



TRIBUNAL UNIVERSITARIO



Documento de Seguridad de Datos Personales

# DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES



## INTRODUCCIÓN

El presente documento de seguridad tiene por objetivo plantear las medidas de seguridad aplicables al sistema de datos personales para este órgano colegiado, asegurando con ello la integridad, confidencialidad y disponibilidad de los datos personales que posee en el ejercicio de sus atribuciones.

Con relación a las actividades que se desarrollan, el Tribunal Universitario cuenta con un sistema de datos personales denominado "Sistema de Gestión Documental de la Secretaría del Tribunal Universitario", a través de cual se tiene un control y seguimiento a la documentación que se recibe con motivo de las remisiones que realizan las autoridades competentes a este órgano colegiado.

En este documento se da cuenta del mencionado sistema, de tipo de datos personales que contiene, se designa a los responsables y usuarios del sistema, estableciendo medidas técnicas, administrativas y físicas para proteger dicha información.

Cabe precisar que, es un documento que se podrá perfeccionar conforme se vayan cumpliendo las tareas trazadas en el mismo, se hagan verificaciones de medidas implementadas o se cree o modifique sustancialmente el sistema de tratamiento de datos personales.



SISTEMA DE GESTIÓN DOCUMENTAL DE LA SECRETARÍA DEL TRIBUNAL UNIVERSITARIO

Contenido

1. Inventario de Sistemas de Tratamiento de Datos Personales
2. Estructura y descripción de los sistemas de tratamiento de datos personales
3. Análisis de riesgo
4. Análisis de brecha
5. Plan de trabajo
6. Medidas de seguridad implementadas
7. Mecanismos de monitoreo y revisión de las medidas de seguridad
8. Programa específico de capacitación
9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales
11. Aprobación del documento de seguridad



# **1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**



Sistema de Gestión Documental de la Secretaría del Tribunal Universitario

1. Inventario de Sistemas de Tratamiento de Datos Personales

<b>Secretaría del Tribunal Universitario</b>	
<b>Identificador único*</b>	SecTU
<b>(Nombre del sistema A1) *</b>	<b><u>Sistema de Gestión Documental de la Secretaría del Tribunal Universitario</u></b>
<b>Datos personales (sensibles o no) contenidos en el sistema*:</b>	<ul style="list-style-type: none"> <li>• El nombre de las personas que intervienen en el procedimiento.</li> <li>• Información académica de las personas que intervienen en el procedimiento.</li> <li>• Clave Única de Registro de Población de las personas que intervienen en el procedimiento.</li> <li>• Registro Federal de Contribuyentes de las personas que intervienen en el procedimiento.</li> <li>• Firmas de las personas que intervienen en el procedimiento.</li> <li>• Domicilio particular de las personas que intervienen en el procedimiento.</li> <li>• Teléfonos particulares, fijos y de celular de las personas que intervienen en el procedimiento.</li> <li>• Direcciones electrónicas personales, correos electrónicos particulares y datos de redes sociales particulares.</li> <li>• Número de seguridad social.</li> <li>• Fecha de nacimiento.</li> <li>• Edad.</li> <li>• Sexo.</li> <li>• Fotografías.</li> <li>• Número de cuenta del remitido, de los afectados, testigos y otras personas que sean llamados a participar en el procedimiento.</li> <li>• Historial académico del remitido, de los afectados, testigos y otras personas que sean llamados a participar en el procedimiento.</li> </ul>
<b>Responsable*:</b>	Secretaría del Tribunal Universitario



## Documento de Seguridad de Datos Personales

<b>Nombre<sup>1</sup>:</b>	Janet Becerra Ramos
<b>Cargo*:</b>	Secretaria Suplente del Tribunal Universitario
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Suplir al Secretario del Tribunal Universitario en la atención de los asuntos y trámites que son de su competencia.</li><li>• Acceder, consultar y en su caso remitir la documentación recabada con motivo de los asuntos que en materia disciplinaria universitaria le sean turnados en el ámbito de su competencia, lo anterior a través del Sistema de Gestión Documental. Cuenta con voz, pero no voto.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p> <p>Asignar el área física para el resguardo de los expedientes físicos que contienen datos personales.</p> <p>Concentrar e integrar la base de datos del Tribunal Universitario en que se contienen datos personales.</p> <p>Supervisar el espacio físico y el mobiliario destinados al resguardo de los expedientes en donde se pudieran contener datos personales.</p> <p>Emitir de manera inmediata el informe correspondiente al Responsable de Seguridad de Datos Personales sobre cualquier incidente que se presente en el acceso, resguardo, consulta o transmisión de los datos personales, y simultáneamente hacer el registro correspondiente.</p>

<sup>1</sup> **Responsable del Sistema de Datos Personales:** Persona funcionario universitario que decide sobre el tratamiento de los datos personales, su finalidad, la protección y las medidas de seguridad de estos.



