrega de manera física en el momento de ser autorizada su contratación
	☐ Digital	

Temporalidad de obtención	Por evento (en el momento que se tiene la autorización para que el personal sea contratado)

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Mediante listado de documentos que se le entrega al interesado, y los cuales debe de reunir en máximo 5 días posteriores y entregarlos al Jefe de Recursos Humanos para su trámite.	Se abre un expediente físico en folders individuales, los cuales se resguardan en el archivero correspondiente para utilizarlos cuando sea necesario. El uso de los datos es para ingresarlos en diversos campos dentro del sistema SIP de personal, el cual es institucional para llevar a cabo los movimientos del personal de la dependencia. Los documentos probatorios se digitalizan por medio del SIP, en donde se almacenan.	Personal de la Dirección General de personal de la UNAM tiene acceso a la información utilizando el Sistema Integral de Personal (SIP) para su trámite.	No se destruye la información.

¿Los datos se transfieren o comparten?	☒ Compartir ☒ Transferir	☐ No	¿Con quién?	¿Para qué?
	☐ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Dirección General de Personal de la UNAM	Para dar dar trámite a los diversos movimientos de personal solicitados.

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Lic. Oscar Ramírez González
Cargo:	Jefe de Unidad Administrativa
Funciones:	• Recaban, a solicitud de los titulares de las áreas de la CVTT se envía el listado de documentos para la contratación de personal por estructura. • Revisa la información ingresada en el SIP, en su caso autoriza la solicitud de revisión y autorización del movimiento por parte de la DGP. • Firma autógrafa de solicitudes de movimientos autorizados por la DGP, para su formalización.
Obligaciones:	• Confidencialidad: ○ Resguardar las credenciales de acceso al SIP y de la FEU. ○ Solicitar el acceso o eliminación de accesos a usuarios del SIP. • Integridad: ○ Revisar los datos en las solicitudes ingresadas al SIP por el Jefe de Personal. • Disponibilidad: ○ Autorizar al Jefe de personal que permita el acceso a la información de los colaboradores de la CVTT en el momento que sea solictado.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Mtro. Salvador Cuandón Vieyra	Jefe de personal	• Recabar: cita al personal de nuevo ingreso para entregarle listado de documentos para su alta y se le da un plazo de no más de 5 días para que los entregue en la Unidad Administrativa • Procesa: ○ Se genera y resguarda un expediente físico por persona. ○ Dentro del sistema de personal SIP, se digitalizan los documentos probatorios y se llenan los campos de acuerdo a los requerimientos del programa para cada tipo de solicitud. • Comparte: ○ Transferir mediante el SIP las solicitudes de movimientos aprobadas por el Jefe de la Unidad. ○ Una vez que esté autorizado el trámite imprimir el movimiento para firma autografa de los interesados y testigos, para posteriormente entregarlas de forma física anexando los documentos a la Dirección General de Personal. • Resguardo: una vez que se libera el trámite se resguarda el documento con sello original de la Dirección General de Personal y se integra al expediente.	• Confidencialidad: ○ Resguardar las credenciales de acceso al SIP. ○ Archivar la información del personal dentro de los lugares asignados. ○ Resguardar la llave del archivero en la que se resguardan los expedientes. • Integridad: ○ Cotejar la información original entregada por los colaboradores para su trámite. . ○ Manejar de manera clara y objetiva la información que se requiera para los movimientos del personal. • Disponibilidad: ○ Mantener la información que sea necesaria al momento que se requiera a las personas autorizadas por el Jefe de la Unidad Administrativa.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: UA-02 Servicios profesionales

Objetivo del sistema	Elaborar y gestionar contratos por servicios profesionales.

Datos personales (sensibles o no) contenidos en los expedientes:	Nombre, apellidos, domicilio, número de cuenta para pagos, RFC, CURP, teléfono personal, facturas.

Para que se usan los datos	Para elaborar contratos por servicios profesionales y gestión de pagos.

¿Cómo se obtienen los datos personales?	☒ Físico	Entrega de fotocopias de la siguiente documentación: ✓ Acta de nacimiento ✓ Constancia de último Grado Estudios, Título o grado académico ✓ Comprobante de Domicilio ✓ Registro Federal de Contribuyentes RFC (Cédula Fiscal) ✓ CURP proporcionados por la SHCP ✓ Identificación Oficial Vigente con Fotografía (IFE o Pasaporte) ✓ Estado de Cuenta Bancario ✓ Constancia de situación fiscal
	☒ Digital	Envío de correo electrónico con la digitalización de la siguiente documentación: ✓ Acta de nacimiento ✓ Constancia de último Grado Estudios, Título o grado académico ✓ Comprobante de Domicilio ✓ Registro Federal de Contribuyentes RFC (Cédula Fiscal) ✓ CURP proporcionados por la SHCP ✓ Identificación Oficial Vigente con Fotografía (IFE o Pasaporte) ✓ Estado de Cuenta Bancario ✓ Constancia de situación fiscal ✓ Factura

Temporalidad de obtención	Por evento (en el momento que se tiene la autorización para que el personal sea contratado)

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Físicamente o vía correo electrónico institucional al jefe de personal.	• Se abre un expediente físico en carpetas blancas, los cuales se resguardan en el archivero correspondiente para utilizarlos cuando sea necesario. • El uso de los datos es para ingresarlos en diversos campos dentro del sistema de honorarios de la Dirección General de Personal, el cual es institucional para llevar a cabo las contrataciones necesarias para la CVTT • Una vez autorizado de manera electrónica por la Dirección General de Personal, se solicita de manera autógrafa la firma del interesado en su contrato, terminando de recabar las firmas correspondientes. • Para el proceso de pago se captura en el sistema remoto de pagos de la Dirección General de Finanzas para el trámite del pago. • Se resguarda el recibo de la entrega de cheque.	Colaboradores de la Dirección General de personal de la UNAM tiene acceso a la información utilizando el módulo de honorarios para su trámite. Colaboradores de la Dirección General de Finanzas de la UNAM tiene acceso a la información utilizando el sistema remoto de pagos para su trámite.	No se destruye la información.

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☐ CVTT ☒ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		Dirección General de Personal y la Dirección General de Finanzas de la UNAM	Para elaborar contratos por servicios profesionales según las necesidades de la dependencia. Para realizar los pagos correspondientes al personal contratado por servicios profesionales mediante transferencias bancarias o cheques.

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Lic. Oscar Ramírez González
Cargo:	Jefe de Unidad Administrativa
Funciones:	• Recaban, a solicitud de los titulares de las áreas de la CVTT se envía el listado de documentos para contratación de servicios profesionales. • Procesan, supervisa la ejecución de la contratación. • Firma autógrafa de contratos por servicios profesionales.
Obligaciones:	• Confidencialidad: ○ Solicitar el acceso o eliminación de accesos a usuarios del módulo de honorarios de la Dirección General de Personal. ○ Solicitar el acceso o eliminación de accesos a usuarios al sistema remoto de pagos de la Dirección General de Finanzas. ○ Autoriza al Jefe de Presupuesto para compartir clave de acceso al sistema remoto de pagos de la Dirección General de Finanzas. • Disponibilidad: ○ Autorizar al Jefe de personal que permita el acceso a la información de los servicios profesionales de la CVTT en el momento que sea solicitado.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Mtro. Salvador Cuandón Vieyra	Jefe de Personal	• Recaban, recibe de manera electronica o física la documentación para elaborar contrato por servicios profesionales. • Procesan: ○ Se integra la documentación física al expediente del proyecto o año correspondiente. ○ Dentro del módulo de honorarios de la Dirección General de Personal, se integran los documentos probatorios y datos de acuerdo a los requerimientos del sistema. ○ Una vez que esté autorizado el trámite imprimir el movimiento para firma autografa de los interesados y testigos, para posteriormente entregarlas de forma física anexando los	• Confidencialidad: ○ Resguardar las credenciales de acceso al módulo de honorarios. ○ Resguardar las credenciales de acceso al sistema remoto de pagos. ○ Resguardar la llave de la oficina donde se encuentra las carpetas en las que se archiva los documentos. • Integridad: ○ Cotejar la información original entregada por los servicios profesionales para su trámite. ○ Manejar de manera clara y objetiva la información que se requiera para los trámites de servicios profesionales. • Disponibilidad: ○ Mantener la información que sea necesaria al momento que se requiera a las personas autorizadas por el Jefe de la Unidad Administrativa.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personales.

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		documentos a la Dirección General de Personal. ○ Para el proceso de pago se captura en el sistema remoto de pagos de la Dirección General de Finanzas para el trámite del pago. • Resguardo: ○ Una vez que se libera el trámite se resguarda el documento con sello original de la Dirección General de Personal y se integra al expediente. ○ Se resguarda el recibo de la entrega de cheque.	

Inventario de Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: UA-03: PROVEEDORES

Datos personales (sensibles o no) contenidos en el sistema:	DATOS PERSONALES DE PROVEEDORES Constancia de situación fiscal del SAT. (Nombre/Razón social, RFC, Régimen, domicilio Fiscal, teléfono, correo electrónico). Caratula de Estado de Cuenta Bancaria. (Número de cuenta y clabe interbancaria)

Para que se usan los datos	Alta de proveedores de la UNAM, para el trámite de pago por medio de transferencia bancaria. Circulares y Lineamientos emitidos por el Patronato Universitario

¿Cómo se obtienen los datos personales?	☒ Físico	Fotocopias • Constancia de situación fiscal del SAT • Caratula de Estado de Cuenta Bancaria
	☒ Digital	Vía correo electrónico se recibe archivos en formato PDF • Constancia de situación fiscal del SAT • Caratula de Estado de Cuenta Bancaria

Temporalidad de obtención	Por evento

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
Recepción de documentos probatorios de proveedor vía correo electrónico y en fotocopias.	Se digitalizan los documentos recibidos en físico. Se capturan los datos personales y los bancarios en el sistema de proveedores UNAM, anexando los archivos electrónicos de formato PDF. Se archiva los documentos en un expediente.	A través del sistema de proveedores con la Dirección General de Contabilidad y la Dirección General de Finanzas de Pagos para su validación y autorización para la asignación del número de proveedor. A través del sistema de proveedores con el personal de las unidades administrativas de la UNAM.	No aplica

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién?	¿Para qué?
	☐ CVTT ☒ Áreas Universitarias ☐ Gobierno federal		Dirección General de Contabilidad Dirección General de Finanzas	Validación de datos personales y bancarios.

	☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro		

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Responsable de seguridad de datos personales:	Lic. Oscar Ramírez González
Cargo:	Jefe de la Unidad Administrativa
Funciones:	• Recaban, Supervisar que se tengas completa la información de los datos personales (Constancia de situación fiscal SAT, Caratula estado de cuenta bancaria) • Procesan, Supervisar que la captura de los datos personales este completa • Comparten, Supervisar la captura de datos y envió de archivos
Obligaciones:	• Confidencialidad, Supervisar el resguardo de la información en el expediente correspondiente • Integridad, Supervisar que no se difundan los datos personales para evitar el mal uso de ellos. • Disponibilidad, Verificar que no se permita el acceso a la información por otros

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
No aplica			

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Ramón Alvarez Rodríguez	Jefe de Departamento	• Recaban, solicitar los datos al proveedor para darlos de alta en el sistema • Procesan, capturar los datos personales y los bancarios en el sistema de proveedores UNAM, anexando en archivo electrónico de formato PDF. • Comparten, Captura de datos y envió de archivos.	• Confidencialidad, ○ Resguardar la información en el expediente correspondiente. ○ Resguardo de credenciales de acceso al Sistema de proveedores de la UNAM. • Integridad, No difundir los datos para evitar el mal uso de ellos. • Disponibilidad, No permitir el acceso a la información por otros
María del Mar Rubí Guerrero	Apoyo del área de presupuesto	• Recaban, solicitar los datos al proveedor para darlos de alta en el sistema • Digitalización de documentación entregada en físico. • Procesan, capturar los datos personales y los bancarios en el sistema de proveedores UNAM, anexando en archivo electrónico de formato PDF.	• Confidencialidad, Resguardar la información en el expediente correspondiente • Integridad, No difundir los datos para evitar el mal uso de ellos. • Disponibilidad, No permitir el acceso a la información por otros

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Involucrados del sistema de tratamiento de datos personale

Involucrados en las actividades de tratamiento [2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
		• Comparten, Captura de datos y envió de archivos.	

Anexo 2

Estructura y descripción de los sistemas de tratamiento de datos personales

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: CCPE-01: Actualización Directorio UNAM

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Sistema de Directorio UNAM	[redacted]

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

¿Cuál es el tratamiento de los datos?

Recaban	Procesan	Comparten	Suprimen
	En caso de los expedientes físicos, estos se encuentran en [redacted]		

¿Los datos se transfieren o comparten?	☒ Comparten ☐ Transfieren	☐ No	¿Con quién? 1. DJ de la CVTT.	¿Para qué? Para revisión, registros y firma de convenios de colaboración.
	☒ CVTT ☐ Áreas Universitarias ☐ Gobierno federal ☐ Gobierno local ☐ Personas físicas ☐ Personas morales ☐ Otro			

Responsable:	**Coordinación de Vinculación y Transferencia Tecnológica**
Nombre:	Mtra. María Isabel Mascorro Velarde
Cargo:	Directora de Transferencia de Tecnología
Funciones:	• Recabar información para identificar y promover proyectos universitarios y de personas que participan en convocatorias. • Procesar la información de proyectos universitarios para promoción con las empresas y de personas que participan en convocatorias. • Compartir información con personal adscrito a la CVTT.
Obligaciones:	• Confidencialidad: guardar la privacidad de los datos personales. • Integridad: asegurar la información mediante claves, contraseñas y barreras físicas. • Disponibilidad: tener disponible la información para la ejecución las labores en la CVTT.

Encargados[1]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
NO APLICA			

Involucrados en las actividades de tratamiento[2]			
Nombre	*Cargo*	*Funciones*	*Obligaciones*
Julio César Cosbert Vásquez	Coordinador de Transferencia de Tecnología de Proyectos para la Salud.	• Recabar la información específica de los proyectos que se tienen asignados.	• Utilizar de manera confidencial los datos personales recabados. • Integridad: elaborar las claves y contraseñas para resguardo

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.
[2] Se tienen que ingresar los datos de todos los Usuarios del sistema de tratamiento de datos personales.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: CCPE-03: Levantamiento y Proceso de Multimedia

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Almacenamiento digital en dos computadoras para su uso inmediato.	[redacted]
Digital	Redes sociales administradas por los responsables designados de la CCPE	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

		[redacted]
Digital	Unidad de disco externa con respaldo de información, material audiovisual y documentos de años previos.	
Digital	Almacenamiento interno en servidores de la CVTT, contiene un respaldo de material audiovisual obtenido en años anteriores por distintos colaboradores.	

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU–01: Talleres de Emprendimiento

Soportes		
Tipo de soporte	*Descripción*	*Características*
Digital	Hoja de cálculo almacenada en el Google Drive de la cuenta de laboratorio.innovaunam@gmail.com	[redacted]
Digital	Documento de hoja de cálculo almacenada en el Repositorio Institucional de la CVTT en la cuenta CLAUDIA PALANCARES.	
Digital	Documento de hoja de cálculo almacenada en quipo de cómputo de colaboradores de la DEU.	

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU–02: INNOVAUNAM

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	Expedientes de proyectos empresariales.	[redacted]
Digital	Solicitudes de proyectos empresariales.	
Digital	Solicitudes de proyectos empresariales.	
Digital	Actas de los Comités de evaluación y selección de proyectos para ingresar al programa de incubación en el Sistema InnovaUNAM	
Digital	Expedientes de proyectos empresariales.	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Capacitaciones para emprendedores e incubadoras del Sistema InnovaUNAM	[redacted]
Digital	Comunicación general con la comunidad del Sistema InnovaUNAM.	
Digital	Comunicación general con la comunidad del Sistema InnovaUNAM.	
Digital	Expedientes de proyectos empresariales.	
Digital	Respaldo de videoconferencias y archivos.	

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU–03: Incubación de Base Tecnológica.

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Plataforma de registro para la incubación en el Sistema InnovaUNAM.	[redacted]
Digital	Expedientes para convenios de incubación recibidos por correo electrónico.	
Digital	Expediente digital de "Expedientes de incubación". • Expedientes digitales de incubación que incluye documentos personales como: Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, e imagen de credencial de alumno o trabajador e Identificación oficial.	
Digital	Expediente digital de "Expedientes de incubación". • Expedientes digitales de incubación que incluye documentos personales como: Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, e imagen de credencial de alumno o trabajador e Identificación oficial.	
Físico	Expediente físico de "Expedientes de incubación".	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
	• Expedientes físicos de incubación que incluye documentos personales como: Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, e imagen de credencial de alumno o trabajador e Identificación oficial.	[redacted]
Digital	Grabaciones de videoconferencias de capacitación o sesiones de seguimiento	

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-04: Incubación de Empresas Sociales

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Plataforma de registro para la incubación en el Sistema InnovaUNAM.	[redacted]
Digital	Expedientes para convenios de incubación recibidos por correo electrónico.	
Digital	Expediente digital de "Expedientes de incubación". • Expedientes digitales de incubación que incluye documentos personales como: Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, e imagen de credencial de alumno o trabajador e Identificación oficial.	
Digital	Expediente digital de "Expedientes de incubación". • Expedientes digitales de incubación que incluye documentos personales como: Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, e imagen de credencial de alumno o trabajador e Identificación oficial.	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Físico	Expediente físico de “Expedientes de incubación”. • Expedientes físicos de incubación que incluye documentos personales como: Nombre completo, teléfono fijo, teléfono celular, correo electrónico, número de cuenta o de trabajador, CURP, RFC, e imagen de credencial de alumno o trabajador e Identificación oficial.	[redacted]
Digital	Grabaciones de videoconferencias de capacitación o sesiones de seguimiento	

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-05: Guías para el emprendimiento profesional

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Hoja de cálculo Excel Presentación de Power Point	[redacted]
Digital	Página Web de las Guías para el emprendimiento profesional.	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DEU-06: EMPRENDE CON SANTANDER X Y LA UNAM

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Plataforma de registro a los cursos	[redacted]
Digital	Plataforma de mesa de ayuda	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD–01: Soporte TIC

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	No aplica	[redacted]
Digital	Hoja de cálculo: CVTT-Inventario-2022.xlsx.	
Digital	Plataforma de Gestión de servicios GLPI.	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD–02: Directorio CVTT

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	No aplica	[redacted]
Digital	Hoja de cálculo: Directorio_CVTT_2022.xlsx	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-03: VIDEOCONFERENCIA

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	No aplica	[redacted]
Digital	Sitio web de la plataforma de videoconferencia	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD–04: COGNOS UNAM

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Cognos UNAM	[redacted]
Digital	Correo electrónico	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-05: Gestión convocatorias CVTT

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Plataforma para postulación de Proyecto.	[redacted]
Digital	Plataforma de evaluación de proyectos	
Digital	Nube de la CVTT	
Digital	Plataforma de mesa de ayuda	
Digital	Plataforma de Sello Digital Universitario	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
		[redacted]
Digital	Servicio de respaldo de la CVTT	

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD–06: PLATAFORMA DE REGISTRO DE INFORMACIÓN Y NOTIFICACIÓN DE INFORMACIÓN DE LA CVTT

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Plataforma de registro de información y notificación de información de la CVTT.	[redacted]

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DITD-07: Gestión de Convocatorias Consorcio UNAM TEC

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Plataforma para postulación de Proyecto.	[redacted]
Digital	Plataforma de evaluación de proyectos	
Digital	Nube de la CVTT	
Digital	Plataforma de mesa de ayuda	
Digital	Plataforma de Sello Digital Universitario	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
		[redacted]
Digital	Correo electrónico	
Digital	Servicio de respaldo de la CVTT	

Estructura y Descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DJ-01: Instrumentos Consensuales

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	Expedientes de instrumentos consensuales en los que la Universidad es parte	[redacted]
Digital	Copias de instrumentos consensuales en los que la Universidad es parte	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: DIRECCIÓN DE SERVICIOS TECNOLÓGICOS

ID: DST-01: Vinculación Interna

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Datos personales de los responsables de vinculación de cada entidad y dependencia universitaria que se encuentran en una base de datos en Excel, bajo el nombre de *DIRECTORIO VINCULADORES UNIVERSITARIOS.*	[redacted]

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: DIRECCIÓN DE SERVICIOS TECNOLÓGICOS

ID: DST–02: Vinculación Externa

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Datos personales proporcionados por el usuario en el formato de solicitud de servicios.	[redacted]

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DTT-01: Proceso Transferencia Tecnológica

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Base de datos [redacted]	[redacted]
Digital	Directorio de trabajo, [redacted]	
Físico	Expedientes de cada una de las tecnologías, [redacted]	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DTT-02: PI

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	Expedientes incluidos en carpetas. [redacted]	[redacted]
Digital	Expedientes electrónicos de todos los expedientes de nuevas solicitudes.	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

		[redacted]

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: DTT-03: Contactos DTT

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Digital	Base de datos [redacted]	[redacted]

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: UA-01: Personal de estructura

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	Expedientes con copia de los documentos del personal dado de alta por estructura en la dependencia.	[redacted]
Digital	Sistema Integral de Personal (SIP)	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

ID: UA-02: Servicios profesionales

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	Expedientes de contrataciones por servicios profesionales	[redacted]
Digital	Módulo de honorarios	
Digital	Sistema Remoto de Pagos	
Digital	Equipo de cómputo de Jefe de Personal	
Digital	Correo electrónico de Jefe de Personal [redacted]	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Estructura y descripción de los Sistemas de Tratamiento de Datos Personales

RESPONSABLE: COORDINACIÓN DE VINCULACIÓN Y TRANSFERENCIA TECNOLÓGICA

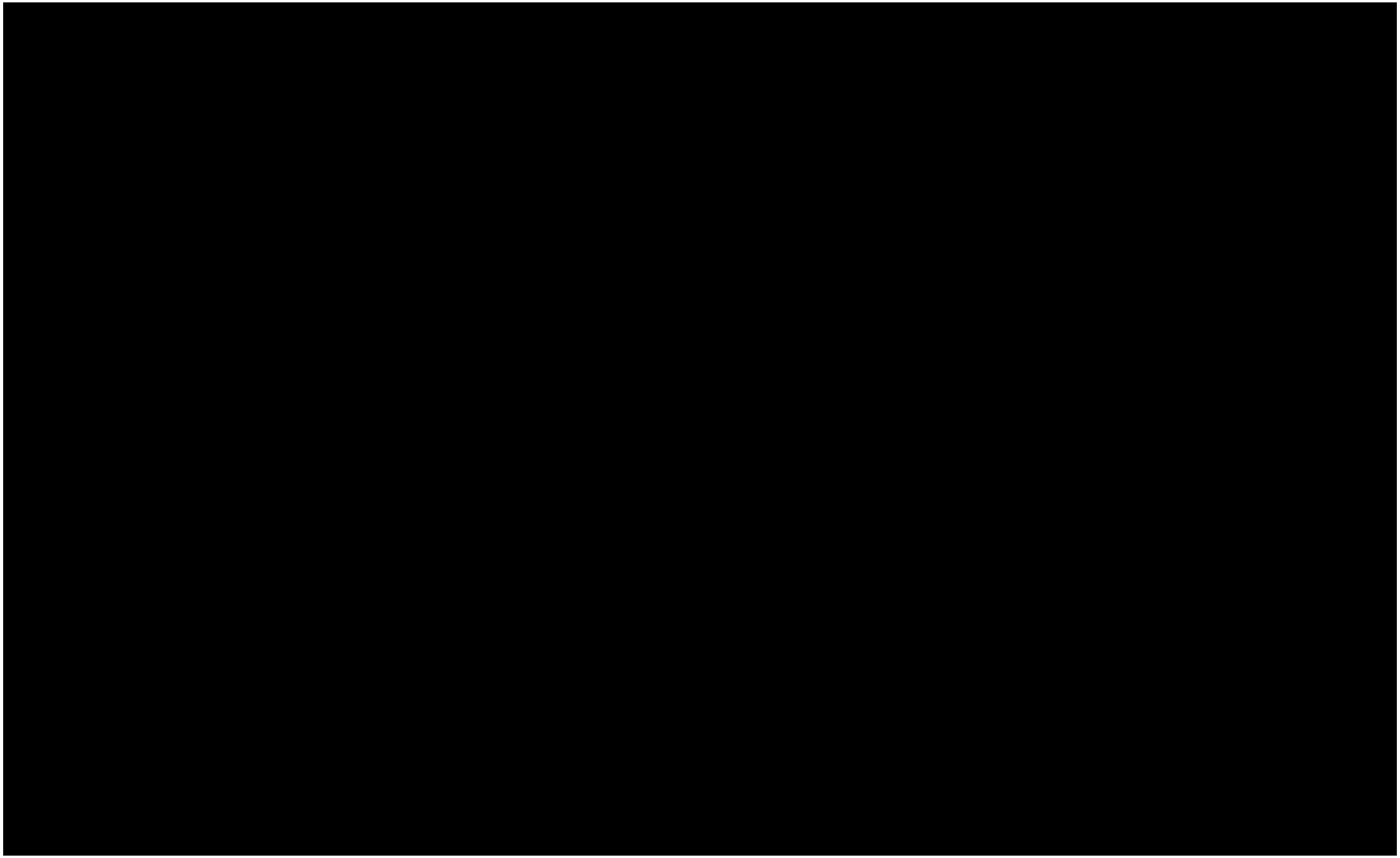
ID: UA-03: Proveedores

Soportes[1]		
Tipo de soporte	*Descripción*	*Características*
Físico	Los datos se encuentran en Expedientes por proveedor	[redacted]
Digital	Sistema de Proveedores	

[1] En caso de que el sistema de tratamiento de datos personales ocupe varios soportes, deberá presentar las descripciones correspondientes a cada uno de ellos.