## Documento de Seguridad de Datos Personales

Encargados:	
(Nombre del Encargado 1*)	NO aplica ya que no se cuenta con contratos suscritos con terceros.
Cargo*:	
Funciones*:	
Obligaciones*:	
Usuarios:	
(Nombre del Usuario 1*)	Dr. José Maximo Carvajal Contreras
Cargo*:	Presidente del Tribunal Universitario
Funciones*:	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario.</li><li>• Cuenta con voz y voto. En caso de empate en los votos de las resoluciones emitidas por el Tribunal Universitario en el marco de sus atribuciones, cuenta con voto de calidad.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental de este órgano colegiado.</li><li>• Emitir en el ámbito de sus atribuciones la documentación necesaria relacionada con los procedimientos disciplinarios de los que conoce el Tribunal.</li><li>• Instruir al personal asignado al Tribunal Universitario de no proporcionar información a personas no autorizadas o no consideradas como usuarias.</li></ul>
Obligaciones*:	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>



## Documento de Seguridad de Datos Personales

<b>(Nombre del Usuario 2*)</b>	Mtro. Hugo Alejandro Concha Cantú
<b>Cargo*:</b>	Secretario del Tribunal Universitario
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Coordina al personal operativo del Tribunal Universitario durante las diligencias de trámite de los asuntos. Cuenta con voz, pero no voto.</li><li>• Acceder, consultar y turnar al personal operativo del Colegiado por conducto de su Suplente los asuntos recibidos en materia de disciplina universitaria, lo anterior a través del Sistema de Gestión Documental de este órgano colegiado.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 3*)</b>	Mtra. Ana Beatriz Castrejón Díaz.
<b>Cargo*:</b>	Vocal permanente
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario. Cuenta con voz y voto.</li><li>• Acceder, consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p>





## Documento de Seguridad de Datos Personales

	<p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 4*)</b>	Dra. María Patricia Kurczyn Villalobos.
<b>Cargo*:</b>	Vocal permanente
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario. Cuenta con voz y voto.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 5*)</b>	Lic. Miguel Mejía Sánchez
<b>Cargo*:</b>	Vocal permanente
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario. Cuenta con voz y voto.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p>



## Documento de Seguridad de Datos Personales

	<p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 6*)</b>	Abel Velázquez Cuevas
<b>Cargo*:</b>	Coordinador
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 7*)</b>	Irvin Javier Espinosa Gutiérrez
<b>Cargo*:</b>	Jefe de Departamento



Documento de Seguridad de Datos Personales

<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li> <li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li> </ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 8*)</b>	Brenda Cortés León
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li> <li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li> </ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos</p>



Documento de Seguridad de Datos Personales

	<p>personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 9*)</b>	Gustavo Brando Alonso Carrillo
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p>



Documento de Seguridad de Datos Personales

	<p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 10*)</b>	Laura Angélica Cruz Torres
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p>



## Documento de Seguridad de Datos Personales

	Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.
(Nombre del Usuario 11*)	Eduardo Vaca Cerón
Cargo*:	Jefe de Departamento
Funciones*:	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
Obligaciones*:	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
(Nombre del Usuario 12*)	Adriana Cruz Hernández
Cargo*:	Jefe de Departamento
Funciones*:	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión</li></ul>



Documento de Seguridad de Datos Personales

	<p>de Honor.</p> <ul style="list-style-type: none"> <li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li> </ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 13*)</b>	Alejandra Madrigal Rivera
<b>Cargo*:</b>	Abogada Auxiliar
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li> </ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p>



## Documento de Seguridad de Datos Personales

	<p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 14*)</b>	Carolina Arellano Segoviano
<b>Cargo*:</b>	Asistente Ejecutiva
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li><li>• Guardia y custodia del archivo del Tribunal Universitario y de su base de datos.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p> <p>Asignar el área física para el resguardo de los expedientes físicos que contienen datos personales.</p> <p>Concentrar e integrar la base de datos del Tribunal Universitario en que se contienen datos personales.</p> <p>Supervisar el espacio físico y el mobiliario destinados al resguardo de los expedientes en donde se pudieran contener datos personales.</p> <p>Vigilar que durante el desempeño de sus funciones, en el espacio físico destinado para el resguardo de los datos personales, no tengan acceso a ellos personas no autorizadas.</p>