Anexo 3

Diagramas de arquitectura

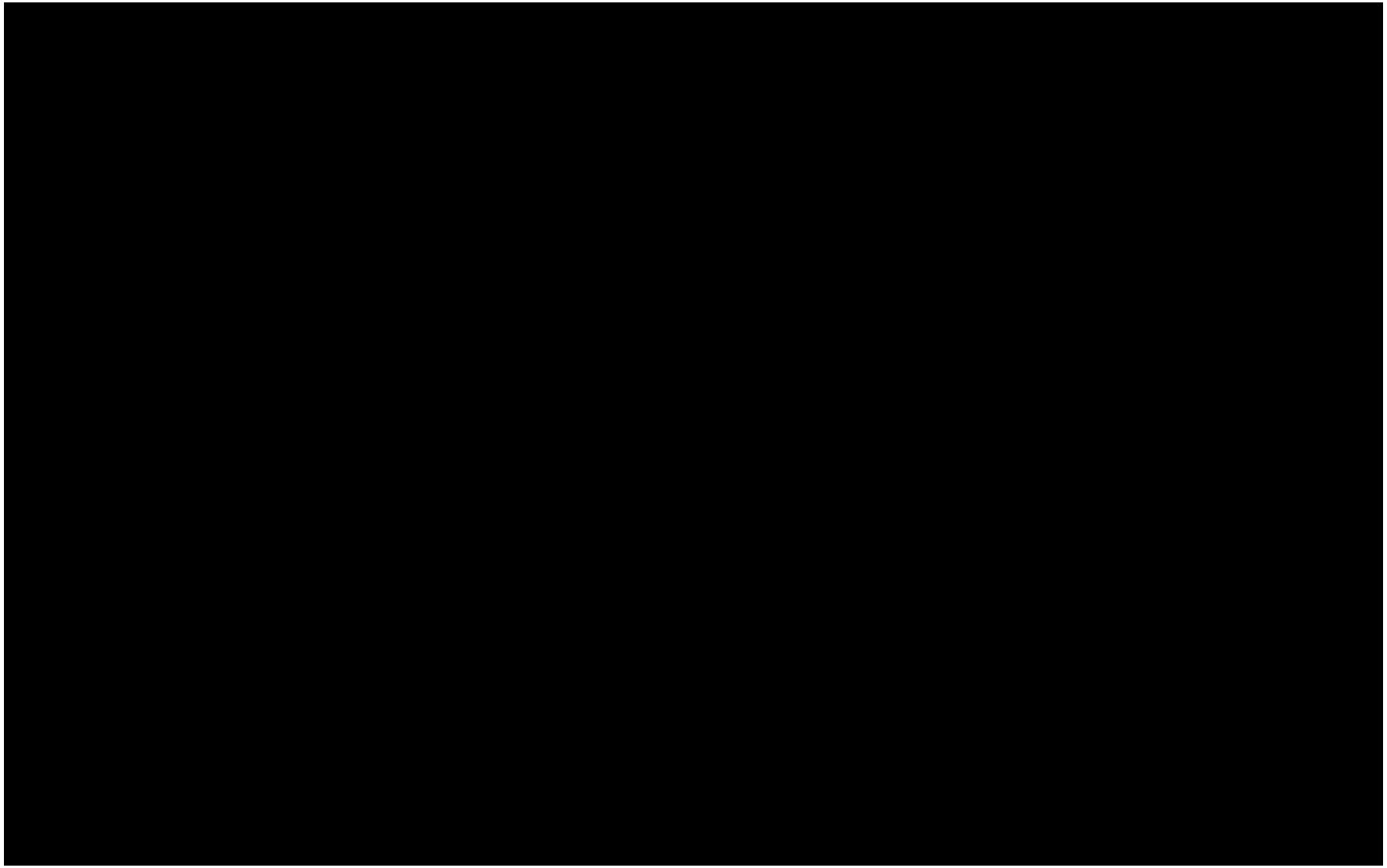


TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE DIAGRAMAS DE ARQUITECTURA YA QUE CONTIENE EL FLUJO DE INFORMACIÓN ENTRE LOS COMPONENTES, SUS RUTAS DE ACCESO A SOPORTES DIGITALES Y DESCRIBE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

Anexo 4

Metodología de análisis de riesgo y análisis de brecha

Metodología de Análisis de Riesgo
BAA

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Junio 2015

Contenido

Notas de versiones

- Versión Junio 2015. Respecto a la versión anterior (Marzo 2014), se actualizó el nombre, logotipo y sigla del Instituto, debido al cambio de naturaleza jurídica del antes Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), por el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Nota Previa

En el marco de la emisión de las Recomendaciones en materia de Seguridad de Datos Personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto) pone a consideración de los interesados, investigadores y expertos en materia de seguridad de la información, la metodología que se desarrolla en el presente documento, a fin de recibir sus comentarios y observaciones respecto de la utilidad que tendría la misma para llevar a cabo el análisis de riesgos en el entorno del tratamiento de datos personales, así como la selección de controles de seguridad a aplicar.

Es importante señalar que esta metodología **no forma parte integral del documento de Recomendaciones en materia de Seguridad de los Datos Personales**, pues primero, es importante para el INAI, y de su especial interés, recibir las opiniones respectivas sobre la viabilidad de esta metodología, la cual fue desarrollada a petición del Instituto.

En ese sentido, la siguiente metodología de análisis de riesgo puede ser valorada por investigadores, expertos e interesados en la materia, para proponer mejoras e incluso nuevos modelos con base en los elementos que se presentan en este documento. Se considera que es una propuesta alternativa a otras metodologías basadas en los estándares y mejores prácticas referidos en las Recomendaciones en materia de Seguridad de los Datos Personales, y en ese sentido, el cumplimiento del deber de seguridad que establece el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP o Ley) dependerá de que los responsables y encargados implementen adecuadamente y mantengan a través del tiempo, los controles de seguridad necesarios para la protección de los datos personales que estén en su posesión.

Metodología de Análisis de Riesgo BAA

1. Introducción

Un acercamiento para evaluar las medidas de seguridad necesarias para proteger los activos de información es a través del análisis de riesgo, de modo que se pueda determinar cuál riesgo es más importante mitigar o cuáles activos se encuentran más expuestos.

La metodología de análisis de riesgos que se presenta en este documento se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

1) **Beneficio para el atacante.** Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).
2) **Accesibilidad para el atacante.** Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero).
3) **Anonimidad del atacante.** Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente a las instalaciones de una empresa).

A partir de lo anterior, se ha dado el nombre de "BAA" a esta metodología de análisis de riesgos, lo cual tiene su origen en el **B**eneficio para el atacante, la **A**ccesibilidad para el atacante y la **A**nonimidad del atacante.

El objetivo de la metodología es realizar una clasificación de los datos personales en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección.

2. Identificación y clasificación de datos personales

Se deben identificar los **tipos de datos personales**, la **sensibilidad de los mismos** y el **número de personas** de quienes se tratan dichos datos para determinar el valor que representan para un atacante.

2.1 Clasificación de datos personales

El responsable debe identificar los tipos de datos personales que se tratan, la sensibilidad de los mismos y el número de titulares para determinar el valor de riesgo inherente de los datos para un tercero no autorizado.

Los datos personales pueden clasificarse en cuatro categorías, de acuerdo a la criticidad de los mismos por nivel de riesgo inherente:

Datos con riesgo inherente bajo
Esta categoría considera información general concerniente a una persona física identificada o identificable, que no corresponda a la información a la que refieren las otras tres categorías, como por ejemplo datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, entre otra información que no refiera a las siguientes tres categorías.

Datos con riesgo inherente medio
Esta categoría contempla los datos que permiten conocer la *ubicación física* de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.

También son datos de riesgo inherente medio aquéllos que permitan inferir el *patrimonio* de una persona*,* que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el *número de tarjeta bancaria de crédito* y*/o débito.*

Son considerados también, los datos de *autenticación* con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos *jurídicos* tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Datos con riesgo inherente alto
Esta categoría de datos contempla a los datos personales sensibles, que de acuerdo a la Ley incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Datos con riesgo inherente reforzado
Los datos de *mayor riesgo* son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o

contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las *personas de alto riesgo* son aquéllas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante. Por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público. Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional. Tratar datos de *personas de alto riesgo* involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros.

Es importante señalar que las categorías antes descritas se desarrollaron exclusivamente para la aplicación de esta metodología, y no pueden ser consideradas como un criterio emitido por el INAI. Más aún, el Pleno del Instituto no ha emitido criterios institucionales al respecto, además de que ciertos datos personales que en principio no se consideran sensibles, podrían llegar a serlo dependiendo del contexto en que se trata la información.

2.2 Identificación de tipos de datos y de nivel de riesgo inherente

De acuerdo al punto anterior, se deberá identificar qué *tipos de datos personales* se están tratando y cuál es el *nivel de riesgo inherente* de los mismos (bajo, medio, alto, reforzado). En la Tabla 1 se presenta un ejemplo de esta identificación:

Tipo de Dato	Nivel de Riesgo Inherente
Ubicación en conjunto con patrimoniales	REFORZADO
Información adicional de tarjeta bancaria	REFORZADO
Titulares de alto riesgo	REFORZADO
Salud	ALTO
Origen, creencias e ideológicos	ALTO
Ubicación	MEDIO
Patrimoniales	MEDIO
Autenticación	MEDIO
Jurídicos	MEDIO
Tarjeta Bancaria	MEDIO
Personales de identificación	BAJO

Tabla 1. Nivel de riesgo inherente

El responsable o encargado deberá documentar los tipos de datos que tiene en tratamiento y su riesgo inherente, para uso en las siguientes secciones de la metodología. Se debe incluir todos los tipos de datos que se tiene en tratamiento.

3. Análisis de riesgos de datos personales

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

Esta metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales (Figura 1):

- **Beneficio**, **factor** que deriva en el nivel de **riesgo por tipo de dato**, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- **Accesibilidad**, **factor** que determina el nivel de **riesgo por tipo de acceso**, es decir, el número de accesos potenciales a los datos.
- **Anonimidad**, **factor** que determina el nivel de **riesgo por tipo de entorno** desde el que se tiene acceso a los datos.

Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

En la siguiente imagen se ilustra el procedimiento de obtención del valor de riesgo latente para los particulares:

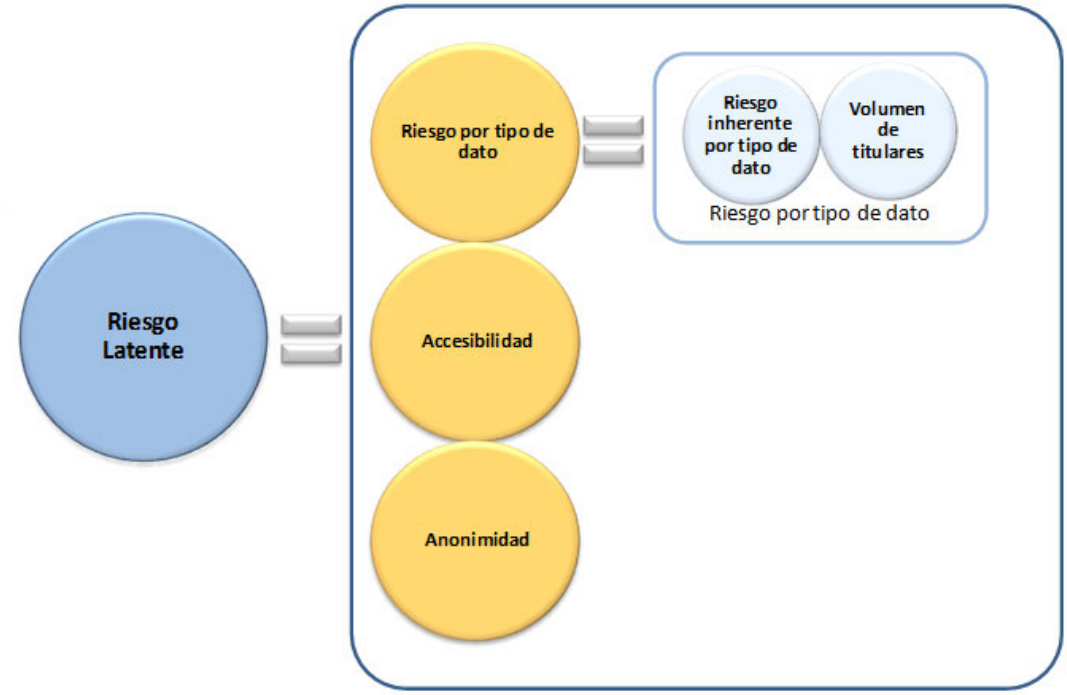


Figura 1. Cálculo de riesgo latente

3.1 Identificación de riesgo por tipo de dato

El nivel de riesgo por tipo de dato es igual al **beneficio** que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

1. Tener el nivel de *riesgo inherente de cada tipo de dato* que se trate, y;
2. Calcular el *volumen de titulares*, cuantificando el número de personas de las que se traten datos personales.

Figura 2. Identificación de riesgo por tipo de dato

El nivel de *riesgo inherente de cada tipo de dato* se determina de acuerdo a la sección **2. Identificación y clasificación de datos personales.** Mientras que el *volumen de titulares* se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

<500: Datos de hasta 500 personas
<5k: Datos entre 501 hasta 5,000 personas
<50k: Datos entre 5,001 hasta 50,000 personas
<500k: Datos entre 50,001 hasta 500,000 personas
>500k: Datos de más de 500,000 personas

Es importante que para llevar a cabo la cuantificación de titulares se consideren tanto los soportes físicos, como los electrónicos.

Se debe seleccionar uno de los rangos anteriores según el tipo de dato y su nivel de riesgo inherente, por ejemplo:

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares
Patrimoniales	**Medio**	**<50k**

3.1.1 Identificación del nivel de riesgo por tipo de dato

Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se podrá identificar el nivel de *riesgo por tipo de dato* que se trata en la organización. Se han establecido cinco niveles posibles (Figura 3) nombrados con valor numérico del 1 al 5, tal como se muestra en la siguiente imagen, donde **1** es el nivel **más bajo** y **5** el **más alto**:

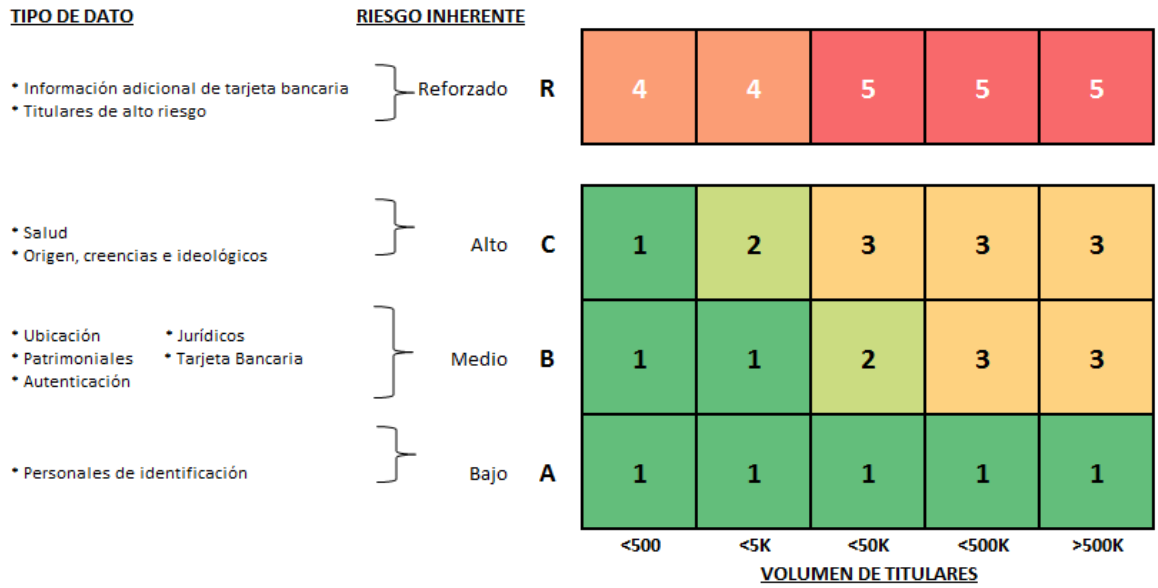


Figura 3. Nivel de riesgo por tipo de dato

A continuación se detallan los niveles mencionados:

Riesgo por tipo de dato **Nivel 1**[1], ocurre cuando:

- El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas
- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas
- El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas

Riesgo por tipo de dato **Nivel 2**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas
- El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas

Riesgo por tipo de dato **Nivel 3**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante
- El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante

Riesgo por tipo de dato **Nivel 4**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas

Riesgo por tipo de dato **Nivel 5**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

[1] Ver sección Cuestionario de Autoevaluación, en la que se explica cómo identificar fácilmente si es nivel de riesgo por tipo de dato 1.

En la Tabla 2 se muestra una relación del tipo de datos con el nivel de riesgo correspondiente.

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<5k	<50k	<500k	>500k
Ubicación en conjunto con patrimoniales	REFORZADO	4	4	5	5	5
Información adicional de tarjeta bancaria	REFORZADO	4	4	5	5	5
Titulares de alto riesgo	REFORZADO	4	4	5	5	5
Salud	ALTO	1	2	3	3	3
Origen, creencias e ideológicos	ALTO	1	2	3	3	3
Ubicación	MEDIO	1	1	2	3	3
Patrimoniales	MEDIO	1	1	2	3	3
Autenticación	MEDIO	1	1	2	3	3
Jurídicos	MEDIO	1	1	2	3	3
Tarjeta Bancaria	MEDIO	1	1	2	3	3
Personales de identificación	BAJO	1	1	1	1	1

Tabla 2. Nivel de riesgo por tipo de dato

Este nivel de riesgo servirá para determinar los controles que debe considerar el responsable para la protección de datos personales, que se describen en la sección relativa a la identificación de medidas de seguridad.

3.2 Cuestionario de autoevaluación

Con el objetivo de facilitar el desarrollo e implementación de la metodología para aquellos particulares cuyo nivel de riesgo sea bajo, se ha desarrollado un cuestionario de autoevaluación que permitirá efectuar un auto diagnóstico para determinar si tiene un nivel de riesgo por tipo de dato 1, el nivel de riesgo más bajo y siendo éste el caso, realizar los siguientes pasos de la metodología, con un enfoque abreviado.

Para identificar si se tiene nivel de riesgo por tipo de dato 1, se debe responder los siguientes cuestionamientos:

Los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita identificar la ubicación del titular.

1. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

○ SI ○ NO

Los datos que permiten inferir el patrimonio del titular, que incluyen entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados.

2. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos de autenticación son información referente a los usuarios y contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, copia de identificaciones oficiales y cualquier otro que permita autenticar al titular.

3. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos dentro de los expedientes jurídicos, penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido de forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

4. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

El número de tarjeta bancaria o de crédito conformado por los 15 o 16 dígitos únicos de la tarjeta de crédito y/o débito.

5. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

De acuerdo a la LFPDPPP, los datos sensibles incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasada, presente o futura; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular. Para efectos del presente documento los datos sensibles serán considerados datos de alto riesgo.

6. ¿De los datos sensibles descritos en este punto; obtiene, usa, divulga o almacena datos de más de 500 personas?

SI NO

Los datos *reforzados* son los que de acuerdo a su naturaleza tienen un nivel superior de riesgo, derivado del beneficio económico o reputacional que pueda representar para un tercero. A continuación se listan los datos de mayor riesgo:

De ubicación en conjunto con patrimoniales: Aquéllos que relacionen datos patrimoniales con ubicación física del titular.

Información adicional de tarjeta bancaria: el número tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, código de seguridad (CVV, CVV2, CAV2, CVC2, CID), datos de banda magnética o número de identificación personal (PIN).

7. ¿Obtiene, usa, divulga o almacena datos correspondientes a los descritos en este punto?

SI NO

Los *titulares de alto riesgo* son las personas que debido a su oficio, profesión o naturaleza están expuestos a una mayor probabilidad de ser atacados debido al beneficio económico o reputacional que sus datos pueden representar para un tercero. Por lo tanto, el tener datos de estos titulares eleva el riesgo de la información de la base de datos completa y en consecuencia para todas las personas contenidas en ella. Los titulares de alto riesgo incluyen líderes políticos, religiosos, empresariales, de opinión, de impartición de justicia, responsables de seguridad nacional y cualquier otra persona que sea considerada como personaje público.

8. ¿Obtiene, usa, divulga o almacena datos de titulares de alto riesgo?

SI NO

Si todas las respuestas a las preguntas anteriores fueron “NO”, entonces los controles de seguridad que deberá implantar en los sistemas que traten, procesen o guarden datos personales, corresponden al **nivel mínimo requerido,** y deberá implantar la lista básica de medidas de seguridad (Lista 1). Esto mismo lo puede corroborar siguiendo los pasos de la metodología simple.

En el **ANEXO A** *Mecanismo de autoevaluación* se encuentra contenido el cuestionario de autoevaluación y algunos pasos acotados para el nivel de riesgo por tipo de dato 1.

Si al menos una de las respuestas fue “SÍ”, deberá implantar medidas de controles de seguridad mayores al nivel mínimo y continuar con las secciones siguientes de este documento.

3.3 Identificación de nivel de accesibilidad

Una vez obtenido el factor **Beneficio**, es decir el nivel de *riesgo por tipo de dato*, es necesario identificar el nivel de *riesgo por tipo de acceso*, (Tabla 3). Se realiza determinando la cantidad de accesos potenciales a los datos personales que se pretende proteger, es decir, definiendo cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro, entre mayor sea la accesibilidad, mayor riesgo existe para la información.

Accesibilidad (Cantidad de accesos a los datos personales)
≤ 20
> 20 ≤ 200
> 200 ≤ 2,000
> 2,000

Tabla 3. Umbrales de nivel de accesibilidad

3.4 Identificación de nivel de anonimidad

Después de obtener el factor **Accesibilidad**, se debe identificar qué tan anónimos son los accesos a la información; es decir, el nivel de *riesgo por tipo de entorno*. Este factor representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la organización, en caso de acceder o hacer uso no autorizado de los datos personales que se tratan.

En la siguiente tabla se listan los entornos de acceso en una escala del 1 al 5, en donde **1** implica **baja anonimidad** y **5 mayor anonimidad** del atacante, es decir, entre más anónimo pueda ser un atacante, mayor confianza obtiene para intentar vulnerar la seguridad.

Entorno	Nivel de Anonimidad
Físico	1
Red interna	2
Red inalámbrica	3
Red de terceros	4
Internet	5

Tabla 4. Nivel de anonimidad

Se deberá seleccionar el nivel aplicable para cada tipo de dato en tratamiento. En caso de que los datos se accedan desde más de un entorno, se deberá considerar el entorno de mayor riesgo por cada tipo de dato. Esto se utilizará en la sección Identificación de Medidas de Seguridad.

A continuación (Figura 4) se presenta un esquema de los entornos digitales:

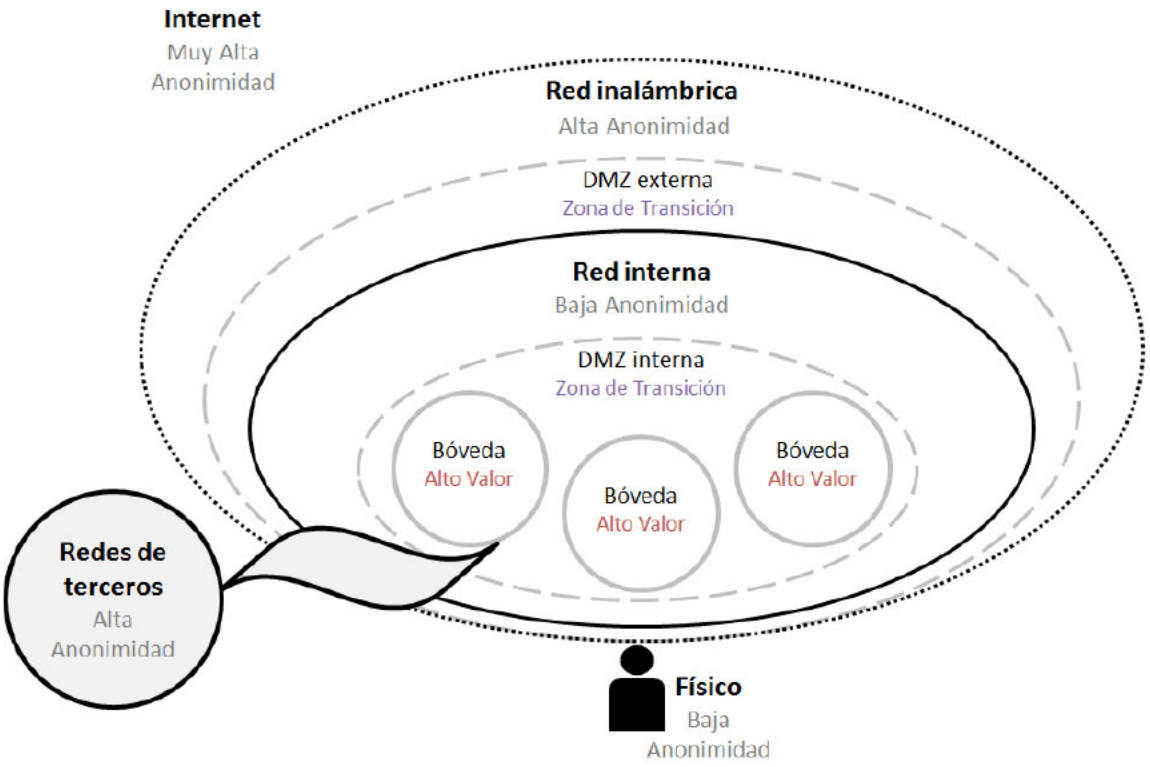


Figura 4. Entornos de acceso

3.5 Identificación de nivel de riesgo latente

La combinación de los tres factores analizados; nivel de *riesgo por tipo de dato* (**beneficio**), nivel de *riesgo por tipo de acceso* (**accesibilidad**) y nivel de *riesgo por tipo de entorno* (**anonimidad**), da como resultado el nivel de **riesgo latente** que presenta cada organización (Figura 5).

Figura 5. Nivel de riesgo latente

4. Identificación de medidas de seguridad

Una vez obtenido el nivel que le corresponde a cada factor de riesgo, se deben identificar las medidas de seguridad aplicables a la organización. Para ello, se desarrollaron cinco tablas matriciales que combinan el nivel de riesgo por tipo de dato, el nivel de accesibilidad y el nivel de anonimidad, dando como resultado un patrón de control o lista de controles a implantar.
Se han definido listas y patrones de control que agrupan medidas de seguridad basadas en ISO/IEC 27002:

- **Listas de controles.** Utilizaremos este término para describir la situación en la que no es imperante implantar todos los controles sugeridos, sino que existirán medidas necesarias y medidas opcionales para que el responsable de seguridad seleccione aquéllas que, sumadas, apoyan a la mitigación del riesgo existente en el contexto de su organización. Es decir, en el caso de las listas, la suma de controles contribuye a la protección de la información, teniendo la posibilidad de seleccionar uno a más controles.
  Existen listas de controles administrativos, de seguridad física y del entorno de red interna.

- **Patrones de control.** Utilizaremos este término para describir la situación en la que, de acuerdo a la situación de riesgo identificada, es necesario implantar en su totalidad los controles descritos dentro del mismo. Los patrones de control existentes son: Controles Básicos, DMZ y Caja Fuerte (entorno recomendado para resguardar información con nivel de riesgo por tipo de dato 4 y 5). Sólo se podrá descartar alguna medida de seguridad en el caso de que no sea aplicable a su infraestructura, por ejemplo, un control enfocado a comercio electrónico se podrá descartar sólo si la organización no cuenta con dicha actividad.

Como se mencionó al inicio de la sección se cuenta con cinco tablas, cada tabla corresponde a un nivel de riesgo por tipo de dato (1 al 5); dentro de las tablas, en las filas se encuentra mapeado matricialmente el nivel de anonimidad (representado por el entorno de acceso a los datos), y en las columnas el nivel de accesibilidad (representado por el número de personas o accesos a los datos). En las celdas de dichas tablas se encuentran distribuidos los patrones de control y las listas de medidas de seguridad a implantar. Asimismo, para el nivel de riesgo por tipo de dato “1”, se definió un conjunto de medidas básicas de seguridad que aplica a todas las combinaciones de anonimidad y accesibilidad, estas medidas de seguridad son las mínimas necesarias y no contempla controles opcionales; esto no exime al responsable o encargado de implementar más controles si fuera necesario.

Se han definido tres tipos de patrones y tres tipos de listas, cada uno de ellos con niveles que atienden a diferentes combinaciones de riesgo.

Patrones de control:

1. CB: Patrón de control de medidas de seguridad básicas. Es aplicable para aquellos particulares cuyo nivel de riesgo por tipo de dato es igual a 1.

2. DMZ: Patrón para accesos desde entornos de alta anonimidad. Hace referencia a la necesidad de implementar una zona desmilitarizada como zona de transición entre un

entorno de mayor riesgo y uno de menor riesgo. Se contemplan dos niveles de este patrón.

   a. DMZ 2. Patrón de control de medidas intermedias de seguridad para accesos desde entornos de alta anonimidad.
   b. DMZ 3. Patrón de control de medidas reforzadas de seguridad para accesos desde entornos de alta anonimidad.

3. CF: Patrón aplicable para datos de nivel 4 y 5 de riesgo por tipo de dato. Su nombre hace referencia a las iniciales de Caja Fuerte, debido a que se recomienda que estos tipos de datos se aíslen y se protejan con medidas de seguridad mucho más estrictas y se construya una "caja fuerte" alrededor de ellos, para protegerlos de accesos no autorizados. Se contemplan dos niveles para este patrón.
   a. CF 1. Patrón de control de medidas de seguridad para caja fuerte nivel 1.
   b. CF 2. Patrón de control de medidas de seguridad para caja fuerte nivel 2.

Listas de medidas de seguridad:

1. AD: Lista de medidas administrativas. Esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista.
   a. AD-2. Medidas administrativas para nivel de riesgo por tipo de dato 2.
   b. AD-3. Medidas administrativas para nivel de riesgo por tipo de dato 3.
   c. AD-4-5. Medidas administrativas para nivel de riesgo por tipo de dato 4 o 5.

2. RI: Lista de medidas de seguridad aplicable para accesos desde la red interna. Esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su red interna. Se cuenta con tres niveles para esta lista; se debe considerar que la suma de controles contribuye a la disminución del riesgo que puede presentarse en la red.
   a. RI 1. Medidas básicas de seguridad para accesos desde red interna.
   b. RI 2. Medidas intermedias de seguridad para accesos desde red interna.
   c. RI 3. Medidas reforzadas de seguridad para accesos desde red interna.

3. F: Lista de medidas de seguridad aplicable para accesos desde el entorno físico. Esta lista contiene controles de seguridad física necesarios y opcionales. Se cuenta con tres niveles para esta lista.
   a. FI 1. Medidas básicas de seguridad para accesos físicos.
   b. FI 2. Medidas intermedias de seguridad para accesos físicos.
   c. FI 3. Medidas reforzadas de seguridad para accesos físicos.

En el Anexo B: Medidas de Seguridad, se encuentran las listas y patrones de control propuestos.

4.1 Tablas de control

A continuación se muestran las cinco tablas mencionadas:

Tabla 1: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 1. Para todas las combinaciones de esta tabla le corresponde el patrón de control de medidas básicas de seguridad (CB), mismo que deberá aplicarse en su totalidad.

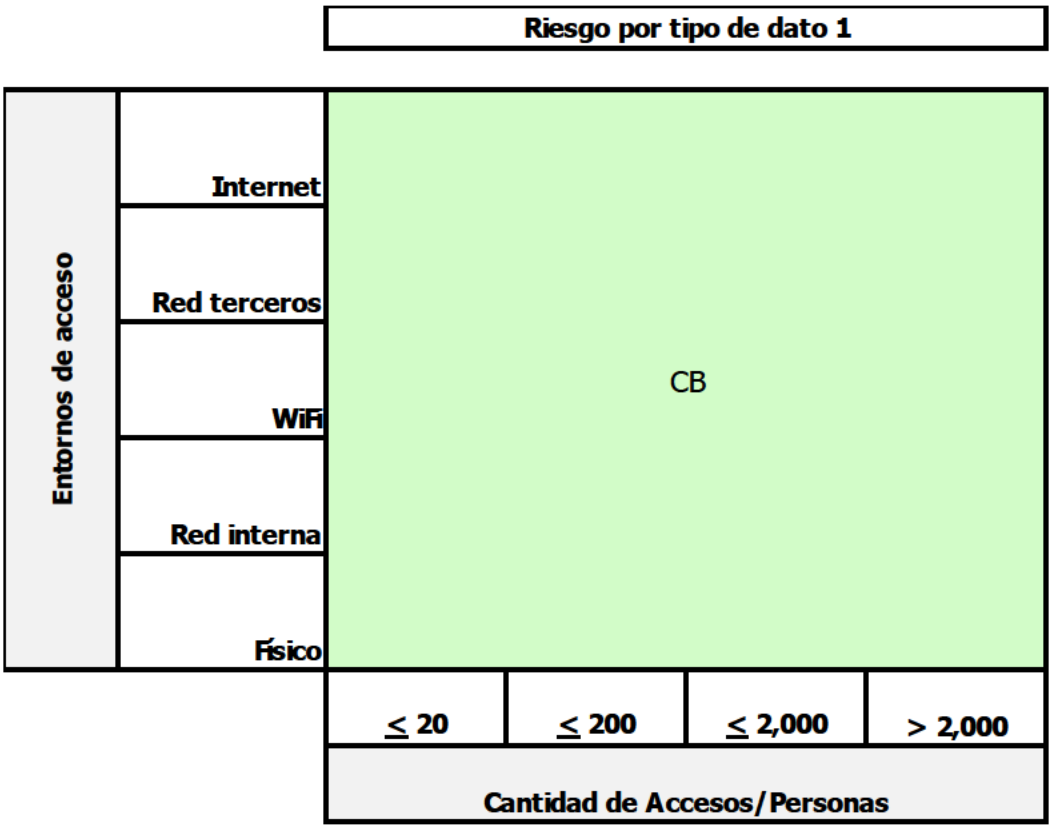


Tabla de control 1. Riesgo por tipo de dato 1

Tabla 2: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 2.

		Riesgo por tipo de dato 2			
		Medidas administrativas aplicables: AD-2			
Entornos de acceso	**Internet**	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red terceros	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	WiFi	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red interna	RI-1 F-1	RI-1 F-1	RI-2 F-2	RI-2 F-2
	Físico	F-1	F-1	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de control 2. Riesgo por tipo de dato 2

Tabla 3: Es la tabla que deberán utilizar los particulares cuyo nivel de riesgo por tipo de dato es 3.

		Med		AD-3	
En o nos de acceso	**nte ne**	RI 2 -2 DMZ-	RI -2	DMZ-	R -3 -2 DM -3
	Red e ce o	RI 2 -2 DMZ-	RI 3 -2 DMZ-	RI-3 -2 DMZ-	R -3 -2 DM -3
	WiF	RI 2 -2 DMZ-	RI 3 -2 DMZ-	RI-3 -2 DMZ-	R -3 -2 DM -3
	Red inte n	RI-2 -2	R -3 -2	R -3 2	R -3 2
	Físic	2	2	2	2
		__ 20	**__ 200**	**__ 2,000**	**> 2,000**
		C ntidad de Ac esos/Pe sonas			

Tabla de control 3. Riesgo por tipo de dato 3

Tabla 4: es la tabla que deberán utilizar los particulares cuyo nivel de riesgo por tipo de dato es 4.

		R o 4			
		M did s dm n s l cab es: AD 4-5			
Ento no de ac e o	Inte net				
	Red ter eros				
	WiF				
	Red in erna	3 C 1	3 C 1	3 C 1	-3 C -2
	Fs co	-3	3	3	3
		_ 20	_ 200	_ 2 000	> 2 000
		Cant dad de Accesos Personas			

Tabla de control 4. Riesgo por tipo de dato 4

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos contra entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, internet o redes inalámbricas.

Tabla 5: Es la tabla que deberán utilizar los particulares cuyo nivel de riesgo por tipo de dato es 5.

		Re o 5			
		Med das admi i i ab es: AD-4 5			
Ento no de ac e o	nterne				
	Red ercero				
	W F				
	Red nte na	-3 C -1	-3 C 2	-3 C 2	-3 C 2
	Fsi o	3	3	3	3
		_ 20	_ 200	_ 2,000	> 2,000
		Cant dad de A cesos Personas			

Tabla de control 5. Riesgo por tipo de dato 5

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos vs. entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, internet o redes inalámbricas.

4.2 Procedimiento de selección de medidas de seguridad

A continuación se describe el procedimiento para identificar la lista de medidas de seguridad o patrón de control a implantar, tomando como base el nivel de riesgo que se obtuvo en la sección "Análisis de riesgos de los datos personales".

Para el uso de las tablas se deben realizar los siguientes pasos:

1. De acuerdo con el nivel de riesgo por tipo de dato, identificar la tabla que le corresponde. Si se obtuvo riesgo por tipo de dato igual a 1, independientemente del entorno de acceso y el número de accesos que se tengan, le corresponde implementar el patrón de control de medidas básicas de seguridad. Si obtuvo un nivel de riesgo por tipo de dato mayor a 1 continuar con los siguientes pasos.
2. Seleccionar la fila con el entorno de accesos a los datos personales de mayor riesgo, identificado en la sección de identificación de nivel de anonimidad.
3. Seleccionar la columna con el rango de accesos identificado en la sección de identificación de nivel de accesibilidad.
4. Identificar la celda de la matriz en la cual se cruzan la columna y la fila seleccionadas.
5. Identificar la lista o patrón de control que le corresponde aplicar de acuerdo a su nivel de riesgo. Nótese que existen casos en los que además de implementar un patrón de control se deberá implementar una lista de red interna y una lista de acceso físico.

La aplicación de controles en cada entorno deberá ser exhaustiva y deberá cubrir las necesidades de anonimidad, accesibilidad y riesgo por tipo de dato pertinentes para cada tipo de dato personal recabado. De acuerdo con el criterio del responsable o encargado, si así se desea, se pueden implementar más controles que los recomendados.

El patrón de control y las listas de medidas de seguridad correspondientes al nivel de riesgo serán la base con la que se trabajará en el análisis de brecha.

Ejemplo:

Si en el análisis de riesgos se identificó que se cuenta con datos de salud de más de 50,000 titulares, y por lo tanto le corresponde un nivel de riesgo por tipo de dato 3, se deberá seleccionar la tabla 3. Con ello se identifica que le corresponde la lista de medidas administrativas AD-3.

Siguiendo con el ejemplo, decimos que en el análisis de riesgos se identificó que se tienen menos de doscientos accesos a los datos personales y que estos accesos son desde la red interna, el entorno físico y redes de terceros.

Por lo tanto se debe seleccionar la celda que cruza la fila de red de terceros (entorno de mayor anonimidad en este ejemplo) con el rango de accesos menor o igual a 200.

		Medidas administrativas aplicables: AD-3			
Entornos de acceso	**Internet**	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red terceros	RI-2 F-2 DMZ-3	**RI-3 F-2 DMZ-3**	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	WiFi	RI-2 F-2 DMZ-2	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red interna	RI-2 F-2	RI-3 F-2	RI-3 F-2	RI-3 F-2
	Físico	F 2	F 2	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de controles 3. Riesgo por tipo de dato 3

La celda seleccionada indica que se deberá implementar:

- el patrón DMZ-3,
- la lista de medidas de seguridad de red interna RI-3,
- la lista de medidas de seguridad para acceso físico F-2;
- esto además de la lista de medidas administrativas AD-3.

Es importante tomar en cuenta que este ejercicio se debe hacer por cada tipo de dato.

5. Optimización de los niveles de riesgo

Existen acciones que se pueden implementar en la metodología BAA para disminuir el riesgo latente de los datos y así reducir el nivel de seguridad requerido, como las que se muestran a continuación:

Disociar la información

Por medio de la correcta aplicación del control de disociación se despersonalizan los datos y con ello se minimiza el riesgo para las personas, logrando así que ya no sean identificables. Es decir, cuando los datos se aíslan de manera que por sí mismos no aporten información valiosa o no puedan volver identificable a una persona, entonces se considera que la información está disociada. Para que dicho mecanismo sea efectivo es necesario contar con autenticaciones distintas para acceder a los diferentes datos aislados.

Separación de la información
Separando la información en bases de datos de menor tamaño ayuda a disminuir el riesgo que representan, pues mientras mayor cantidad de datos tenga una sola base de datos, la probabilidad de que un atacante tenga interés en ella se incrementa. Es necesario considerar que para que el control de separación sea efectivo, no debe existir ningún acceso por medio del cual se pueda acceder al total de información, es decir, es necesario que cada base de datos requiera una autenticación distinta.

Incluir datos de menor riesgo en la caja fuerte. Debido a que el nivel de protección de la red interna está determinado por el dato con mayor nivel de riesgo, existen casos en los que, implementar los controles de protección requeridos a lo largo de la red es costoso. Una estrategia recomendada para disminuir los costos de protección es aislar los datos de menor riesgo dentro de la caja fuerte, bajando automáticamente el nivel de protección requerido para la red interna.
Es recomendable analizar los costos de tomar esta medida o no, para tomar la opción que le brinde mayor eficiencia en la implementación de las medidas.

Reducción de accesibilidad
Disminuir la cantidad de accesos a los datos personales contribuye a la reducción del riesgo latente de los datos, por lo tanto se recomienda analizar si todos los accesos a los datos personales son necesarios, para llevar a cabo una depuración de los mismos. Con esta acción bajamos el nivel de riesgo y con ello el nivel de protección requerido.

Eliminar entornos de acceso
Existen entornos de acceso que suponen un nivel de riesgo mayor pues presentan niveles de anonimidad alta, por lo que descartar el acceso a los datos personales desde entornos que no sean específicamente necesarios aporta a la disminución del riesgo latente de los datos personales.

6. Inventario de datos y sistemas de tratamiento

Se deben inventariar los soportes físicos (archivos, gavetas, entre otros) y electrónicos (sistemas, aplicaciones, bases de datos, entre otros) donde se tratan los datos personales.

La organización debe identificar exclusivamente aquellos sistemas de tratamiento que manejan datos personales. Todos aquellos sistemas de tratamiento que no manejan datos personales, no están en el alcance de este procedimiento y para fines del presente no es necesario inventariarlos.

Por cada uno de los datos personales identificados, se deben identificar los soportes físicos, tales como archiveros, gavetas, anaqueles y bodegas en los cuales se procesan y almacenan dichos datos. En el mismo sentido se deben identificar los soportes electrónicos, tales como aplicaciones, bases de datos, unidades de almacenamiento, equipos y toda aquella infraestructura tecnológica en los cuales se procesan y almacenan dichos datos.

Para desarrollar el inventario, se recomienda tomar en cuenta los siguientes:

- Si se obtuvo un nivel de riesgo por tipo de dato igual a 1, 2 o 3, entonces:
    - El inventario de datos es simple, es suficiente enlistar los sistemas de tratamiento físico o electrónico.

- Si se obtuvo un nivel de riesgo por tipo de dato igual a 4 o 5, entonces:
    - Se recomienda realizar un inventario de sistemas físicos y electrónicos con mayor nivel de detalle donde se tratan los datos personales y sensibles.

El inventario debe considerar los tipos de datos personales y sensibles que se tratan, y recabar al menos la siguiente información:

Sistemas de tratamiento físico

- **Lista de soportes físicos.** Enlistar y describir los soportes físicos donde se almacenan los datos, por mencionar algunos: gavetas, archiveros, bóvedas de documentación histórica, cajas de documentación, entre otra.
- **Número de soportes físicos.** Enumerar la cantidad o volumen de soportes físicos.

Sistemas de tratamiento electrónico

- **Lista de aplicaciones.** Enlistar y describir las aplicaciones a través de las cuales se tratan los datos, por ejemplo ERP´s, sistemas legados, paquetes de software, entre otros.
- **Número de aplicaciones.** Enumerar la cantidad o volumen de aplicaciones desde donde se traten datos.
- **Lista de servidores / equipos.** Enlistar y describir los servidores físicos o virtuales desde donde se tratan datos, considerar las bases de datos, servidores de archivos, servidores de aplicación, entre otros.
- **Número de servidores / equipos.** Enumerar la cantidad o volumen de servidores o equipos que traten los datos.

7. Resumen de la metodología

El objetivo final de esta metodología es determinar los controles recomendados de protección de datos de acuerdo al entorno de riesgo existente. Por lo tanto, estas listas de controles se identificarán al final, utilizando tres factores:

- Riesgo por tipo de dato (beneficio);
- Nivel de accesibilidad, y
- Nivel de anonimidad.

Los pasos a seguir son:

1. Identificar el riesgo por tipo de dato, de acuerdo con los datos personales que se tratan (nivel de riesgo inherente).
2. Con el número identificado en la primera tabla (nivel de riesgo inherente), se procede a buscar la tabla que le corresponde a ese número, para en ella utilizar como coordenadas las otras dos variables: accesibilidad y anonimidad.
3. Utilizando el grado de accesibilidad y anonimidad, es decir, desde dónde se accede a los datos (anonimidad) y qué cantidad de accesos existen (accesibilidad), se identifica la celda correspondiente en la cual se identificarán los patrones de controles que se requiere implantar.

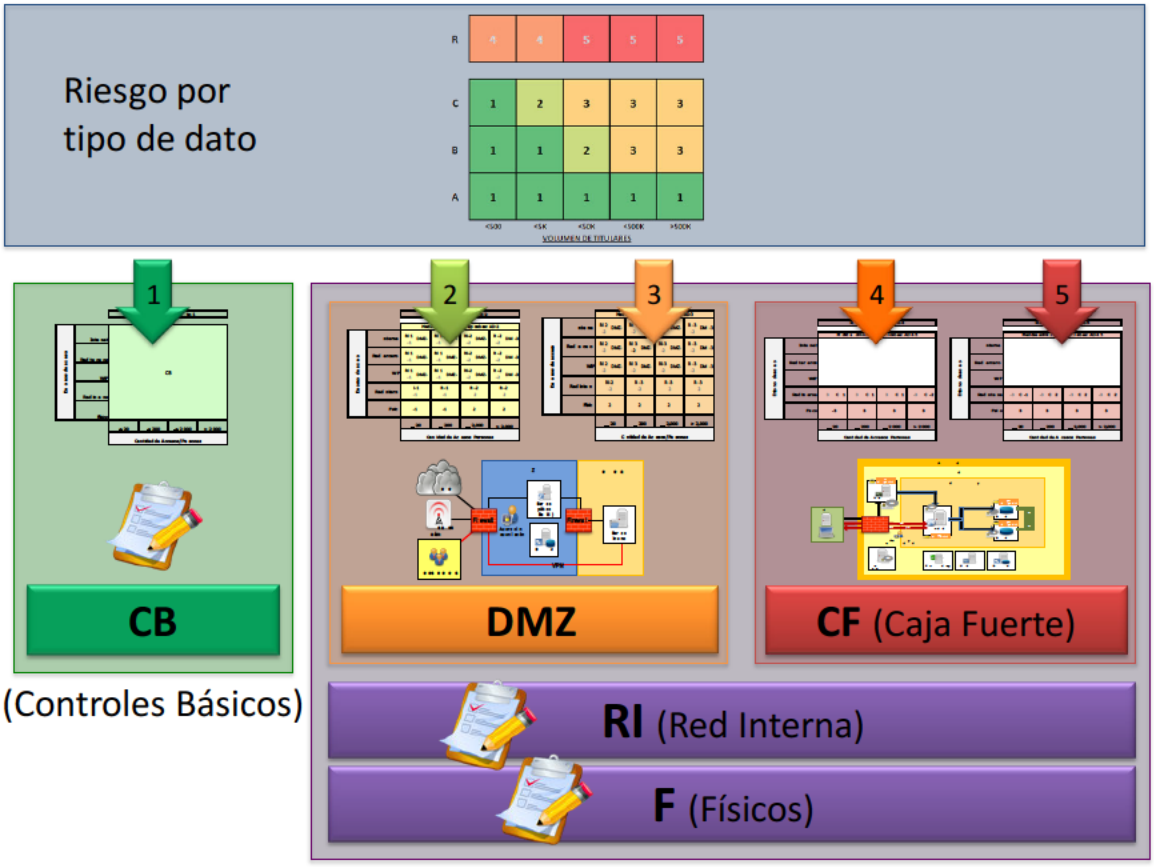


Figura 6. Resumen de la metodología

ANEXO A. MECANISMO DE AUTOEVALUACIÓN

Razón social:	
Dirección:	
Actividad comercial:	
Fecha de elaboración:	

Obtener, usar, divulgar o almacenar datos personales es legítimo, sin embargo la seguridad en el contexto de la Ley busca prevenir el mal uso y el acceso no autorizado a estos datos.

Este mecanismo le permitirá llevar acabo un autodiagnóstico para determinar su nivel de riesgo de acuerdo con los datos personales que obtiene, usa, divulga o almacena. A partir del nivel de riesgo identificado se recomendará el conjunto de controles aplicables. Se recomienda llevar a cabo el ejercicio de resolución del mecanismo de autoevaluación por lo menos de forma anual.

Se deberá entender como datos personales cualquier información concerniente a una persona física identificada o identificable, como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, dependientes, beneficiarios y familiares, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, referencias laborales, referencias personales, información migratoria y cualquier otro dato que pudiera identificar o hacer identificable al titular.

¿Obtiene, usa, divulga o almacena información concerniente a una persona física identificada o identificable?

○ SI ○ NO

En el caso de haber contestado “NO”, entonces no tiene la obligación de cumplir con lo dispuesto en la Ley. En caso contrario se deberá continuar con la sección 1 y 2.

NOMBRE	FECHA	FIRMA

<u>Sección 1: Cuestionario de autoevaluación sobre tipo de datos personales y volumen de personas</u>

Datos de nivel de riesgo medio:

Los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita identificar la ubicación del titular.

1. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos que permiten inferir el patrimonio del titular, que incluyen entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados.

2. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos de autenticación son información referente a los usuarios y contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, copia de identificaciones oficiales y cualquier otro que permita autenticar al titular.

3. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos dentro de los expedientes jurídicos, penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido de forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

4. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

El número de tarjeta bancaria o de crédito conformado por los 15 o 16 dígitos únicos de la tarjeta de crédito y/o débito.

5. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Datos de nivel de riesgo alto:

De acuerdo con la LFPDPPP, los datos sensibles incluyen los datos sensibles incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasada, presente o futura; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular. Para efectos del presente documento los datos sensibles serán considerados datos de alto riesgo.

6. ¿De los datos sensibles descritos en este punto; obtiene, usa, divulga o almacena datos de más de 500 personas?

SI NO

Datos reforzados:

Los datos ***reforzados*** son los que de acuerdo a su naturaleza tienen un nivel superior de riesgo, derivado del valor económico o reputacional que pueda representar para un tercero. A continuación se listan los datos de mayor riesgo:

De ubicación en conjunto con patrimoniales: Aquellos que relacionen datos patrimoniales con ubicación física del titular.

Información adicional de tarjeta bancaria: el número tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, código de seguridad (CVV, CVV2, CAV2, CVC2, CID), datos de banda magnética o número de identificación personal (PIN).

7. ¿Obtiene, usa, divulga o almacena datos correspondientes a los descritos en este punto?

SI NO

Los ***titulares de alto riesgo*** son las personas que debido a su oficio, profesión o naturaleza están expuestos a una mayor probabilidad de ser atacados debido al valor económico o reputacional que sus datos pueden representar para un tercero. Por lo tanto, el tener datos de estos titulares eleva el riesgo de la información de la base de datos completa y en consecuencia para todas las personas contenidas en ella. Los titulares de alto riesgo incluyen líderes políticos, religiosos, empresariales, de opinión, de impartición de justicia, responsables de seguridad nacional y cualquier otra persona que sea considerada como personaje público. Recomendamos que se mantenga un nivel elevado de protección de los datos de los titulares descritos en el párrafo anterior.

8. ¿Obtiene, usa, divulga o almacena datos de titulares de alto riesgo?

SI NO

Si todas las respuestas a las preguntas anteriores fueron “NO”, entonces los controles de seguridad que deberá implantar en los sistemas que traten, procesen o guarden datos personales corresponde al **nivel mínimo requerido** y deberá continuar con la sección 2 de este anexo.

Si al menos una de las respuestas fue “SÍ”, deberá implantar controles de seguridad mayores a las estipuladas en este anexo.

Con el objetivo de simplificar la operación y administración de las medidas de seguridad para el nivel de riesgo por tipo de dato “1”, se recomienda la documentación e implementación de un Contrato de Adhesión (CDA), que conjunte de forma sencilla los controles y funja como una lista de control de accesos a los datos personales. El CDA se incluye en la siguiente sección del presente anexo.

Sección 2: Contrato de Adhesión (CDA).

Si después de haber contestado el cuestionario de autoevaluación la sección 1, se determinó que el nivel de seguridad aplicable es el **mínimo requerido,** de acuerdo con los datos personales que se obtienen, usan, divulgan o almacenan; entonces se recomienda implementar el patrón de control básico (ver ANEXO B), o el CDA mismo que mantiene de forma simplificada los controles incluidos en el patrón mencionado.

1. **Personal autorizado**. A continuación enliste las personas autorizadas para obtener, usar, divulgar, almacenar o acceder a los datos personales.

Nombre Completo	Función	Fecha inicio	Fecha fin	Firma

1.1. El personal interno o externo que interviene en el tratamiento de los datos personales tiene, entre otras, las siguientes obligaciones:
- Resguardar la confidencialidad de los datos personales a los que se tiene acceso.
- Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos en el exterior.
- Leer el CDA y firmarlo aceptando el entendimiento de las obligaciones que tiene respecto a la protección de los datos personales.

1.2. Responsabilidades de Seguridad:
Todos los empleados, contratistas y terceros deben cumplir con las medidas de seguridad dispuestas para la protección de los datos personales y hacer uso de los datos personales únicamente para la función para la que fue autorizada.

1.3. Sanciones:
La divulgación o uso no autorizado de los datos personales podrán ser sancionados conforme a lo estipulado en el capítulo X de la LFPDPPP.

2. El CDA deberá ser llenado y actualizado anualmente para asegurar que el tratamiento de los datos personales no ha cambiado y se mantienen las medidas de protección de los mismos.

3. Se debe garantizar que las bases de datos personales, tanto físicas, como electrónicas, mantienen las siguientes medidas de seguridad:

Medida de seguridad	Indicar si se tiene implementado (SI / NO)	Fecha de implementación (sólo si es posterior a la generación inicial del CDA)
Control de acceso por medio de contraseña, llave, cerradura.		

Protector de pantalla con solicitud de contraseña para desbloqueo.		
Mecanismos contra código malicioso.		
Considerar contraseñas para los dispositivos de red diferentes a las provistas por defecto.		
Establecer contraseña a la red inalámbrica.		
Instalar actualizaciones de seguridad en los equipos de forma semestral		

3.1. Registrar los soportes físicos (p.e.: archiveros, entre otros) o electrónicos (p.e.: computadoras portátiles o de escritorio, discos duros, servidores de archivos, aplicaciones, etc.) donde se traten datos personales.

Soportes físicos

ID Soporte	Nombre de Soporte Físico	Ubicación
1	*Archivero de documentos "A"*	

Sistemas electrónicos

ID Soporte	Nombre de Soporte Electrónico
1	*Sistema "A"*
2	*Computadora de escritorio "a"*
3	*Computadora de escritorio "b"*

3.2. Se debe garantizar la eliminación de los accesos otorgados al vencimiento de la fecha o rango autorizado. El activo o llave otorgados para llevar a cabo las funciones deben ser devueltos.

3.3. Protección de equipo: El equipo debe estar situado de forma que se eviten accesos no autorizados.

4. Cuando el tratamiento de la información ya no sea necesario, se debe:
    - Garantizar la destrucción de los medios físicos que contengan datos personales, de tal forma que no sea posible reconstruirlos.
    - Garantizar el borrado de la información en bases de datos lógicas que contengan datos personales, de tal forma que no sean fácilmente recuperables.

Aunado a los controles mencionados anteriormente, se debe poner en práctica un programa de capacitación, actualización y concienciación del personal sobre las obligaciones en materia de protección de datos personales, como lo indica el artículo 68 del Reglamento de la LFPDPPP. Asimismo, el responsable debe cumplir con todos los principios y deberes que establece la LFPDPPP, su Reglamento y normativa aplicable.

NOMBRE DEL RESPONSABLE DE LOS DATOS PERSONALES	FECHA	FIRMA

ANEXO B. MEDIDAS DE SEGURIDAD

En el presente anexo se encuentran los patrones de control y las listas de medidas de seguridad definidas para las combinaciones disponibles de riesgo por tipo de dato, accesibilidad y anonimidad. Los controles (medidas de seguridad) fueron seleccionados de las mejores prácticas, como ISO 27002.

Es importante señalar que implantar un grupo de controles tiene más beneficio que la selección e implantación de controles de manera individual, ya que la conjunción de los mismos representa en cierta medida una acumulación de las capacidades de mitigación de riesgos y protección de información.

Para apoyar a la identificación del grupo de medidas de seguridad que le corresponde de acuerdo a su nivel de riesgo se definieron cinco tablas matriciales, una por cada nivel de riesgo por tipo de dato, en las que las filas son los entornos de acceso a los datos y las columnas son los umbrales de accesos potenciales a los datos.

Para determinar la lista o patrón correspondiente, se deberán seguir los siguientes pasos:

- Identificar la tabla que le corresponde de acuerdo con el nivel de riesgo por tipo de dato que se obtuvo en el análisis de riesgos.
- Una vez que se encuentre posicionado en la tabla que le corresponde, identificar el rango de accesos potenciales que se tiene para cada tipo de dato y el entorno de acceso de máxima anonimidad desde el que se accede a los datos. La celda que cruza en las filas y columnas corresponde al patrón de control o lista de controles a implantar.

Para más detalle ver la sección de identificación de medidas de seguridad.

A continuación se presentan las cinco tablas disponibles:

Tabla 1: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 1.

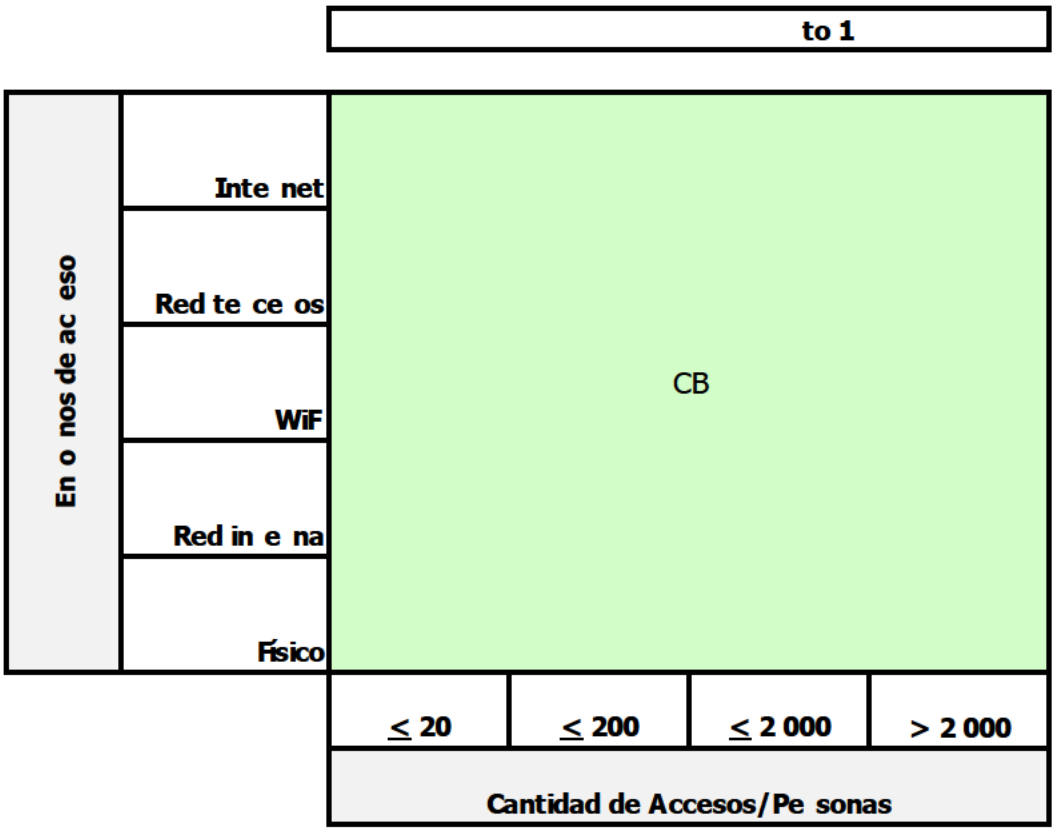


Tabla de control 1. Riesgo por tipo de dato 1

Tabla 2: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 2.

		o 2			
		Med d		ap cab es: AD-2	
En orno de ac e o	nterne	RI 1 -1 DMZ-	RI 1 -1 -	RI-2 -2 DMZ-	R -2 -2 DM -3
	Red ercero	RI 1 -1 DMZ-	RI 1 -1 DMZ-	RI-2 -2 DMZ-	R -2 -2 DM -3
	W F	RI 1 -1 DMZ-	RI 1 -1 DMZ-	RI-2 -2 DMZ-	R -2 -2 DM -3
	Red ntern	I-1 -1	R -1 -1	R -2 2	R -2 2
	Fsic	-1	-1	2	2
		_ 20	_ 200	_ 2,000	> 2,000
		Can idad de Ac esos Personas			

Tabla de control 2. Riesgo por tipo de dato 2

Tabla 3: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 3.

		Med		AD-3	
En o nos de acceso	nte ne	RI 2 -2 DMZ-	RI -2	DMZ-	R -3 -2 DM -3
	Red e ce o	RI 2 -2 DMZ-	RI 3 -2 DMZ-	RI-3 -2 DMZ-	R -3 -2 DM -3
	WiF	RI 2 -2 DMZ-	RI 3 -2 DMZ-	RI-3 -2 DMZ-	R -3 -2 DM -3
	Red inte n	RI-2 -2	R -3 -2	R -3 2	R -3 2
	Físic	2	2	2	2
		_ 20	**_ 200**	**_ 2,000**	**> 2,000**
		C ntidad de Ac esos/Pe sonas			

Tabla de control 3. Riesgo por tipo de dato 3

Tabla 4: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 4.

		R o 4			
		M did s dm n s l cab es: AD 4-5			
Ento no de ac e o	Inte net				
	Red ter eros				
	WiF				
	Red in erna	3 C 1	3 C 1	3 C 1	-3 C -2
	Fs co	-3	3	3	3
		_ 20	_ 200	_ 2 000	> 2 000
		Cant dad de Accesos Personas			

Tabla de control 4. Riesgo por tipo de dato 4

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos vs. entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, Internet o redes inalámbricas.

Tabla 5: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 5.

		Re o 5			
		Med das admi i i ab es: AD-4 5			
Ento no de ac e o	nterne				
	Red ercero				
	W F				
	Red nte na	-3 C -1	-3 C 2	-3 C 2	-3 C 2
	Fsi o	3	3	3	3
		_ 20	_ 200	_ 2,000	> 2,000
		Cant dad de A cesos Personas			

Tabla de control 5. Riesgo por tipo de dato 5

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos vs. entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, Internet o redes inalámbricas.

B.1 Medidas de seguridad

Se han definido listas de controles y patrones de control que agrupan medidas de seguridad basadas principalmente en ISO/IEC 27002. La selección de medidas será de acuerdo con el nivel de riesgo obtenido y será conforme a las tablas de control definidas.

- Listas de controles. Utilizaremos este término para describir la situación en la que no es imperante implantar todos los controles sugeridos, sino que existirán medidas necesarias y medidas opcionales para que el responsable de seguridad seleccione aquéllas que, sumadas, apoyan a la mitigación del riesgo existente en el contexto de su organización. Es decir, en el caso de las listas la suma de controles contribuye a la protección de la información, teniendo la posibilidad de seleccionar uno a más controles. Existen listas de controles administrativos, de seguridad física y del entorno de red interna.

- Patrones de control. Utilizaremos este término para describir la situación en la que, de acuerdo a la situación de riesgo identificada, es necesario implantar en su totalidad los controles descritos dentro del mismo. Los patrones de control existentes son: Controles Básicos, DMZ y Caja Fuerte (entorno recomendado para resguardar información con nivel de riesgo por tipo de dato 4 y 5). Sólo se podrá descartar alguna medida de seguridad en el caso de que no sea aplicable a su infraestructura, por ejemplo un control enfocado a comercio electrónico se podrá descartar sólo si la organización no cuenta con dicha actividad.

B.2 Listas de medidas de seguridad

El responsable de seguridad deberá determinar el mínimo de controles opcionales que requiere conforme al contexto de su red.

Se cuenta con tres tipos de listas, cada una de ellas aplica para diferentes combinaciones de riesgo:

- AD: Lista de medidas administrativas, esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista.
    a. AD-2. Medidas administrativas para nivel de riesgo por tipo de dato 2
    b. AD-3. Medidas administrativas para nivel de riesgo por tipo de dato 3
    c. AD-4-5. Medidas administrativas para nivel de riesgo por tipo de dato 4 o 5

- RI: Lista de medidas de seguridad aplicable para accesos desde la red interna, esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista; se debe considerar que la suma de controles contribuye a la disminución del riesgo que puede presentarse en la red.
    a. RI 1. Medidas básicas de seguridad para accesos desde red interna
    b. RI 2. Medidas intermedias de seguridad para accesos desde red interna
    c. RI 3. Medidas reforzadas de seguridad para accesos desde red interna

- F: Lista de medidas de seguridad aplicable para accesos desde el entorno físico, esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista; se debe considerar que la suma de controles contribuye a la disminución del riesgo que puede presentarse al acceder de forma física a los datos personales.
    a. FI 1. Medidas básicas de seguridad para accesos físicos
    b. FI 2. Medidas intermedias de seguridad para accesos físicos
    c. FI 3. Medidas reforzadas de seguridad para accesos físicos

B.2.1 Medidas administrativas

AD-2 Lista de medidas administrativas para nivel 2

A continuación se incluyen las medidas de seguridad administrativas aplicables a particulares con bases de datos personales con nivel de riesgo por tipo de dato 2.

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles por patrón como política de seguridad.	5.1.1	Necesario
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	Necesario
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual	6.1.5	Necesario
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	Se deben identificar todas las interacciones entre la organización y el cliente en los cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa.	6.2.2	Necesario

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene, procese, transmita u otorgue acceso datos personales o sensibles.	7.1.1	Necesario
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Estos contratos deben ser firmados por los empleados, contratistas y usuarios de terceros.	8.1.1	Necesario
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Ninguno	8.2.2	Necesario
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Evitar el uso de medios removibles, cuando sea necesario justificar, documentar y autorizar su uso.	10.7.1	Necesario
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo con lo establecido en la LFPDPPP y su Reglamento.	10.8.2	Necesario

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	6.1.3	Opcional
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad.	6.2.3	Opcional
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	Opcional
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	Opcional
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	Opcional

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	Ninguno	10.1.3	Opcional
Seguimiento y revisión de los servicios de terceros: Los servicios, reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.	Revisiones anuales.	10.2.2	Opcional
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Realizar revisiones aleatorias de las bitácoras de acceso para identificar accesos no autorizados. Considerar una frecuencia semestral.	10.10.2	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno	11.3.3	Opcional
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos.	12.1.1	Opcional
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	Considerar la aprobación del cambio por parte del responsable de seguridad. El procedimiento debe considerar la capacidad de realizar roll-back del cambio.	12.5.1	Opcional

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad.	12.5.2	Opcional
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	Incluir los criterios de tipificación de un incidente.	13.2.1	Opcional
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y presentar evidencias de acuerdo a las reglas de la jurisdicción.	Ninguno	13.2.3	Opcional
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	Opcional

AD-3 Lista de medidas administrativas para nivel 3

A continuación se incluyen las medidas de seguridad administrativas aplicables a particulares con bases de datos personales con nivel de riesgo por tipo de dato 3.

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles por patrón como política de seguridad.	5.1.1	Necesario
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	Necesario
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	6.1.5	Necesario
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	Se deben identificar todas las interacciones entre la organización y el cliente en los cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa.	6.2.2	Necesario

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad	6.2.3	Necesario
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene, procese, transmita u otorgue acceso datos personales o sensibles.	7.1.1	Necesario
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante.	8.1.1	Necesario
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Ninguno	8.1.3	Necesario
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Ninguno	8.2.2	Necesario

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Evitar el uso de medios removibles, cuando sea necesario justificar, documentar y autorizar su uso.	10.7.1	Necesario
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la LFPDPPP y su Reglamento.	10.8.2	Necesario
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Mantener un procedimiento de monitoreo constante.	10.10.2	Necesario
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	Necesario
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	Considerar la aprobación del cambio por parte del responsable de seguridad. El procedimiento debe considerar la capacidad de realizar roll-back del cambio.	12.5.1	Necesario

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	Incluir los criterios de tipificación de un incidente.	13.2.1	Necesario
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	6.1.3	Opcional
Proceso de autorización de instalaciones de procesamiento de la información: Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información debe ser definido e implementado.	Ninguno	6.1.4	Opcional
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión anual. Evitar conflictos de interés, puede ser revisión externa.	6.1.8	Opcional
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	Opcional
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	Opcional

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Retorno de los activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez se termine el trabajo, contrato o acuerdo.	Cotejar contra inventario los activos entregados al empleado, contratista o tercero.	8.3.2	Opcional
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	Opcional
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	Ninguno	10.1.3	Opcional
Seguimiento y revisión de los servicios de terceros: Los servicios, reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.	Revisiones anuales pactadas contractualmente.	10.2.2	Opcional
Gestión de cambios a los servicios de terceros: Los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de políticas de seguridad, procedimientos y controles deberán ser gestionados. Considerando la criticidad de los sistemas de negocio, los procesos involucrados y la reevaluación de riesgos.	Se deberá incluir la autorización del responsable de seguridad en cualquier cambio que se realice en contratos o acuerdos de nivel de servicio con tercero.	10.2.3	Opcional
Aceptación del sistema: Se deberán establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones; se deberán llevar a cabo pruebas de los sistemas durante y previo a la aceptación de los mismos.	Ninguno	10.3.2	Opcional

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos de manejo de información: Se deberán documentar e implementar procedimientos para el manejo y almacenaje de información para protegerla de divulgación o uso no autorizado.	Documentar y autorizar las extracciones o transferencias de datos personales.	10.7.3	Opcional
Seguridad de la documentación de los sistemas: Deberá protegerse la documentación del sistema contra accesos no autorizados.	Definir un repositorio único para toda la documentación del sistema. Proteger el repositorio con contraseña. Cifrado Opcional.	10.7.4	Opcional
Política de control de acceso: Se deberá establecer, documentar y revisar una política de control de accesos. La misma deberá ser revisada de acuerdo a los requerimientos de negocio para los accesos.	Incluir: - Criterios para la generación y asignación de accesos - Responsabilidades del usuario Revisión anual de la política.	11.1.1	Opcional
Revisión de los derechos de acceso de usuario: La gerencia deberá revisar los derechos de acceso de los usuarios. Realizar estas revisiones en intervalos planeados, mediante un proceso formal.	Revisiones anuales	11.2.4	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno	11.3.3	Opcional
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos.	12.1.1	Opcional

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad.	12.5.2	Opcional
Reporte de vulnerabilidades de seguridad: Se debe requerir a todos los empleados, contratistas y terceras partes que notifiquen cualquier vulnerabilidad o evento de seguridad de la información en los sistemas o servicios.	Ninguno	13.1.2	Opcional
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y presentar evidencias de acuerdo a las reglas de la jurisdicción.	Ninguno	13.2.3	Opcional

AD-4-5 Lista de medidas administrativas para nivel 4 y 5

A continuación se incluyen las medidas de seguridad administrativas aplicables a particulares con bases de datos personales con nivel de riesgo por tipo de dato 4 y 5.

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles por patrón como política de seguridad.	5.1.1	Necesario
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	Necesario
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	6.1.5	Necesario
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión semestral. Evitar conflictos de interés, puede ser revisión externa.	6.1.8	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	Se deben identificar todas las interacciones entre la organización y el cliente en los cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa.	6.2.2	Necesario
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad.	6.2.3	Necesario
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Documentar roles y responsabilidades en perfiles de puesto.	8.1.1	Necesario
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Ninguno	8.1.3	Necesario
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Ninguno	8.2.2	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	Ninguno	10.1.3	Necesario
Aceptación del sistema: Se deberán establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones; se deberán llevar a cabo pruebas de los sistemas durante y previo a la aceptación de los mismos.	Ninguno	10.3.2	Necesario
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Evitar el uso de medios removibles, cuando sea necesario justificar, documentar y autorizar su uso. Todos los medios removibles deberán ser inventariados como activos de información.	10.7.1	Necesario
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la LFPDPPP y su Reglamento.	10.8.2	Necesario
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Mantener un procedimiento de monitoreo constante.	10.10.2	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Política de control de acceso: Se deberá establecer, documentar y revisar una política de control de accesos. La misma deberá ser revisada de acuerdo a los requerimientos de negocio para los accesos.	Incluir: - Criterios para la generación y asignación de accesos - Responsabilidades del usuario Revisión anual de la política.	11.1.1	Necesario
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	Necesario
Administración de contraseñas de usuarios: La asignación de contraseñas deberá controlarse mediante un proceso formal de administración.	Gestión de cuentas privilegiadas.	11.2.3	Necesario
Revisión de los derechos de acceso de usuario: La gerencia deberá revisar los derechos de acceso de los usuarios. Realizar estas revisiones en intervalos planeados, mediante un proceso formal.	Revisiones anuales.	11.2.4	Necesario
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ninguno	12.3.1	Necesario
Administración de llaves de cifrado: Se deben implantar procesos de administración de llaves de cifrado que soporten el uso de técnicas de cifrado en la organización.	Ninguno	12.3.2	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	Considerar la aprobación del cambio por parte del responsable de seguridad. El procedimiento debe considerar la capacidad de realizar roll-back del cambio.	12.5.1	Necesario
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	Incluir los criterios de tipificación de un incidente.	13.2.1	Necesario
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	6.1.3	Opcional
Proceso de autorización de instalaciones de procesamiento de la información: Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información debe ser definido e implementado.	Ninguno	6.1.4	Opcional
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	Opcional

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Investigación de antecedentes: Las verificaciones de antecedentes para todos los candidatos, contratistas y usuarios de terceras partes, deben llevarse a cabo de acuerdo a leyes relevantes, regulaciones y ética, y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información que será accedida y a los riesgos percibidos.	La investigación deberá ser proporcional a las responsabilidades del puesto.	8.1.2	Opcional
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	Opcional
Retorno de los activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez se termine el trabajo, contrato o acuerdo.	Cotejar contra inventario los activos entregados al empleado, contratista o tercero.	8.3.2	Opcional
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	Opcional
Trabajando en áreas seguras: Se deberán diseñar y aplicar pautas y controles de protección física para trabajar en áreas seguras.	Considerar: - No ingresar a áreas seguras con dispositivos de almacenamiento móvil - No ingresar a áreas seguras con dispositivos de grabación de imágenes o video	9.1.5	Opcional
Seguimiento y revisión de los servicios de terceros: Los servicios, reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.	Revisiones anuales pactadas contractualmente.	10.2.2	Opcional

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Gestión de cambios a los servicios de terceros: Los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de políticas de seguridad, procedimientos y controles deberán ser gestionados. Considerando la criticidad de los sistemas de negocio, los procesos involucrados y la reevaluación de riesgos.	Se deberá incluir la autorización del responsable de seguridad en cualquier cambio que se realice en contratos o acuerdos de nivel de servicio con tercero.	10.2.3	Opcional
Procedimientos de manejo de información: Se deberán documentar e implementar procedimientos para el manejo y almacenaje de información para protegerla de divulgación o uso no autorizado.	Documentar y autorizar las extracciones o transferencias de datos personales, considerar cifrado de los datos para estas acciones.	10.7.3	Opcional
Seguridad de la documentación de los sistemas: Deberá protegerse la documentación del sistema contra accesos no autorizados.	Definir un repositorio único para toda la documentación del sistema. Proteger el repositorio con contraseña. Cifrado obligatorio.	10.7.4	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno	11.3.3	Opcional
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos.	12.1.1	Opcional

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad.	12.5.2	Opcional
Reporte de eventos de seguridad de la información: Se deben comunicar los eventos de seguridad de la información tan pronto como sea posible y de acuerdo a los canales de comunicación adecuados.	Ninguno	13.1.1	Opcional
Reporte de vulnerabilidades de seguridad: Se debe requerir a todos los empleados, contratistas y terceras partes que notifiquen cualquier vulnerabilidad o evento de seguridad de la información en los sistemas o servicios.	Ninguno	13.1.2	Opcional
Aprendizaje de los incidentes de seguridad: Se deben implantar los mecanismos necesarios para monitorear y cuantificar los costos y esfuerzos de los incidentes de seguridad de la información.	Documentar una base de conocimiento.	13.2.2	Opcional
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y presentar evidencias de acuerdo a las reglas de la jurisdicción.	Ninguno	13.2.3	Opcional

B.2.2 Medidas de seguridad de red interna

RI-1. Medidas básicas de seguridad para accesos desde red interna

A continuación se incluyen las medidas básicas de seguridad para accesos a los datos personales desde la red interna.

Lista RI-1			
Control	**Parámetro**	**ID**	**Carácter**
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso y usuario que accede.	10.10.1	Necesario
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	Contraseña	11.3.1	Necesario
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	11.3.2	Necesario
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1	Opcional

Lista RI-1			
Control	**Parámetro**	**ID**	**Carácter**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	10.6.1	Opcional
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Frecuencia de verificación semestral	12.6.1	Opcional
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo En particular en los equipos que intervienen en el tratamiento de datos personales	12.3.1	Opcional

RI-2. Medidas intermedias de seguridad para accesos desde red interna

A continuación se incluyen las medidas intermedias de seguridad para accesos a los datos personales desde la red interna.

Lista RI-2			
Control	**Parámetro**	**ID**	**Carácter**
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1	Necesario
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	10.6.1	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario y cambios a realizar Asegurar que se registren las actividades de administración del sistema	10.10.1 10.10.4	Necesario
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	Poner especial atención en los usuarios de altos privilegios.	11.2.2	Necesario

Lista RI-2			
Control	**Parámetro**	**ID**	**Carácter**
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	Contraseña de mínimo 10 caracteres	11.3.1	Necesario
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	11.3.2	Necesario
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Ninguno	11.5.2	Necesario
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1	Necesario
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Ninguno	9.2.6	Opcional
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2	Opcional

Lista RI-2			
Control	**Parámetro**	**ID**	**Carácter**
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4	Opcional
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1	Opcional
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP	10.10.6	Opcional
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo. En particular en los equipos que intervienen en el tratamiento de datos personales	12.3.1	Opcional

RI-3. Medidas avanzadas de seguridad para accesos desde red interna

A continuación se incluyen las medidas básicas de seguridad para accesos a los datos personales desde la red interna.

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Ninguno	9.2.6	Necesario
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1	Necesario
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	10.6.1	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario y cambios a realizar. Asegurar que se registren las actividades de administración del sistema.	10.10.1 10.10.4	Necesario

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	Poner especial atención en los usuarios de altos privilegios. Gestionar de forma centralizada los privilegios para reducir número de lugares donde se autentican y autorizan los accesos.	11.2.2	Necesario
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	Contraseña de mínimo 12 caracteres	11.3.1	Necesario
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	11.3.2	Necesario
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	No utilizar usuarios genéricos No compartir usuarios	11.5.2	Necesario
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1	Necesario

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo. En particular en los equipos que intervienen en el tratamiento de datos personales	12.3.1	Necesario
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1	Necesario
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Se recomienda alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2	Opcional
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4	Opcional
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Asegurar que los registros de auditoría no puedan modificarse	10.10.3	Opcional
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP	10.10.6	Opcional

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos de acceso seguro a los sistemas (log-on): Se debe controlar el acceso a los sistemas operativos, mediante un proceso seguro de inicio de sesión (log-on)	Ninguno	11.5.1	Opcional
Tiempo de expiración de las sesiones: se deben desactivar las sesiones inactivas después de un periodo de inactividad definido.	Considerar como tiempo de expiración 10 minutos como máximo para accesos a información personal	11.5.5	Opcional
Protección de las herramientas de auditoría de los sistemas de información: Se debe prevenir el acceso a las herramientas de auditoría de los sistemas de información para prevenir cualquier compromiso o mal uso de dicha información.	Cuando accedan a información personal	15.3.2	Opcional
Filtros de contenido para correo electrónico, internet y mensajería.	En particular cuidar las salidas de información personal	SM.1	Opcional

B.2.3 Medidas de seguridad de acceso físico

F-1. Medidas básicas de seguridad para accesos físicos

A continuación se incluyen las medidas básicas de seguridad para accesos a los datos personales desde el entorno físico.

Lista F-1			
Control	**Parámetro**	**ID**	**Carácter**
Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados y llaves en archiveros y habitaciones que resguarden datos personales.	9.1.1	Necesario
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Acceso Físico: Registrar fecha de acceso y usuario que accede.	10.10.1	Necesario
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno	9.2.1	Opcional

Lista F-1			
Control	**Parámetro**	**ID**	**Carácter**
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos.	9.2.5	Opcional
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	10.7.2	Opcional

F-2. Medidas intermedias de seguridad para accesos físicos

A continuación se incluyen las medidas intermedias de seguridad para accesos a los datos personales desde el entorno físico.

Lista F-2			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Ninguno	8.3.3	Necesario
Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados, llaves y tarjetas de acceso en archiveros y habitaciones que resguarden datos personales.	9.1.1	Necesario
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7	Necesario
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	10.7.2	Necesario

Lista F-2			
Control	**Parámetro**	**ID**	**Carácter**
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, nombre completo de la persona que accede y cambios a realizar	10.10.1	Necesario
Implementar un sistema de cámaras de seguridad.	Ninguno	SM.22	Necesario
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Considerar sitios donde se le de tratamiento a información física y electrónica. Considerar tarjetas de proximidad, teclados de combinación.	9.1.2	Opcional
Áreas de acceso público, carga y entrega: Los puntos de acceso tales como los de entrega, áreas de carga y otros puntos donde personas no autorizadas pueden entrar a las instalaciones, debe estar controladas y, si es posible, aisladas de las instalaciones donde se procesa información para evitar accesos no autorizados.	Ninguno	9.1.6	Opcional
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno	9.2.1	Opcional

Lista F-2			
Control	**Parámetro**	**ID**	**Carácter**
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos, utilizar candados para equipos.	9.2.5	Opcional
Separación de la información en diferentes bases de datos e infraestructura.	Ninguno	SM.3	Opcional

F-3. Medidas reforzadas de seguridad para accesos físicos

A continuación se incluyen las medidas reforzadas de seguridad para accesos a los datos personales desde el entorno físico.

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Ninguno	8.3.3	Necesario
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Considerar sitios donde se le de tratamiento a información física y electrónica. Considerar tarjetas de proximidad, biométricos, dobles factores de autenticación.	9.1.2	Necesario
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7	Necesario

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos (empulpado, trituración, incineración).	10.7.2	Necesario
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha y hora de acceso, nombre completo de la persona que accede, cambios a realizar y justificación de los cambios.	10.10.1	Necesario
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Proteger las bitácoras de acceso para evitar modificación o accesos no autorizados. Proteger los videos de vigilancia generados. Considerar controles de restricción física como se establece en 9.1.2 y 9.2.1	10.10.3	Necesario

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	Cada solicitud de acceso a los datos sensibles debe ser autorizada por el área de seguridad de la información.	11.2.2	Necesario
Implementar un sistema de cámaras de seguridad.	Ninguno	SM.22	Necesario
Monitorear cámaras de seguridad, respaldar y resguardar videos generados.	Resguardar respaldos durante un año.	SM.23	Necesario
Áreas de acceso público, carga y entrega: Los puntos de acceso tales como los de entrega, áreas de carga y otros puntos donde personas no autorizadas pueden entrar a las instalaciones, debe estar controladas y, si es posible, aisladas de las instalaciones donde se procesa información para evitar accesos no autorizados.	Ninguno	9.1.6	Opcional
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno	9.2.1	Opcional
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos, utilizar candados, alarmas y mensajes grabados físicamente en el equipo.	9.2.5	Opcional
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4	Opcional

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Evitar el acceso a áreas seguras con artículos o accesorios que permitan la extracción de información personal. Revisiones físicas a la salida de las personas para detectar posibles fugas de información personal.	12.5.4	Opcional
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno	SM.2	Opcional
Separación de la información en diferentes bases de datos e infraestructura	Ninguno	SM.3	Opcional

B.3 Patrones de control

Se han definido dos tipos de patrones, cada uno de ellos con niveles de patrón que atienden a diferentes combinaciones de riesgo. A continuación se listan:

- CB: Patrón de control de medidas de seguridad básicas, es aplicable para aquellos particulares cuyo nivel de riesgo por tipo de dato es igual a 1.

- DMZ: Patrón para accesos desde entornos de alta anonimidad, hace referencia a la necesidad de implementar una zona desmilitarizada como zona de transición entre un entorno de mayor riesgo y uno de menor riesgo. Se contemplan tres niveles de este patrón.
    a. DMZ 2. Patrón de control de medidas intermedias de seguridad para accesos desde entornos de alta anonimidad
    b. DMZ 3. Patrón de control de medidas reforzadas de seguridad para accesos desde entornos de alta anonimidad

- CF: Patrón aplicable para datos de nivel 4 y 5 de riesgo por tipo de dato, su nombre hace referencia las iniciales de Caja Fuerte, debido a que se recomienda que estos tipos de datos se protejan con medidas de seguridad mucho más estrictas y se construya una caja fuerte alrededor de ellos para protegerlos de accesos no autorizados. Se contemplan dos niveles para este patrón. Cabe mencionar que una vez implementada la caja fuerte, el acceso a ella y salida de información de esta debe controlarse estrictamente.
    a. CF 1. Patrón de control de medidas de seguridad para caja fuerte nivel 1
    b. CF 2. Patrón de control de medidas de seguridad para caja fuerte nivel 2

B.3.1 Medidas de seguridad básicas

Con el objetivo de simplificar la operación y administración de las medidas de seguridad para el nivel de riesgo “1” se recomienda la documentación e implementación de un Contrato de Adhesión (CDA), que conjunte de forma sencilla los controles y funja con una lista de control de accesos a los datos personales.

El CDA deben incluir los accesos permitidos a los datos personales, el inventario de bases de datos físicas y electrónicas, así como las medidas de seguridad implementadas. Todos los empleados que intervengan en el tratamiento de datos personales deberán firmarlo.

El Contrato de Adhesión (CDA) puede ser consultado en el ANEXO A.

CB. Patrón de control de medidas de seguridad básicas

A continuación se listan las medidas de seguridad básicas y un mapeo con el contrato de adhesión (CDA).

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles como política de seguridad.	5.1.1	1
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	1
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno.	6.1.3	1
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	6.1.5	1.1
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión anual del documento de autoevaluación o el Contrato de Adhesión (CDA).	6.1.8	2

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	Los terceros que accedan a los datos deben firmar la lista de accesos de personal autorizado, indicando la actividad a realizar, fecha o rango de fechas en las que tendrán acceso y aceptar el conocimiento de las medidas de seguridad necesarias para la protección de los datos personales.	6.2.3	1
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene o procese datos personales o sensibles.	7.1.1	3.1
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	1.1
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Estos contratos deben ser firmados por los empleados, contratistas y usuarios de terceros.	8.1.1	1.2

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Sólo considerar campañas anuales de concienciación.	8.2.2	1.1
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	1.3
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	3.1
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados y llaves en archiveros y habitaciones que resguarden datos personales.	9.1.2	3
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno.	9.2.1	3.2
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos.	9.2.5	1.1

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno.	10.4.1	3
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Considerar contraseñas para los dispositivos de red diferentes a las provistas por defecto. WIFI: establecer contraseña.	10.6.1	3
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	10.7.2	4
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la LFPDPPP y su Reglamento.	10.8.2	1.1
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno.	10.8.3	1.1

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Registrar las personas con acceso autorizado a los datos personales incluyendo fecha de acceso (o rango de acceso permitido) y firma.	10.10.1	1
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	3
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña.	11.3.1	3
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	11.3.2	3
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno.	11.3.3	1
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Instalación de actualizaciones semestralmente.	12.6.1	3

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	2

B.3.2 Patrones de control para DMZ

DMZ-2. Patrón de control de medidas intermedias de seguridad para accesos desde entornos de alta anonimidad

A continuación se incluye la representación gráfica (Figura 7) del patrón de control para mitigar el riesgo cuando los accesos a los datos personales son desde redes inalámbricas, redes de terceros o internet; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

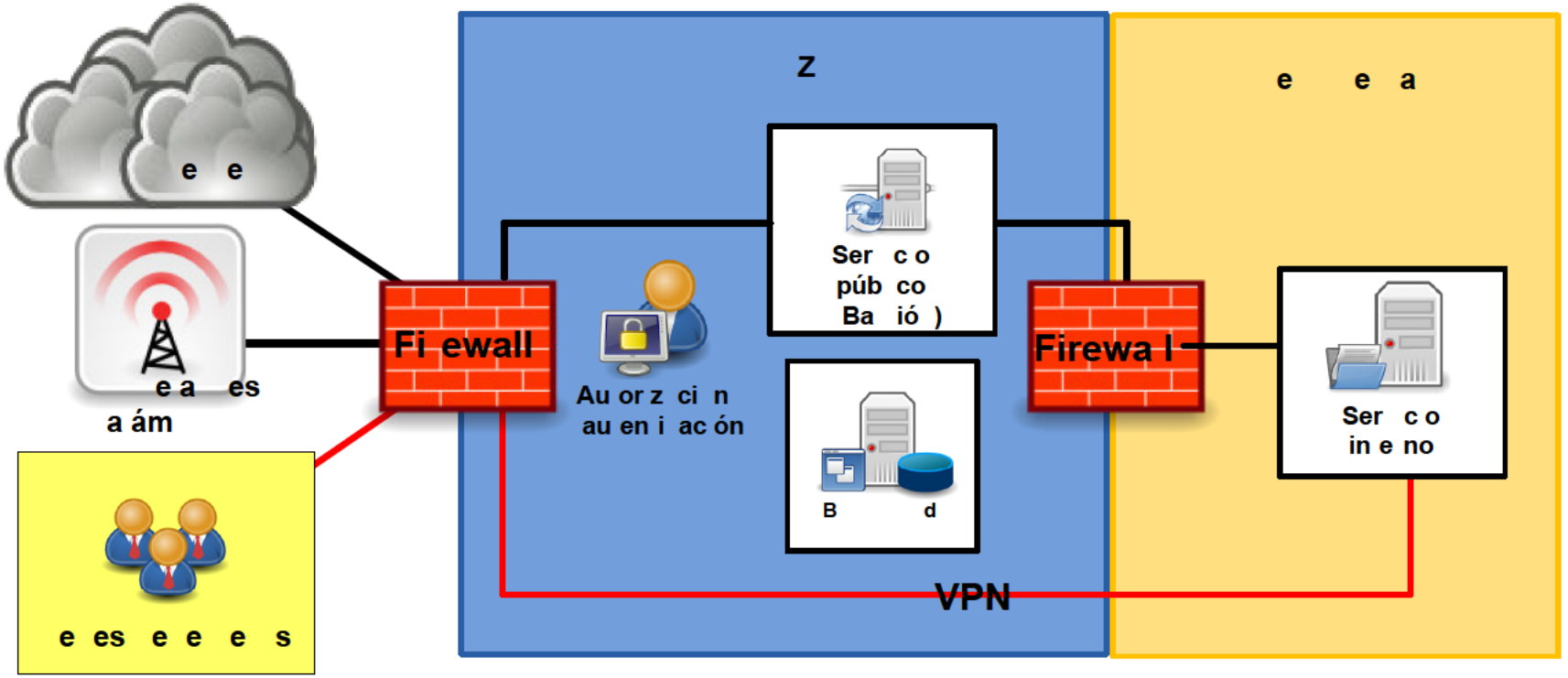


Figura 7. Patrón de control de DMZ-2

Patrón de control DMZ-2		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Evitar uso de protocolos en texto claro Eliminar contraseñas por defecto	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Protocolos Seguros Cifrado del medio Autenticación Disociación de información cuando los datos pasen a un entorno de mayor anonimidad.	10.8.1
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar registrar los accesos a los datos personales y las salidas de información. Incluir IP origen e IP destino para cada conexión.	10.10.1
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	El área de seguridad debe estar involucrada en el proceso de autorización	11.2.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Ninguno	11.4.1
Autenticación del usuario para las conexiones externas: Se deberá utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	La conexión a los sistemas de información desde o hacia redes de terceros, red inalámbrica o internet, para tratar datos personales, debe ser por medio de soluciones de red privada virtual que cuenten con métodos robustos de autenticación y cifrado.	11.4.2

Patrón de control DMZ-2		
Control	**Parámetro**	**ID**
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo	12.3.1
Definir e implementar listas de control de acceso (ACL)	Ninguno	SM.29
Controles de DNS	Ninguno	SM.30
Únicamente permitir servicios públicos dentro de la DMZ	Ninguno	SM.31
Mejores prácticas de configuración del FW	Ninguno	SM.32
Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.33

Patrón de control DMZ-2		
Control	**Parámetro**	**ID**
Red de terceros conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.34
Controles de tráfico entrante y saliente	NO internet hacia LAN Si LAN hacia internet Si DMZ hacia LAN y desde Si Internet hacia y desde DMZ No permitir conexión desde el exterior hacia interior (sin pasar x DMZ)	SM.35

DMZ-3. Patrón de control de medidas reforzadas de seguridad para accesos desde entornos de alta anonimidad

A continuación se incluye la representación gráfica (Figura 8) del patrón de control para mitigar el riesgo cuando los accesos a los datos personales son desde redes inalámbricas, redes de terceros o internet; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

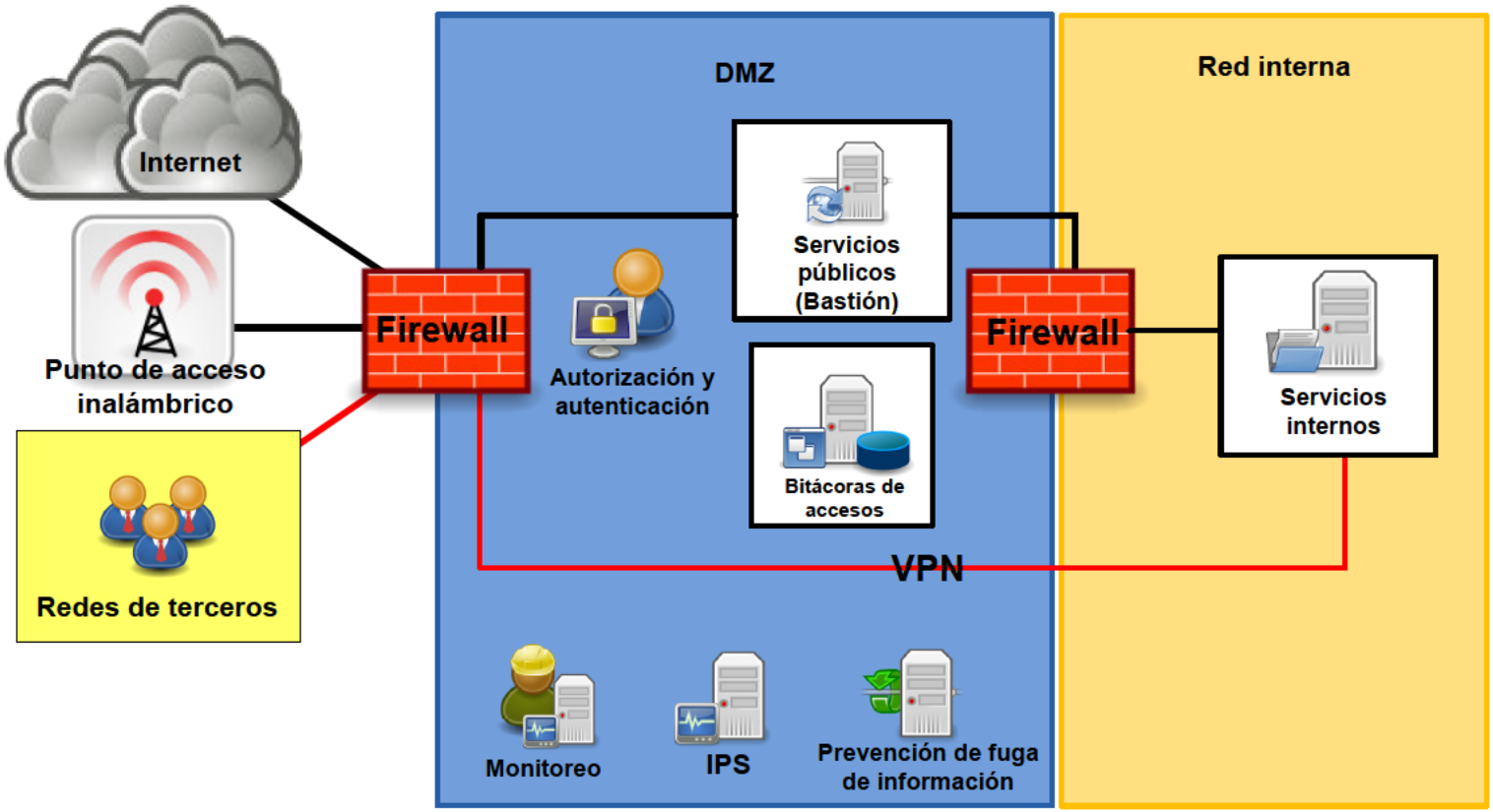


Figura 8. Patrón de control de DMZ-3

Patrón de control DMZ-3		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Evitar uso de protocolos en texto claro Eliminar contraseñas por defecto	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Protocolos Seguros Cifrado del medio Autenticación Disociación de información cuando los datos pasen a un entorno de mayor anonimidad.	10.8.1
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar registrar los accesos a los datos personales y las salidas de información. Incluir IP origen e IP destino para cada conexión.	10.10.1
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Establecer un sistema de monitoreo continuo de los accesos a los datos personales.	10.10.2
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	El área de seguridad debe de estar involucrado en el proceso de autorización	11.2.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Ninguno	11.4.1

Patrón de control DMZ-3		
Control	**Parámetro**	**ID**
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Control de enrutamiento de la red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas y los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.	Ninguno	11.4.7
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno	12.5.4
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno	SM.2
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo	12.3.1
Definir e implementar listas de control de acceso (ACL)	Ninguno	SM.29
Controles de DNS	Ninguno	SM.30

Patrón de control DMZ-3		
Control	**Parámetro**	**ID**
Únicamente permitir servicios públicos dentro de la DMZ	Ninguno	SM.31
Mejores prácticas de configuración del FW	Ninguno	SM.32
Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.33
Red de terceros conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.34
Controles de tráfico entrante y saliente	NO internet hacia LAN Si LAN hacia internet Si DMZ hacia LAN y desde Si Internet hacia y desde DMZ No permitir conexión desde el exterior hacia interior (sin pasar x DMZ)	SM.35
Implementar y monitorear sistemas de prevención de Intrusos (IPS)	Ninguno	SM.36

B.3.3 Patrones de control para caja fuerte

CF-1. Patrón de control de medidas de seguridad para caja fuerte nivel 1

A continuación se incluye la representación gráfica (Figura 9) del patrón de control correspondiente a la caja fuerte; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

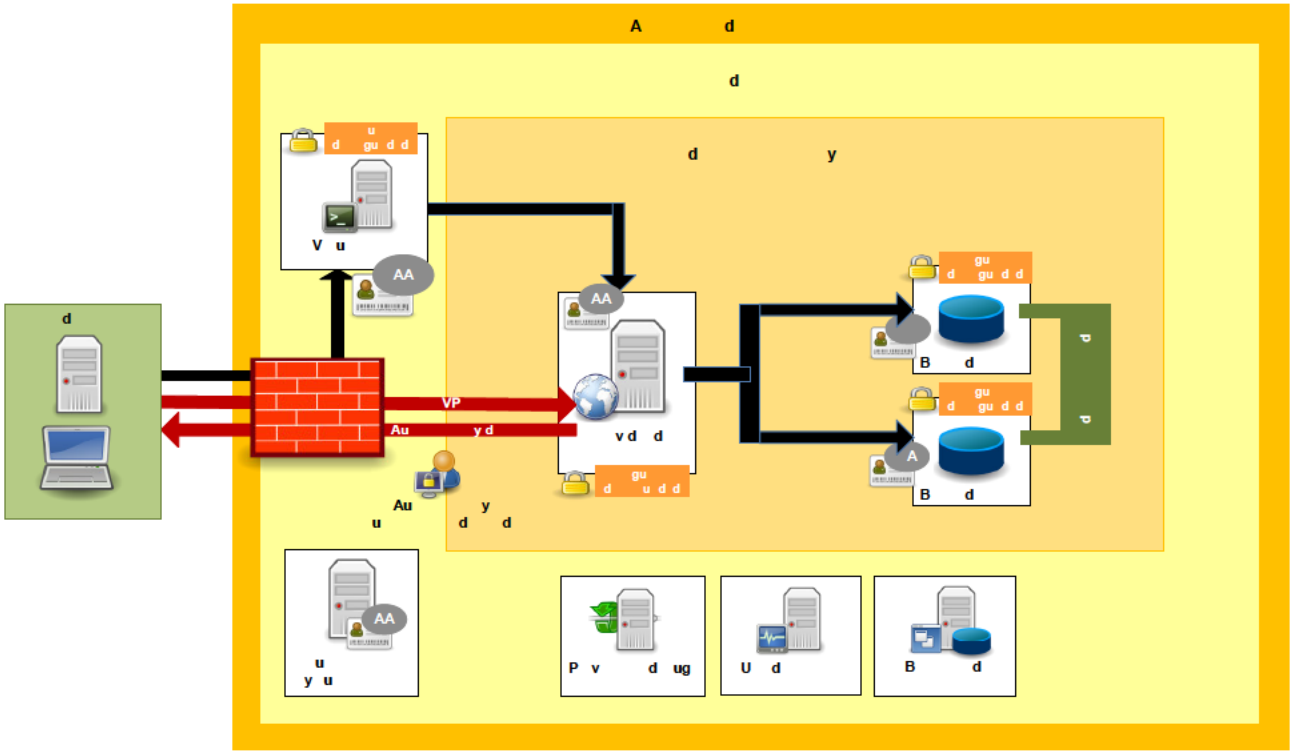


Figura 9. Patrón de control de CF-1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación.	Ninguno	9.2.6
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Se recomienda alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Uso de protocolos seguros Eliminar contraseñas por defecto.	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Se requiere la existencia de una zona de transición en la caja fuerte para evitar que se tenga acceso de forma directa a los datos desde entornos ajenos a la caja fuerte. Considerar los siguientes controles: - Protocolos seguros. - Cifrado del medio. - Autenticación. -Disociación de información cuando los datos salgan de la caja fuerte.	10.8.1
Comercio electrónico: La información involucrada en el comercio electrónico que circule por redes públicas, deberá protegerse de la actividad fraudulenta, divulgación o modificación no autorizada.	Considerar cifrado de los datos ingresados en sitios de comercio electrónico, certificados de seguridad para la transacción.	10.9.1
Transacciones en línea: La información involucrada en transacciones en línea deberá protegerse para impedir su transmisión incompleta, desviación, alteración, divulgación, duplicación o reproducción no autorizada.	Implementar controles de no repudio, considerando cifrado de los datos, certificados de seguridad.	10.9.2

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario, cambios realizados, equipo origen y destino. Asegurar que se registren las actividades de administración del sistema. Garantizar la generación de estas bitácoras.	10.10.1
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Ninguno	10.10.2
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Ninguno	10.10.3
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP.	10.10.6
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Se debe considerar la autorización de acceso a los datos sensibles por el área de seguridad de la información en cada solicitud de acceso.	11.2.1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	El área de seguridad debe estar involucrada en el proceso de autorización. Controlar de la cantidad de datos sensibles que puede tratar un usuario autorizado, con el objetivo de evitar que tenga contacto con una gran cantidad de datos o con las bases de datos completas, mediante el control de tablas y campos.	11.2.2
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña de mínimo 12 caracteres.	11.3.1
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	11.3.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.	11.4.1
Autenticación del usuario para las conexiones externas: Se deberá utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	La conexión a los sistemas de información desde cualquier entorno diferente a la caja fuerte para tratar datos personales, debe ser a través de una zona de transición interna, evitando el acceso directo a los datos y por medio de soluciones de red privada virtual que cuenten con métodos robustos de autenticación y cifrado.	11.4.2

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Identificación de los equipos en la red: La identificación automática de equipo deberá considerarse como un medio de autenticación de conexiones desde lugares y equipos específicos.	Identificación del equipo por medio de dirección MAC o dirección IP.	11.4.3
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Procedimientos de acceso seguro a los sistemas (log-on): Se debe controlar el acceso a los sistemas operativos, mediante un proceso seguro de inicio de sesión (log-on).	Usar protocolos seguros de autenticación.	11.5.1
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Ninguno	11.5.2
Uso de utilidades del sistema: se debe restringir y controlar el uso de programas que tengan la capacidad de sobrepasar los controles de seguridad de los sistemas y de las aplicaciones.	Ninguno	11.5.4
Tiempo de expiración de las sesiones: se deben desactivar las sesiones inactivas después de un periodo de inactividad definido.	Considerar como tiempo de expiración 5 minutos como máximo.	11.5.5

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Aislamiento de sistemas sensibles: los sistemas sensibles deben tener un entorno informático independiente y aislado.	Este control se ve reflejado en la implementación de la caja fuerte.	11.6.2
Validación de los datos de entrada: Se deben validar los datos de entrada a las aplicaciones para asegurar que los datos son apropiados y correctos.	Ninguno	12.2.1
Validación de los datos de salida: Se deben validar los datos de salida de las aplicaciones para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.	Ninguno	12.2.4
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ninguno	12.3.1
Protección de los datos de prueba de los sistemas: Se debe seleccionar cuidadosamente los datos de prueba y deben ser controlados y protegidos adecuadamente.	Considerar la no utilización de datos de producción en ningún ambiente fuera del operativo.	12.4.2
Control de accesos al código fuente: Se debe restringir el acceso al código fuente de los programas.	Ninguno	12.4.3
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno	12.5.4
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Separación de la información en diferentes bases de datos e infraestructura.	Separar la información en bases de datos de menor tamaño para disminuir el interés de un tercero. La separación implica que se implemente una autenticación diferente para cada base de datos.	SM.3
Virtualización de equipos y acceso a la información a través de clientes delgados que impidan guardar la información que se accede en el equipo del usuario.	Ninguno	SM.12
En caso de requerir visualizar o tratar datos personales por medio de sistemas de información o ambientes distintos a producción, se deberán establecer mecanismos de enmascaramiento para prevenir el mal uso de los datos personales y sensibles.	Ninguno	SM.20

CF-2. Patrón de control de medidas de seguridad para caja fuerte nivel 2

A continuación se incluye la representación gráfica (Figura 10) del patrón de control correspondiente a la caja fuerte; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

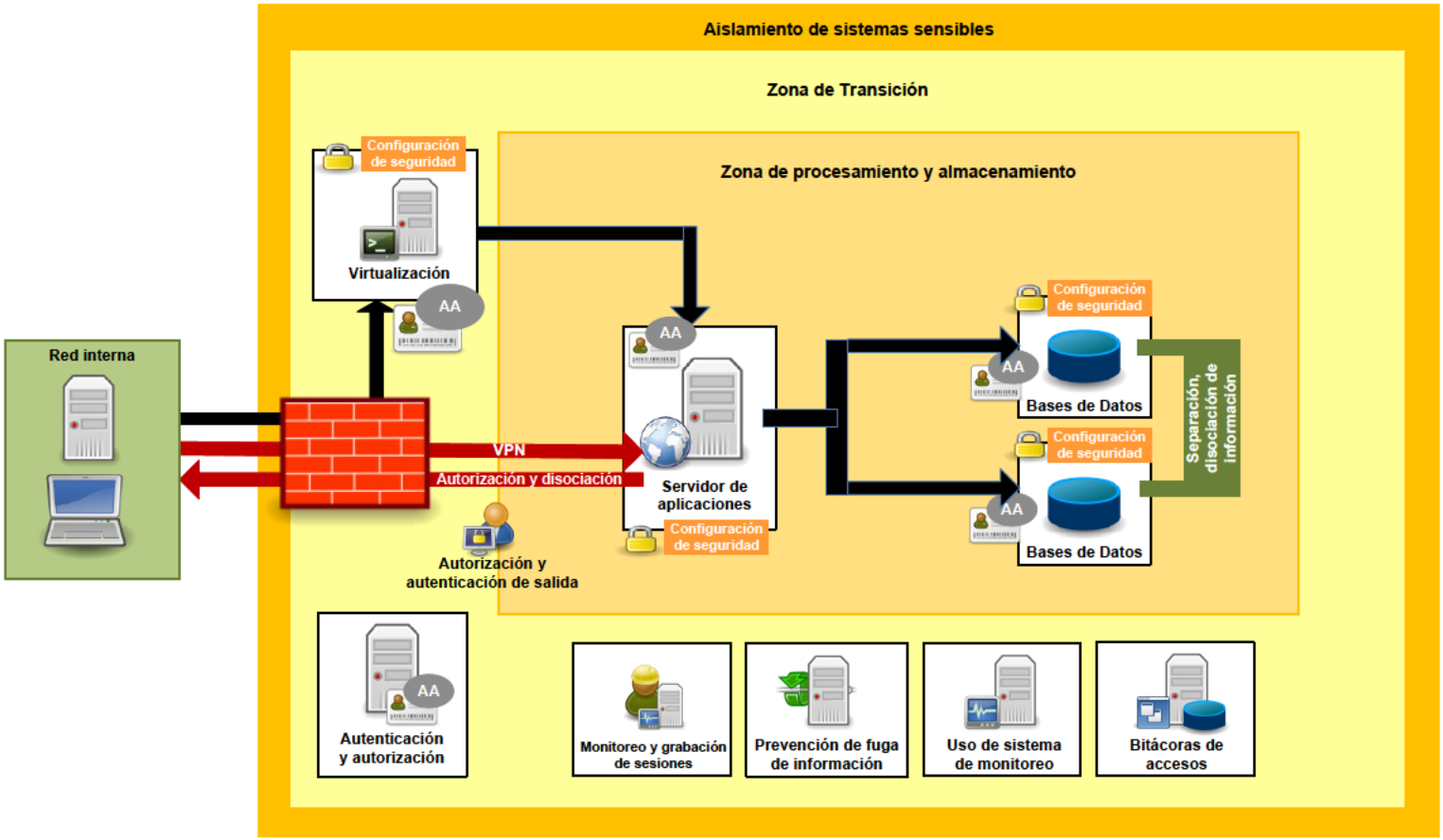


Figura 10. Patrón de control de CF-2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación.	Ninguno	9.2.6
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Se recomienda alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Uso de protocolos seguros Eliminar contraseñas por defecto.	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Se requiere la existencia de una zona de transición en la caja fuerte para evitar que se tenga acceso de forma directa a los datos desde entornos ajenos a la caja fuerte. Considerar los siguientes controles: - Protocolos seguros. - Cifrado del medio. - Autenticación. -Disociación de información cuando los datos salgan de la caja fuerte.	10.8.1
Comercio electrónico: La información involucrada en el comercio electrónico que circule por redes públicas, deberá protegerse de la actividad fraudulenta, divulgación o modificación no autorizada.	Considerar cifrado de los datos ingresados en sitios de comercio electrónico, certificados de seguridad para la transacción.	10.9.1
Transacciones en línea: La información involucrada en transacciones en línea deberá protegerse para impedir su transmisión incompleta, desviación, alteración, divulgación, duplicación o reproducción no autorizada.	Implementar controles de no repudio, considerando cifrado de los datos, certificados de seguridad.	10.9.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario, cambios realizados, equipo origen y destino. Asegurar que se registren las actividades de administración del sistema. Garantizar la generación de estas bitácoras.	10.10.1
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Ninguno	10.10.2
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Ninguno	10.10.3
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP.	10.10.6
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Se debe considerar la autorización de acceso a los datos sensibles por el área de seguridad de la información en cada solicitud de acceso.	11.2.1

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	El área de seguridad debe estar involucrada en el proceso de autorización. Controlar de la cantidad de datos sensibles que puede tratar un usuario autorizado, con el objetivo de evitar que tenga contacto con una gran cantidad de datos o con las bases de datos completas, mediante el control de tablas y campos.	11.2.2
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña de mínimo 12 caracteres.	11.3.1
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	11.3.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.	11.4.1
Autenticación del usuario para las conexiones externas: Se deberá utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	La conexión a los sistemas de información desde cualquier entorno diferente a la caja fuerte para tratar datos personales, debe ser a través de una zona de transición interna, evitando el acceso directo a los datos y por medio de soluciones de red privada virtual que cuenten con métodos robustos de autenticación y cifrado.	11.4.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Identificación de los equipos en la red: La identificación automática de equipo deberá considerarse como un medio de autenticación de conexiones desde lugares y equipos específicos.	Identificación del equipo por medio de dirección MAC o dirección IP.	11.4.3
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Control de enrutamiento de la red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas y los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.	Ninguno	11.4.7
Procedimientos de acceso seguro a los sistemas (log-on): Se debe controlar el acceso a los sistemas operativos, mediante un proceso seguro de inicio de sesión (log-on).	Usar protocolos seguros de autenticación.	11.5.1
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Ninguno	11.5.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Uso de utilidades del sistema: se debe restringir y controlar el uso de programas que tengan la capacidad de sobrepasar los controles de seguridad de los sistemas y de las aplicaciones.	Ninguno	11.5.4
Tiempo de expiración de las sesiones: se deben desactivar las sesiones inactivas después de un periodo de inactividad definido.	Considerar como tiempo de expiración 5 minutos como máximo.	11.5.5
Límite del tiempo de conexión: se deben utilizar restricciones a los tiempos de conexión para proveer seguridad adicional para las aplicaciones de alto riesgo.	Ninguno	11.5.6
Aislamiento de sistemas sensibles: los sistemas sensibles deben tener un entorno informático independiente y aislado.	Este control se ve reflejado en la implementación de la caja fuerte.	11.6.2
Validación de los datos de entrada: Se deben validar los datos de entrada a las aplicaciones para asegurar que los datos son apropiados y correctos.	Ninguno	12.2.1
Integridad de los mensajes: Se deben definir e implantar los controles apropiados para asegurar la autenticidad de los mensajes y para proteger su integridad dentro de las aplicaciones.	Implementar controles de no repudio, considerando cifrado de los datos, certificados de seguridad.	12.2.3
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ninguno	12.3.1
Protección de los datos de prueba de los sistemas: Se debe seleccionar cuidadosamente los datos de prueba y deben ser controlados y protegidos adecuadamente.	Considerar la no utilización de datos de producción en ningún ambiente fuera del operativo.	12.4.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Control de accesos al código fuente: Se debe restringir el acceso al código fuente de los programas.	Ninguno	12.4.3
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno	12.5.4
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1
Separación de la información en diferentes bases de datos e infraestructura.	Separar la información en bases de datos de menor tamaño para disminuir el interés de un tercero. La separación implica que se implemente una autenticación diferente para cada base de datos.	SM.3
Virtualización de equipos y acceso a la información a través de clientes delgados que impidan guardar la información que se accede en el equipo del usuario.	Ninguno	SM.12
En caso de requerir visualizar o tratar datos personales por medio de sistemas de información o ambientes distintos a producción, se deberán establecer mecanismos de enmascaramiento para prevenir el mal uso de los datos personales y sensibles.	Ninguno	SM.20
Monitoreo y grabación del tratamiento de la información sensible que realizan los usuarios.	Ninguno	SM.25

Anexo 5

Análisis de riesgos y análisis de brecha

ID	CCPE-01
Nombre del sistema de tratamiento de datos personales	Actua zac ón de D rector o UNAM
ELABORÓ	R cardo A barrán Romero
Fecha de actualización	15 de Agosto de 2022

Fecha 15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	CCPE-02
Nombre del sistema de tratamiento de datos personales	Administración de los Sitios Web de la CVTT
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

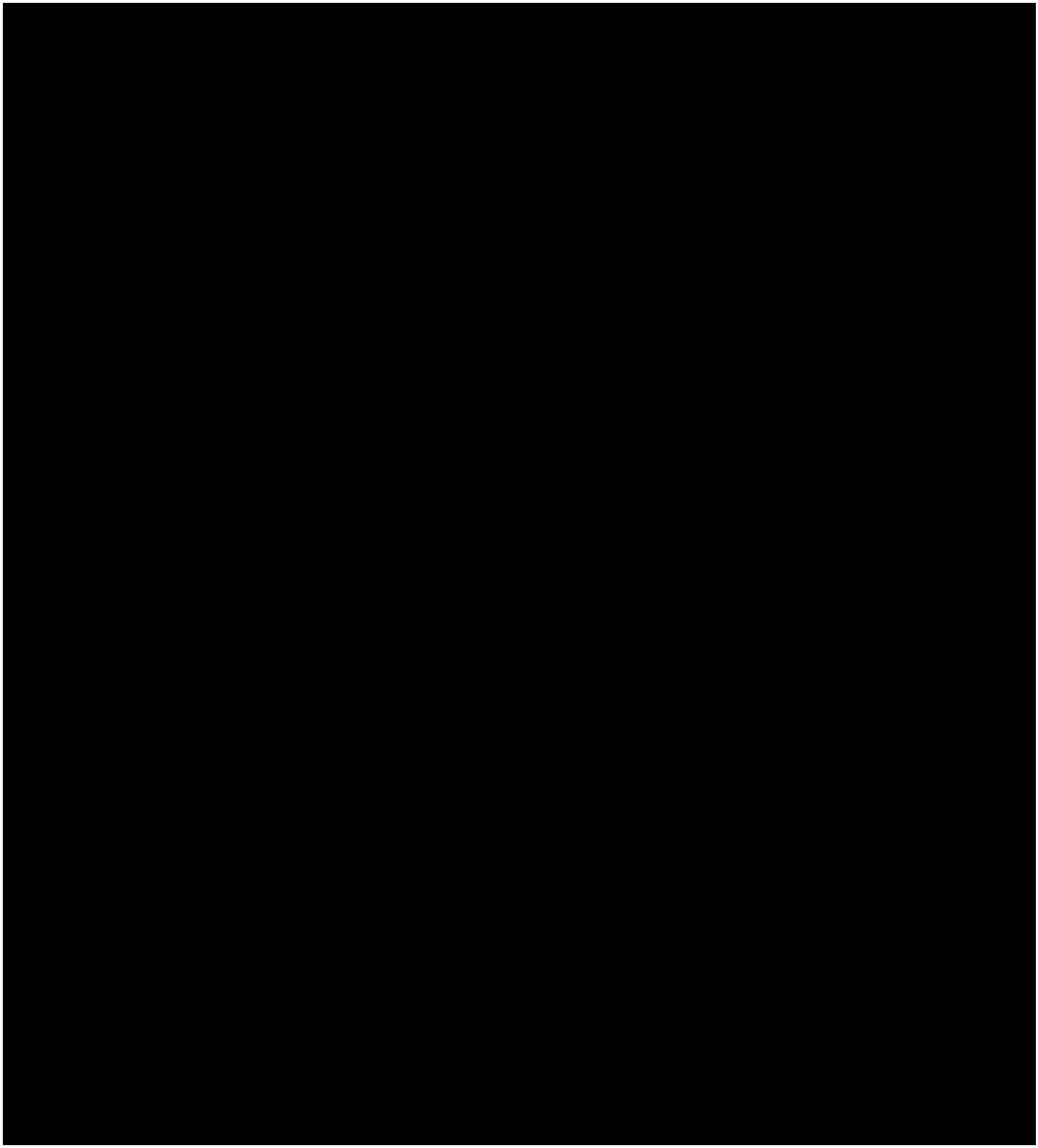
TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

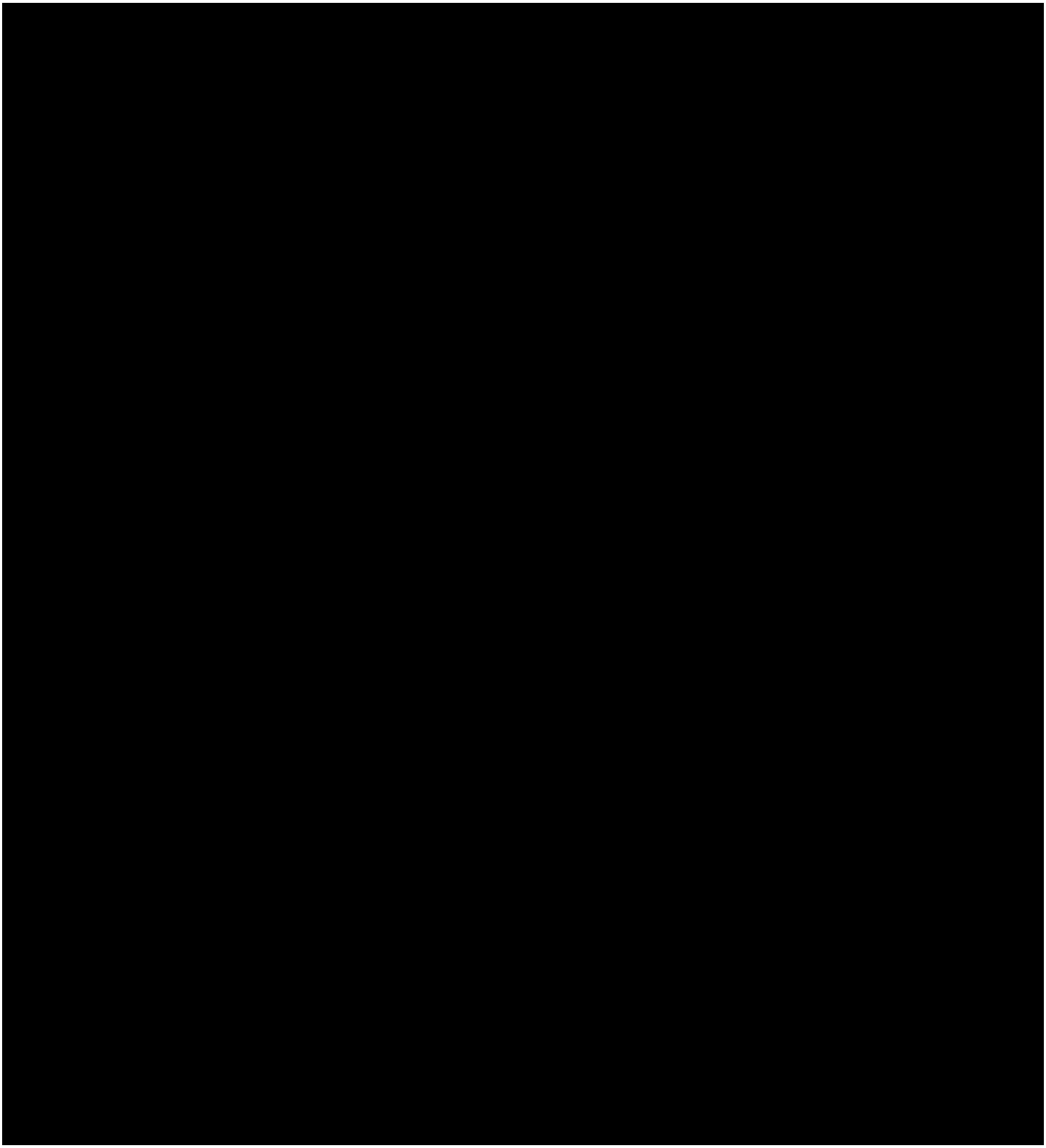
TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	CCPE-03
Nombre del sistema de tratamiento de datos personales	Levantamiento y Procesos de Multimedia
ELABORÓ	Alejandro Arturo Ortega Hernández Alma Rosa García Martínez Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

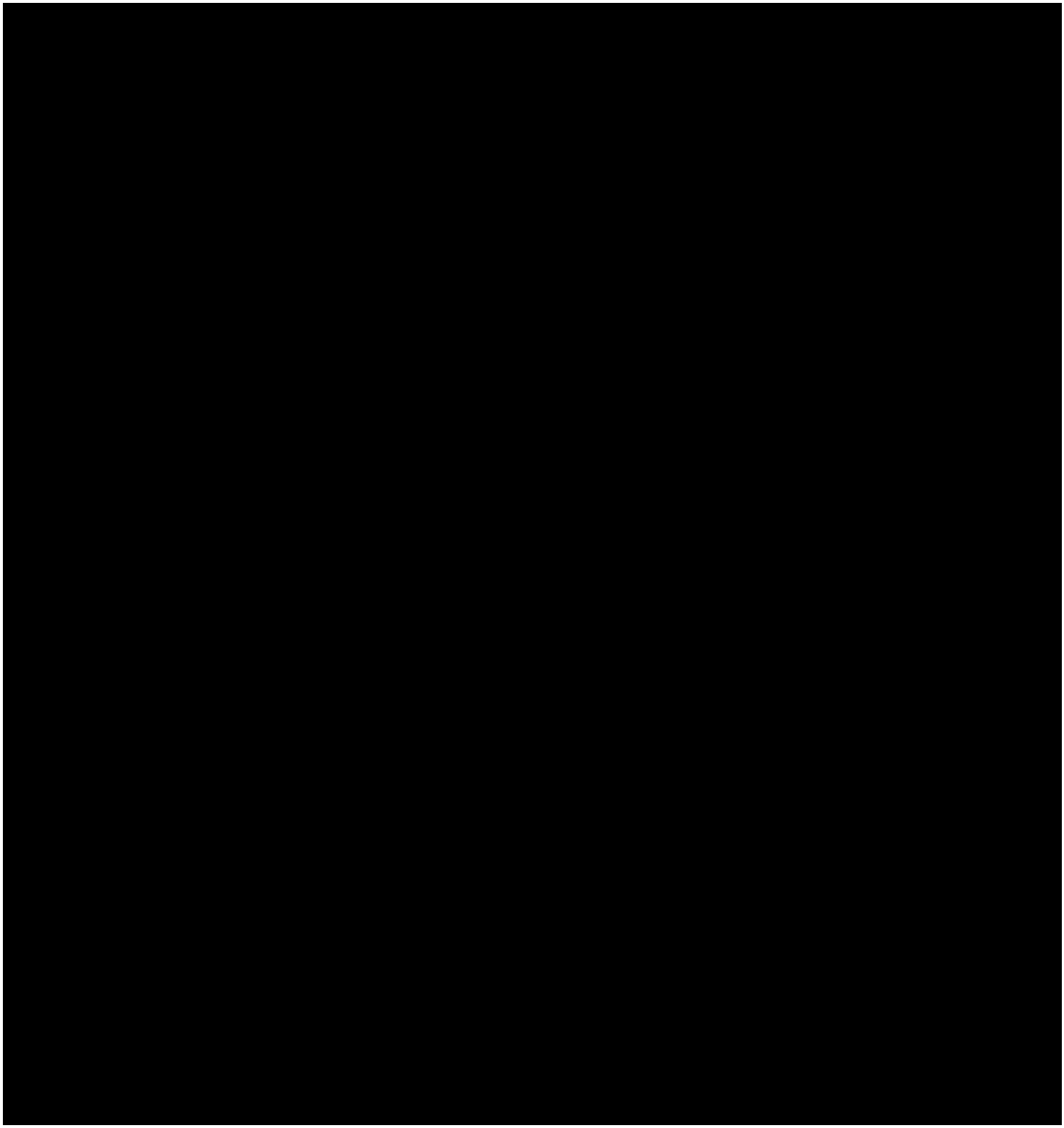
TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DEU-01
Nombre del sistema de tratamiento de datos personales	Talleres de emprendimiento
ELABORÓ	Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

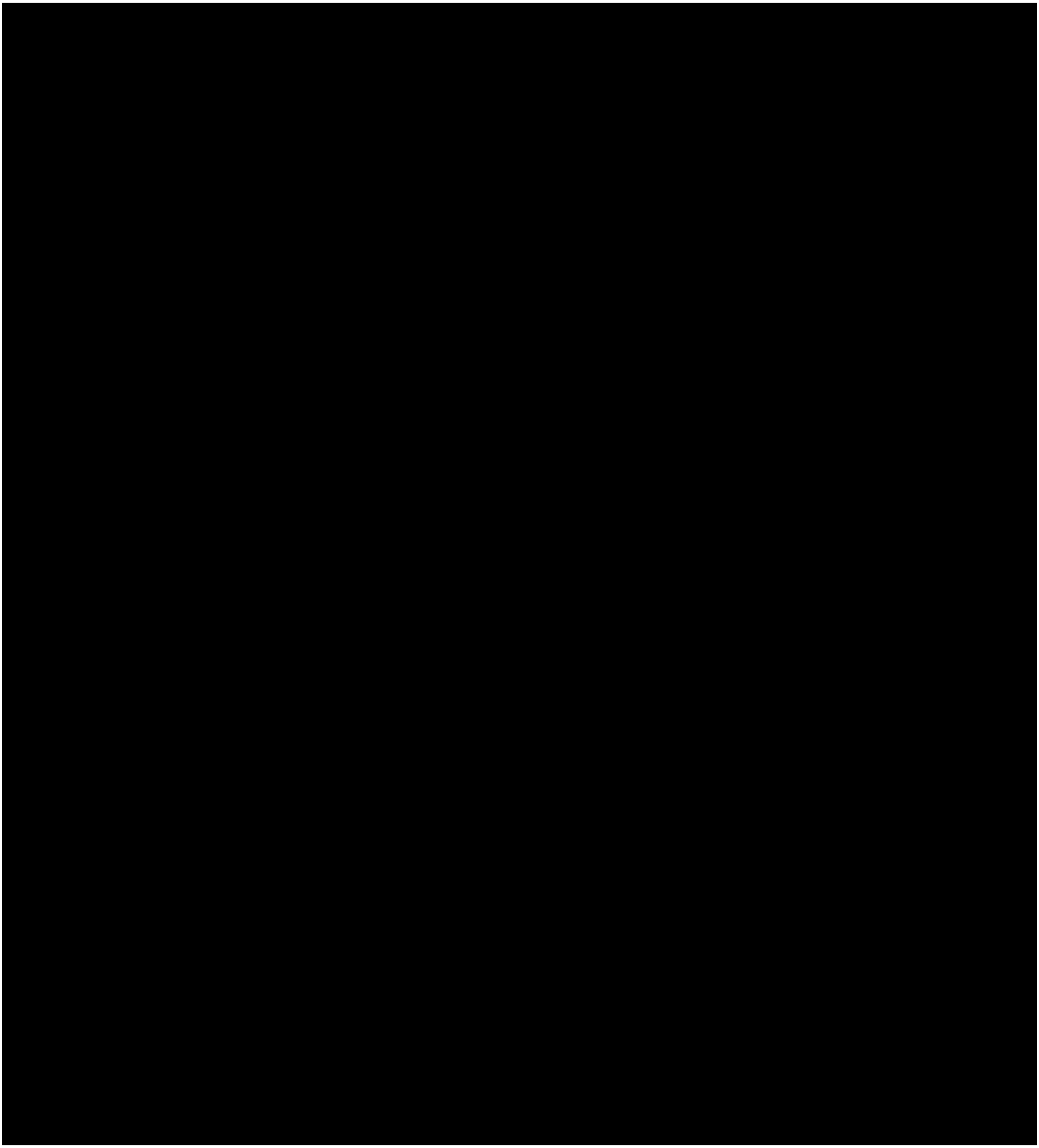
[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

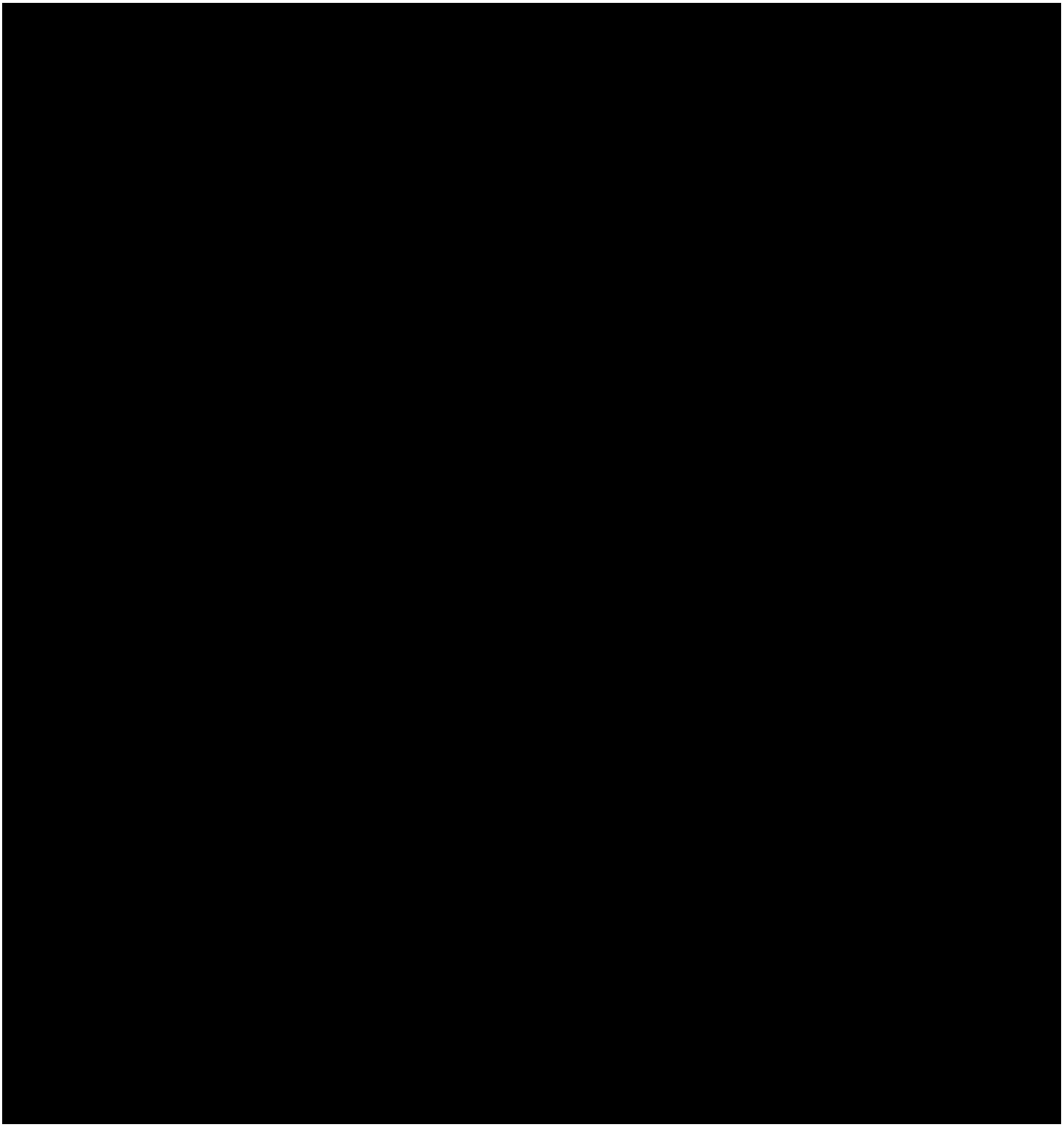
ID	DEU - 02
Nombre del sistema de tratamiento de datos personales	Sistema InnovaUNAM
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



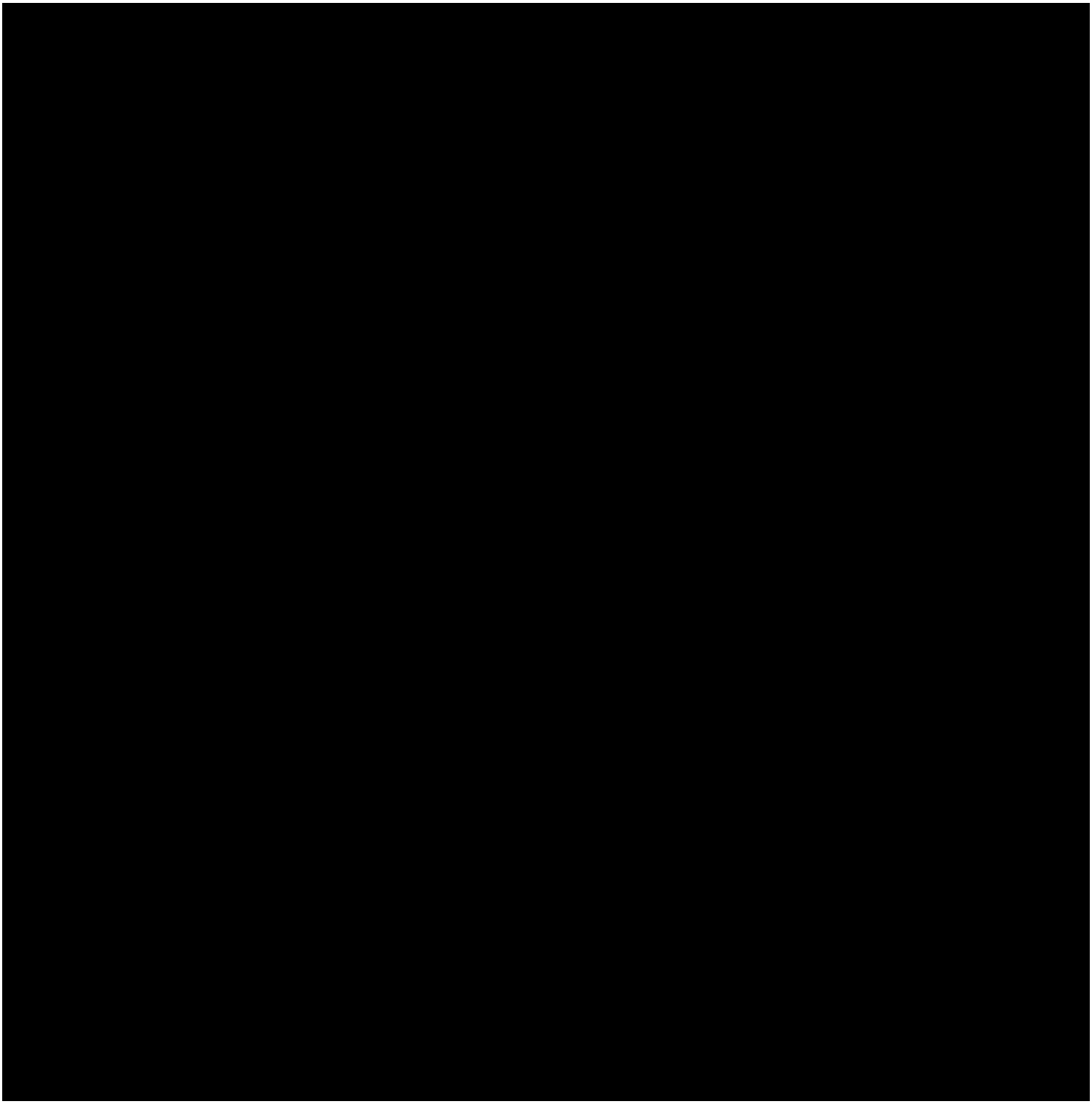
TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DEU-03
Nombre del sistema de tratamiento de datos personales	Incubación de Base Tecnológica
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

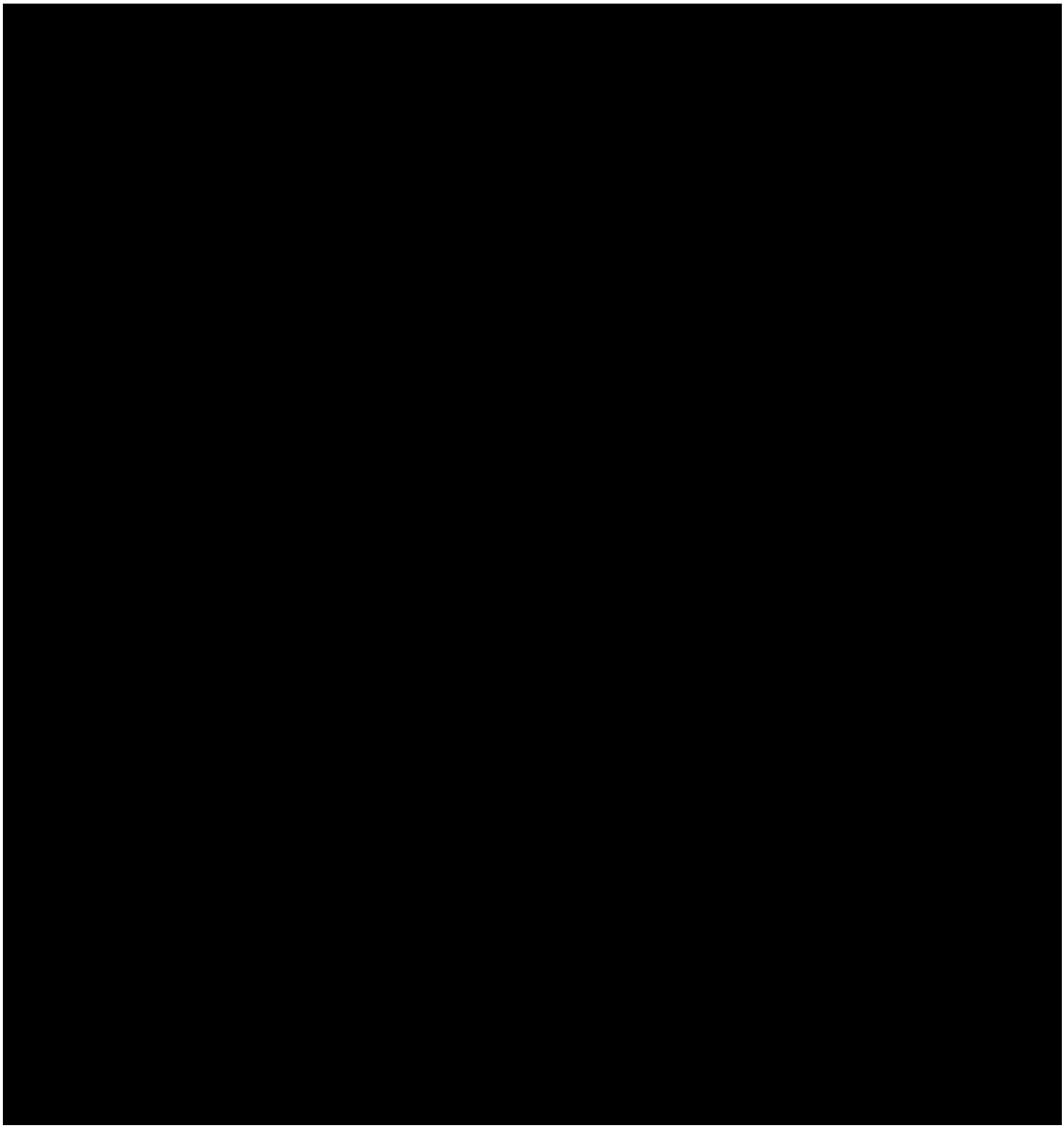
ID	DEU-04
Nombre del sistema de tratamiento de datos personales	Incubación de Empresas Sociales
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

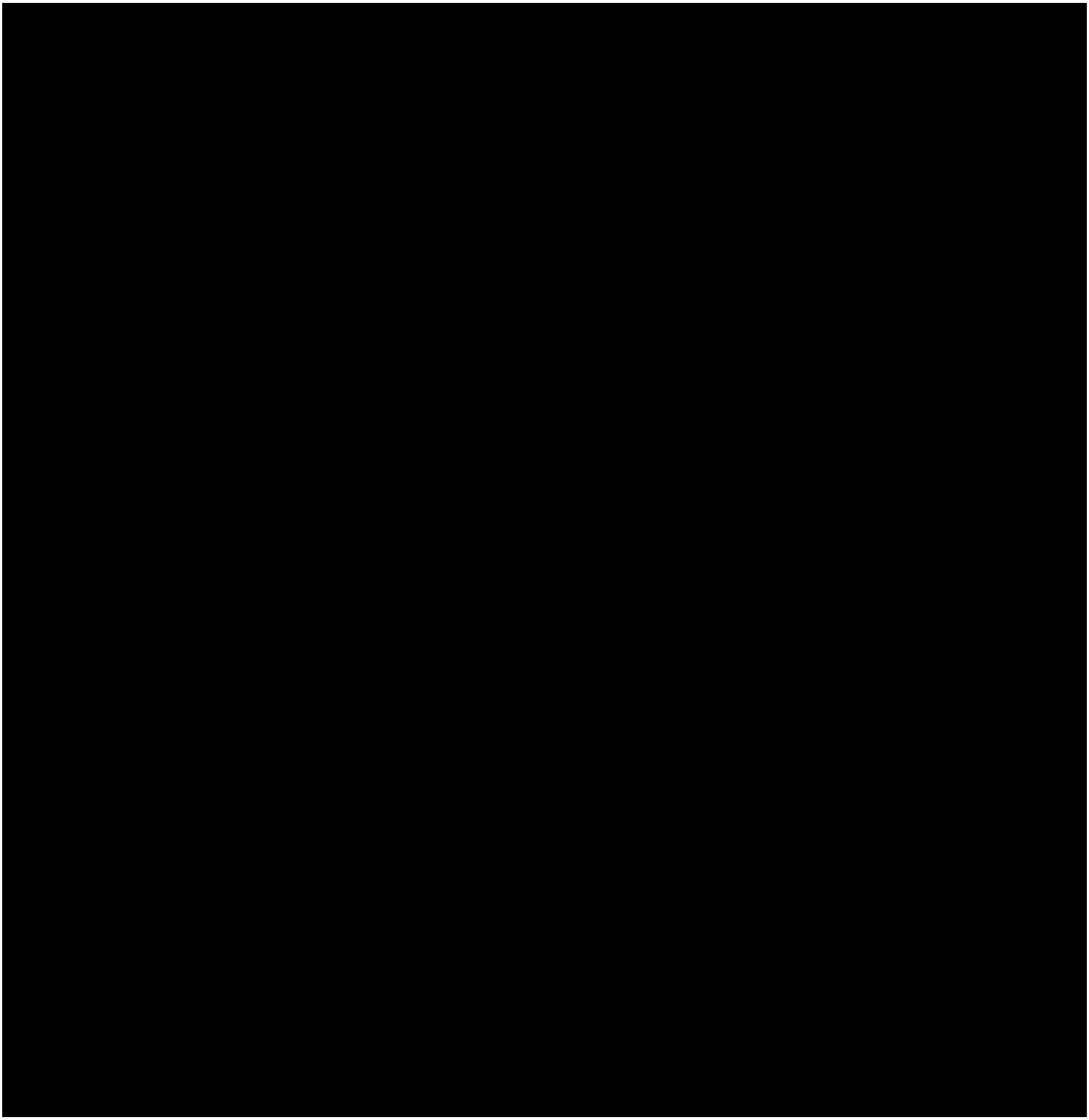
ID	DEU-05
Nombre del sistema de tratamiento de datos personales	Guías para el Emprendimiento Profesional
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

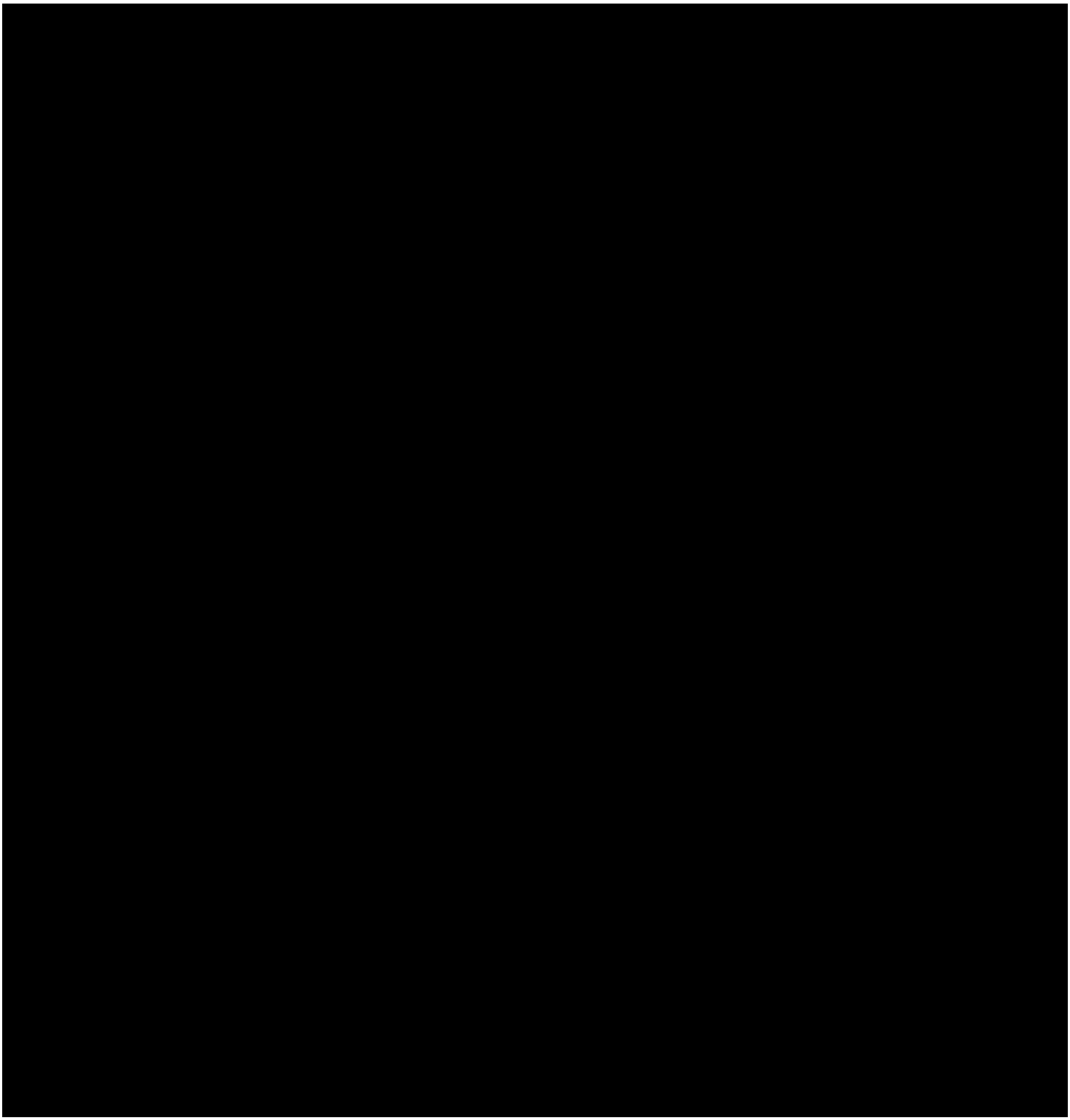
ID	DEU-06
Nombre del sistema de tratamiento de datos personales	Emprende con Santander X y la UNAM
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DITD-01
Nombre del sistema de tratamiento de datos personales	Soporte TIC
ELABORÓ	Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

ID del Documento: IauRQqKMpXUAMN4pU9IKR87b9aCC3mPQL83HFNYePD=

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DITD-02
Nombre del sistema de tratamiento de datos personales	Directorio Interno CVTT
ELABORÓ	Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

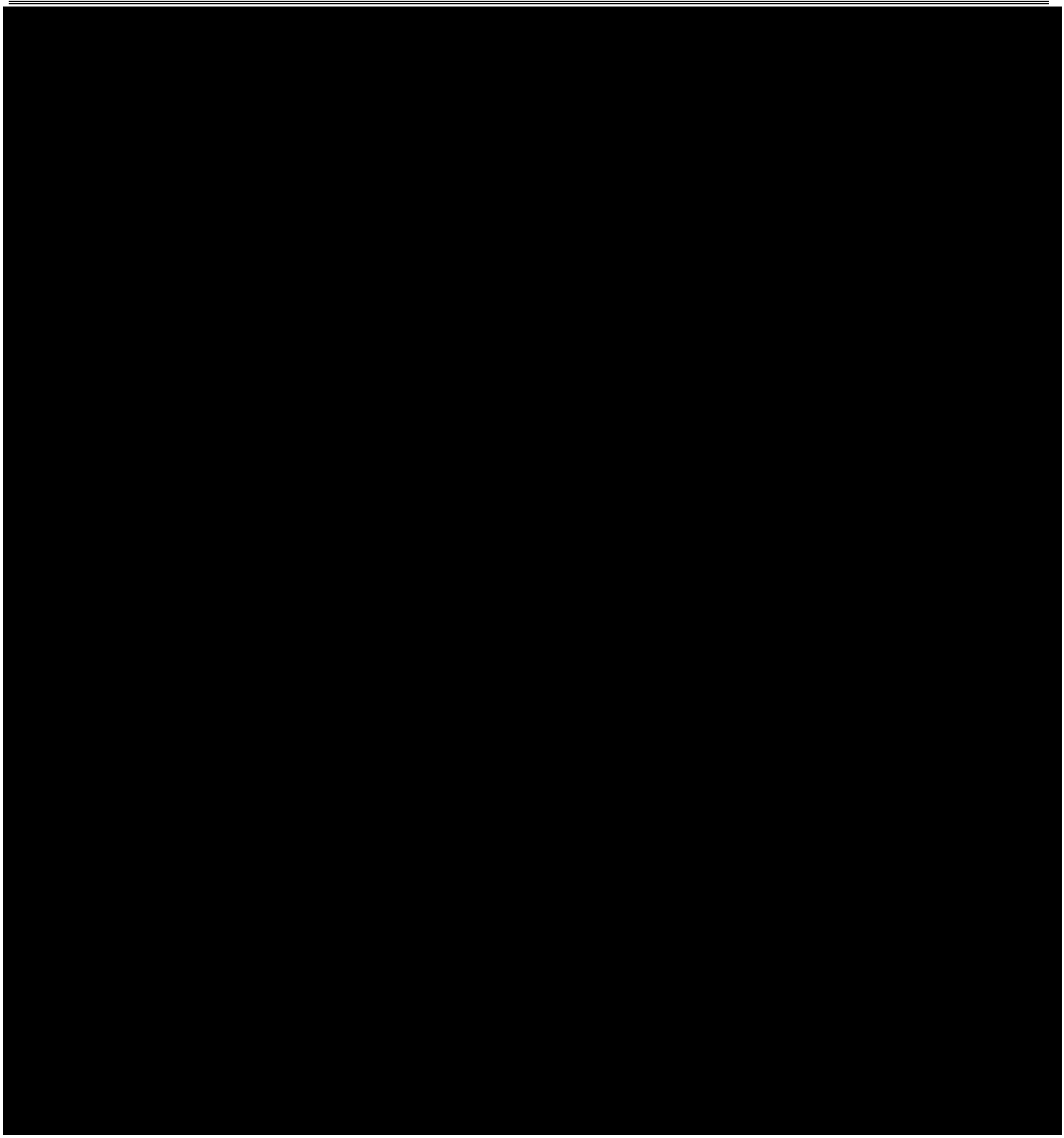
[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

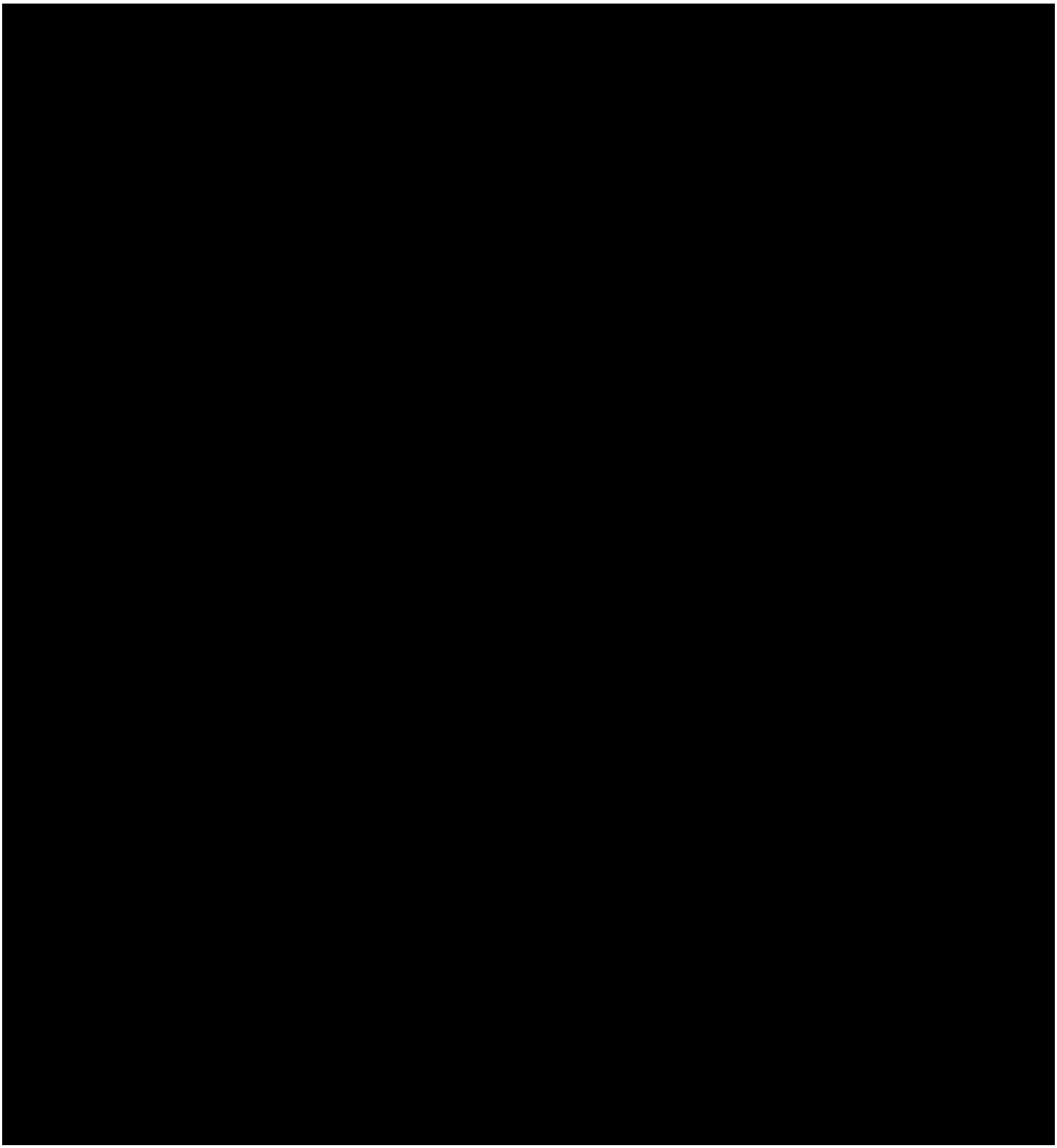
ID	DITD-03
Nombre del sistema de tratamiento de datos personales	Videoconferencia
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



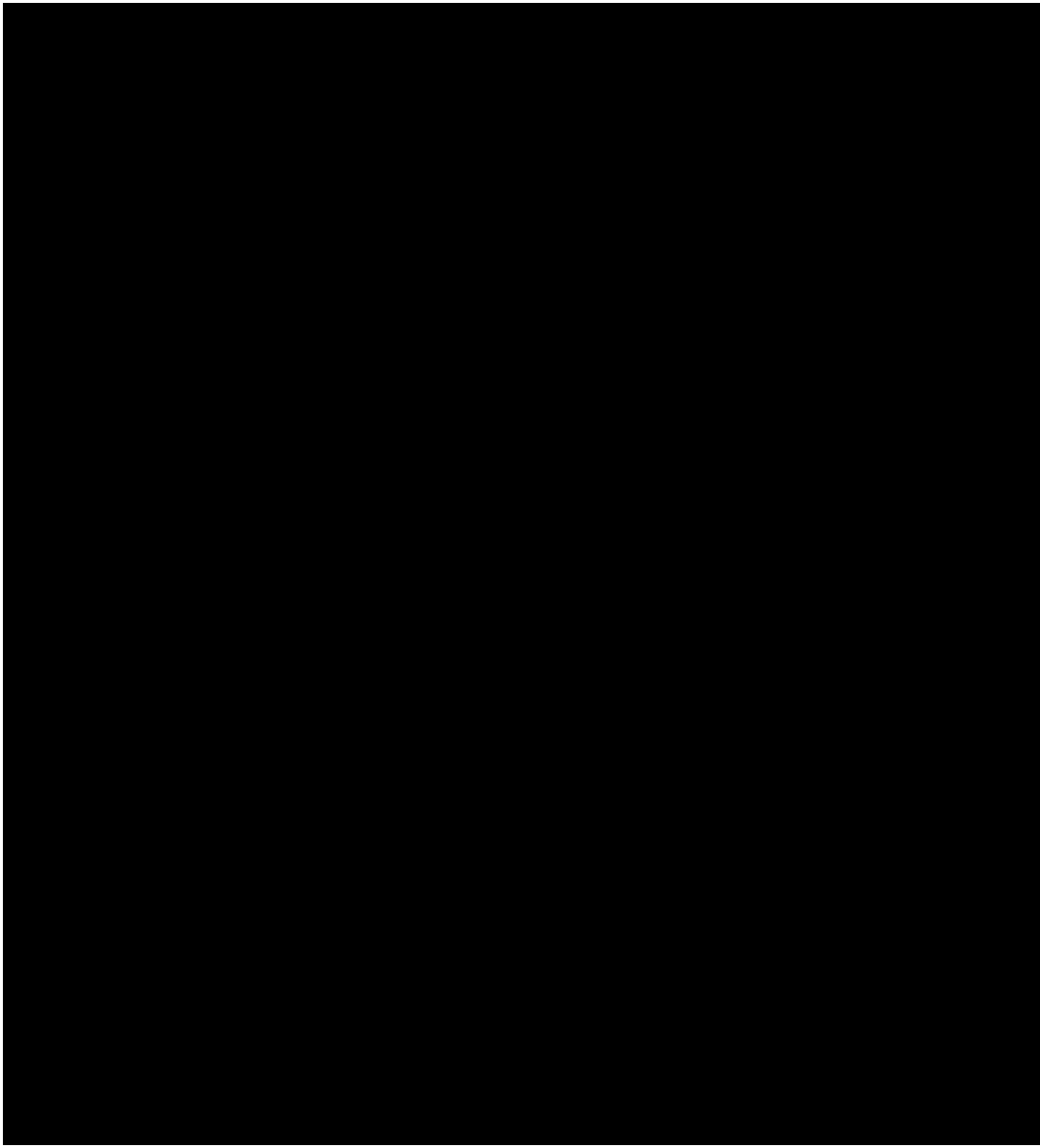
TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DITD-04
Nombre del sistema de tratamiento de datos personales	COGNOS UNAM 2.0
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DITD-05
Nombre del sistema de tratamiento de datos personales	Gestion convocatorias de la CVTT
ELABORÓ	Alma Rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID del Documento: IauRQqKMpXUAMN4pU9lKR87bl9aCC3mPQL83HFNYePO=

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DITD-06
Nombre del sistema de tratamiento de datos personales	Recopilación de información y notificaciones de la CVTT
ELABORÓ	Alma Rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DITD-07
Nombre del sistema de tratamiento de datos personales	Gestion convocatorias Consorcio UNAM TEC
ELABORÓ	Alejandro Arturo Ortega Hernández Alma Rosa García Martínez Ricardo Albarrán Romero
Fecha de actualización	12 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

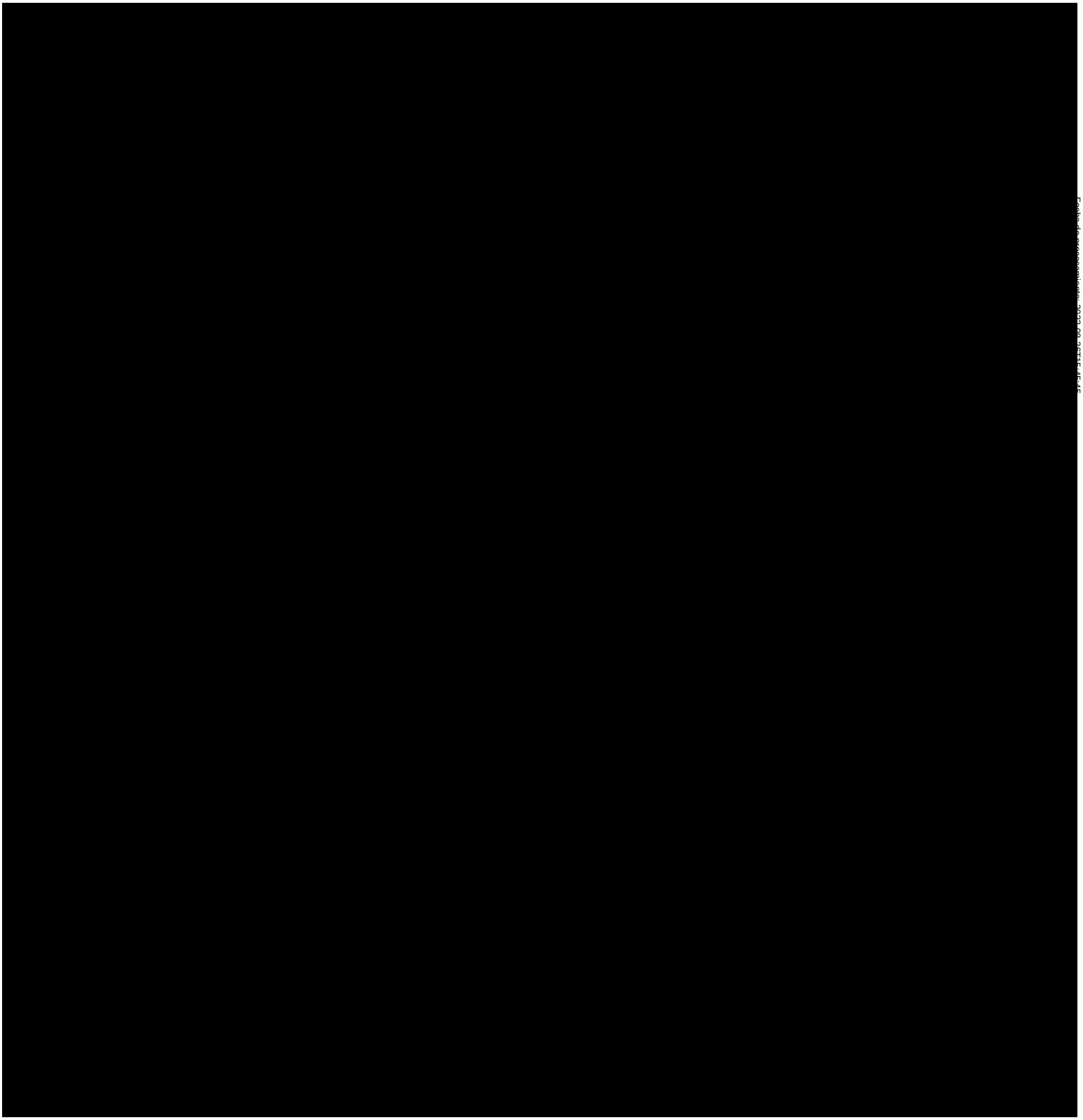
TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DJ-01
Nombre del sistema de tratamiento de datos personales	Instrumentos consensuales
ELABORÓ	Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DST-01
Nombre del sistema de tratamiento de datos personales	Vinculación Interna
ELABORÓ	Alma Rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DST-02
Nombre del sistema de tratamiento de datos personales	Vinculación Externa
ELABORÓ	Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DTT-01
Nombre del sistema de tratamiento de datos personales	Proceso de Transferencia Tecnológica
ELABORÓ	Alma Rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DTT-02
Nombre del sistema de tratamiento de datos personales	Generación de expedientes para presentación de solicitud de protección en materia de Propiedad Intelectual
ELABORÓ	Alejandro Arturo Ortega Hernández Alma Rosa García Martínez Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID del Documento: IauRQqKMpXUAMN4pU9lKR87bl9aCC3mPQL83HFNYeP0=

[redacted]

ID del Documento: IauRQqKMpXUAMN4pU9IKR87b9aCC3mPQL83HFNYePl0=

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

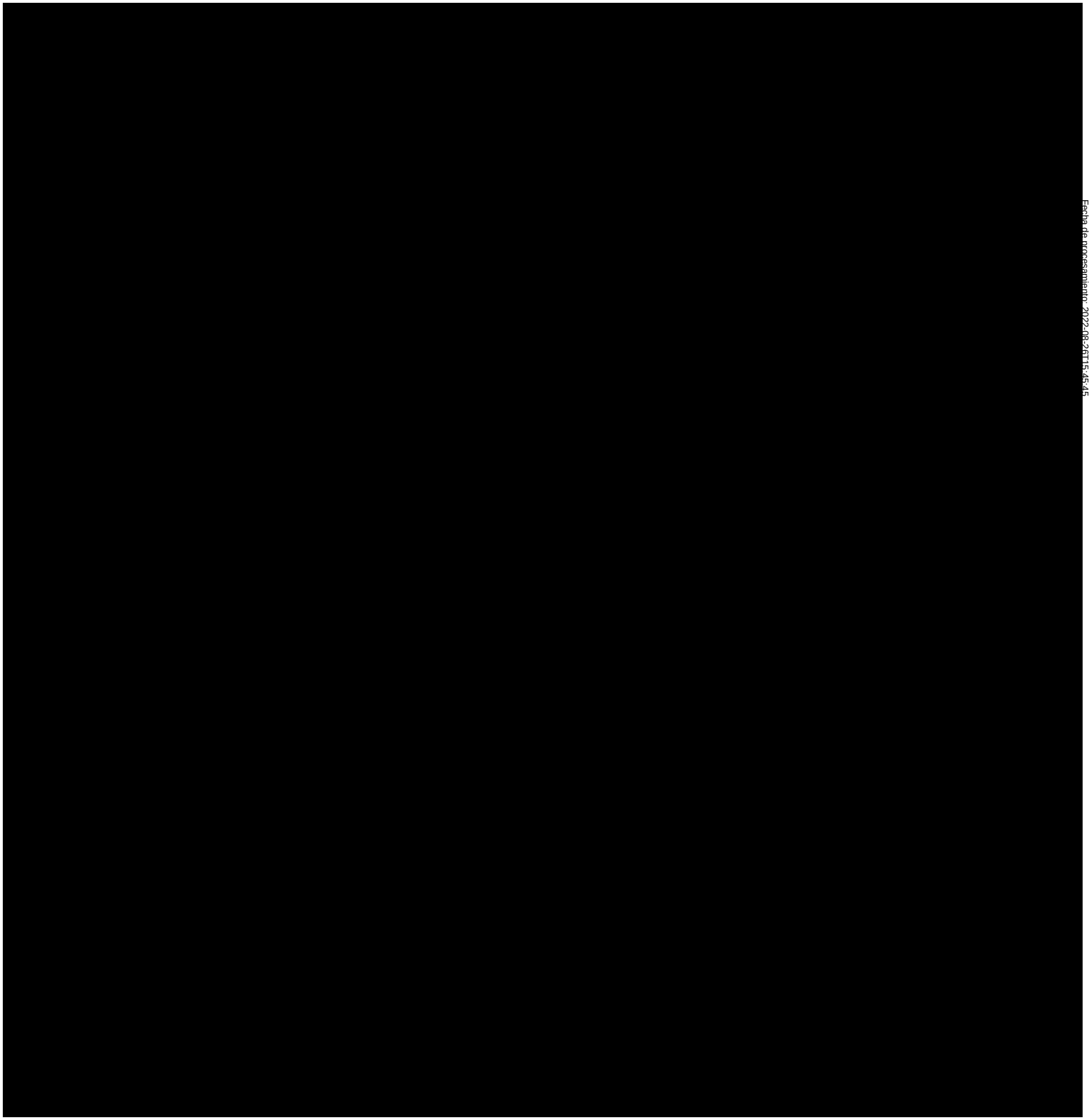
[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	DTT-03
Nombre del sistema de tratamiento de datos personales	Contactos DTT
ELABORÓ	Ricardo Albarrán Romero
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	UA-01
Nombre del sistema de tratamiento de datos personales	Gestión de Personal contratado por estructura de la CVTT
ELABORÓ	Alma rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	UA-02
Nombre del sistema de tratamiento de datos personales	Gestión de contratos por servicios profesionales de la CVTT
ELABORÓ	Alma Rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

ID	UA-03
Nombre del sistema de tratamiento de datos personales	Alta de proveedores
ELABORÓ	Alma Rosa García Martínez
Fecha de actualización	15 de Agosto de 2022

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

ID del Documento: IauRQqKMpXUAMN4pU9IKR87b9aCC3mPQL83HFNYePl0=

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE ANÁLISIS DE RIESGOS Y ANÁLISIS DE BRECHA YA QUE CONTIENE INFORMACIÓN SOBRE SOBRE LAS VULNERABILIDADES Y SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

Anexo 6

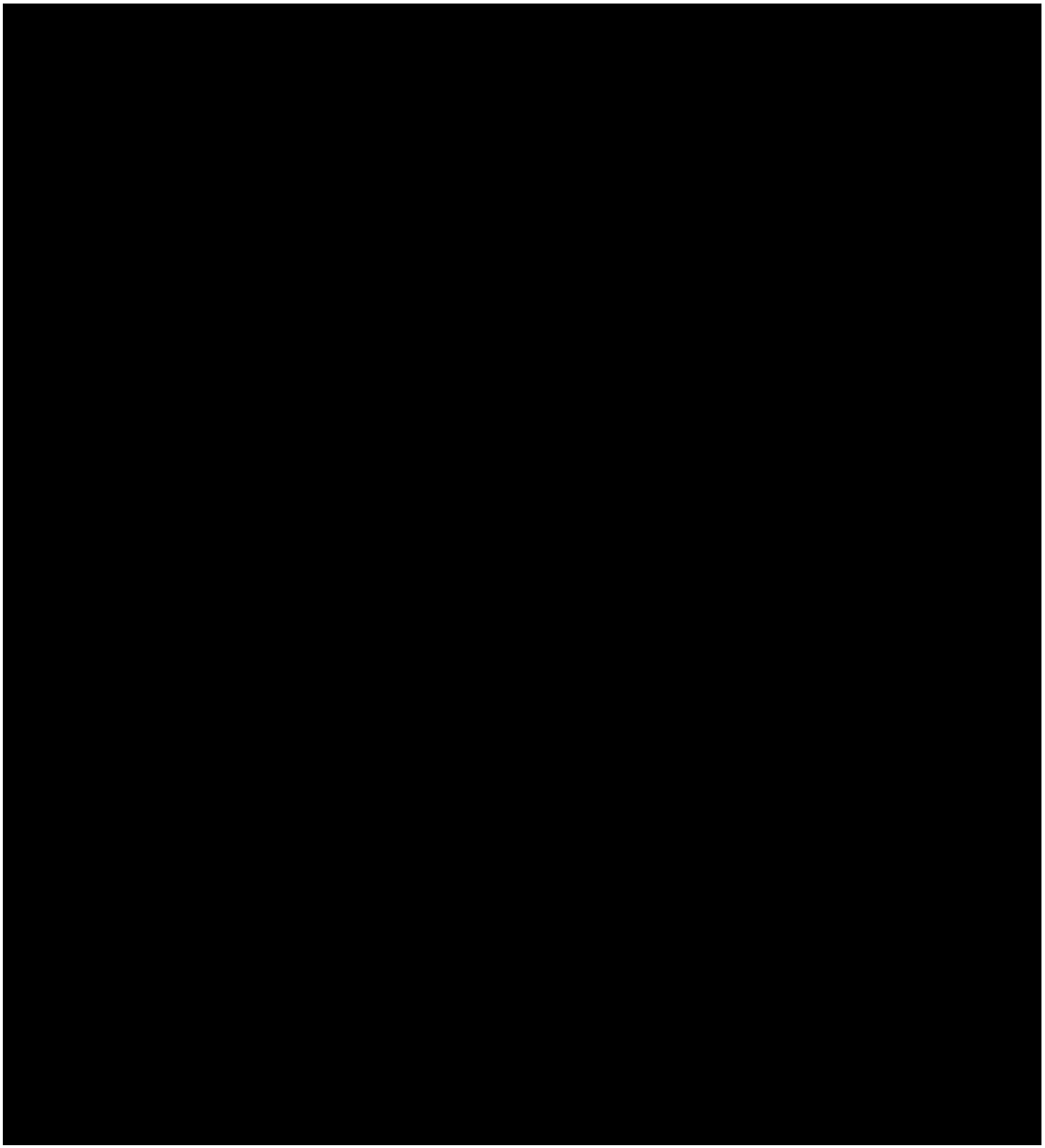
Plan de Trabajo

ID	CVTT-SGS-DP-PT
Nombre	Plan de trabajo
ELABORÓ	Alma Rosa García Martínez Alejandro Arturo Ortega Hernández
Fecha de actualización	15 de agosto de 2022

TESTO ESTE APARTADO DE PLAN DE TRABAJO YA QUE CONTIENE INFORMACIÓN SOBRE CONTROLES DE SEGURIDAD A IMPLEMENTAR DE ACUERDO CON EL RESULTADO DEL ANÁLISIS DE RIESGOS Y DEL ANÁLISIS DE BRECHA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE PLAN DE TRABAJO YA QUE CONTIENE INFORMACIÓN SOBRE CONTROLES DE SEGURIDAD A IMPLEMENTAR DE ACUERDO CON EL RESULTADO DEL ANÁLISIS DE RIESGOS Y DEL ANÁLISIS DE BRECHA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



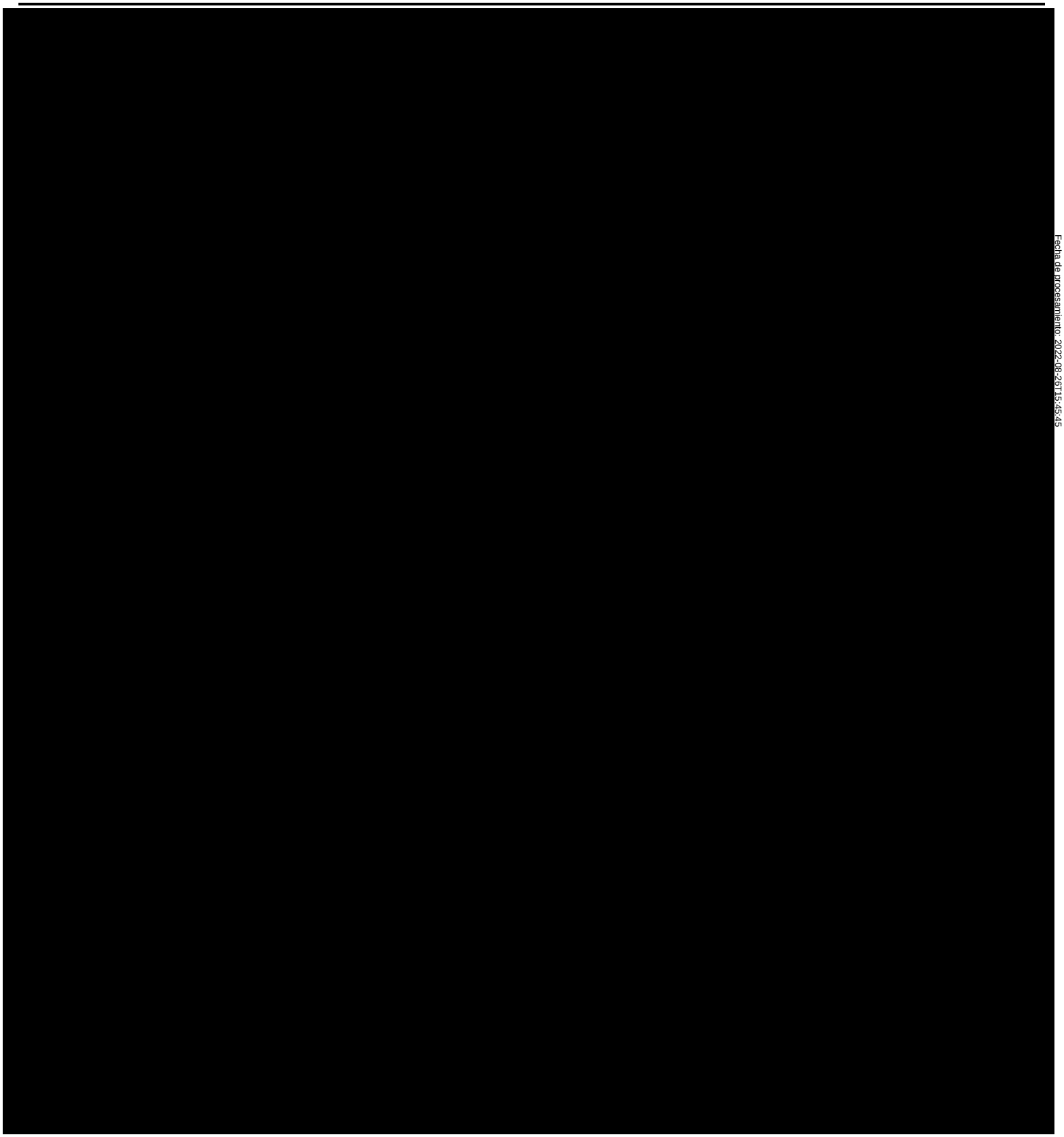
TESTO ESTE APARTADO DE PLAN DE TRABAJO YA QUE CONTIENE INFORMACIÓN SOBRE CONTROLES DE SEGURIDAD A IMPLEMENTAR DE ACUERDO CON EL RESULTADO DEL ANÁLISIS DE RIESGOS Y DEL ANÁLISIS DE BRECHA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE PLAN DE TRABAJO YA QUE CONTIENE INFORMACIÓN SOBRE CONTROLES DE SEGURIDAD A IMPLEMENTAR DE ACUERDO CON EL RESULTADO DEL ANÁLISIS DE RIESGOS Y DEL ANÁLISIS DE BRECHA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.

[redacted]

TESTO ESTE APARTADO DE PLAN DE TRABAJO YA QUE CONTIENE INFORMACIÓN SOBRE CONTROLES DE SEGURIDAD A IMPLEMENTAR DE ACUERDO CON EL RESULTADO DEL ANÁLISIS DE RIESGOS Y DEL ANÁLISIS DE BRECHA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.



TESTO ESTE APARTADO DE PLAN DE TRABAJO YA QUE CONTIENE INFORMACIÓN SOBRE CONTROLES DE SEGURIDAD A IMPLEMENTAR DE ACUERDO CON EL RESULTADO DEL ANÁLISIS DE RIESGOS Y DEL ANÁLISIS DE BRECHA POR UN PERIODO DE CINCO AÑOS, POR TRATARSE DE INFORMACIÓN RESERVADA DE CONFORMIDAD CON EL ARTÍCULO 110 FR.VII DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PUBLICA Y DE CONFORMIDAD CON LA RESOLUCIÓN CTUNAM/529/2022 DEL COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, DE FECHA 24 DE AGOSTO DE 2022.