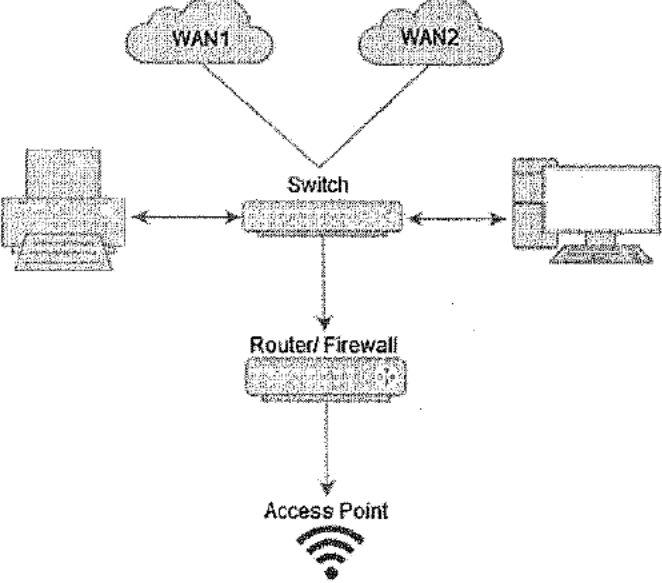




## **2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**



## 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Tribunal Universitario	
<b>Identificador único™</b>	SecTU
<b>(Nombre del sistema A1*)</b>	Sistema de Gestión Documental de la Secretaría del Tribunal Universitario
<b>Tipo de soporte:</b>	Físico y electrónico
<b>Descripción:</b>	Registro de datos contenida en una hoja de cálculo que contiene información esencial de los expedientes tramitados por el Tribunal Universitario y archivo físico de los expedientes tramitados por el Tribunal Universitario.
<b>Características del lugar donde se resguardan los soportes:</b>	<p>Alojamiento local en equipo de cómputo asegurado con antivirus y firewall perimetral, asignada a la titular de la Oficialía de Partes del Tribunal Universitario.</p>  <p>Figura 1. Diagrama de la arquitectura de seguridad.</p>



### **3. ANÁLISIS DE RIESGOS**



3. ANÁLISIS DE RIESGOS

Tribunal Universitario	
Identificador único*	<u>SecTU</u>
(Nombre del sistema A1)*	<u>Sistema de Gestión Documental de la Secretaría del Tribunal Universitario</u>

Riesgos técnicos		
Riesgo*	Impacto*	Mitigación*



Documento de Seguridad de Datos Personales

Riesgos técnicos		
Riesgo*	Impacto*	Mitigación*
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



Documento de Seguridad de Datos Personales

Riesgos administrativos y físicos		
Riesgo*	Impacto*	Mitigación*
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



Documento de Seguridad de Datos Personales

Riesgos administrativos y físicos		
Riesgo*	Impacto*	Mitigación*



## 4. ANÁLISIS DE BRECHA





4. ANÁLISIS DE BRECHA

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1) *	Sistema de Gestión Documental de la Secretaría del Tribunal Universitario

Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación*
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



Documento de Seguridad de Datos Personales

Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación*
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



TRIBUNAL UNIVERSITARIO

Documento de Seguridad de Datos Personales



## **5. PLAN DE TRABAJO**



### 5. PLAN DE TRABAJO

El Tribunal Universitario de acuerdo a los recursos asignados y al personal disponible implementará las acciones para el control de seguridad de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado, mediante el siguiente plan de trabajo:

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1) *	Sistema de Gestión Documental de la Secretaría del Tribunal Universitario

Actividad*	Descripción*	Duración*	Cobertura*



Documento de Seguridad de Datos Personales

Actividad*	Descripción*	Duración*	Cobertura*
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]



Documento de Seguridad de Datos Personales

Actividad*	Descripción*	Duración*	Cobertura*
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]



## **6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS**



**6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS**

En este apartado se describen cómo se implementan las políticas para la protección del sistema de tratamiento de datos personales de este Tribunal, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios en correspondencia a su naturaleza.

**I. TRANSFERENCIAS DE DATOS PERSONALES**

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1)*	Sistema de Gestión Documental del Tribunal Universitario
<b>TRANSFERENCIAS DE DATOS PERSONALES</b>	
Transferencias mediante el traslado de soportes físicos:	No aplica/ No se realizan transferencias.
Transferencias mediante el traslado de soportes electrónicos:	No aplica/ No se realizan transferencias.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica/ No se realizan transferencias.

**II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS**

**1. Medidas de seguridad implementadas para el resguardo de los soportes físicos del sistema.**

- Se dispone en las instalaciones del Tribunal Universitario con puertas de acceso restringido con cerraduras para mantener control de entrada del personal usuario a la documentación y equipo de cómputo que contiene el sistema de tratamiento de datos personales.
- Los soportes físicos del sistema constan de expedientes impresos que se encuentran en carpetas físicas con un número de control interno y ubicados en estantes y gavetas localizadas dentro de las oficinas con puertas y cerradura, cuya llave de acceso únicamente la posee una persona previamente autorizada.
- Se cuenta con personal designado para el control de acceso a los expedientes y documentos que pudieran contener datos personales en resguardo físico de las áreas internas del Tribunal Universitario.
- Al momento de utilizar la documentación se tiene el cuidado de mantenerlos en lugares seguros, bajo llave, dentro de cajones cerrados, a fin de promover la restricción a los datos personales que pudieran contener.
- Implementación de formatos de entrada y salida de préstamo de expedientes por





parte de las personas encargadas.

- Se evita dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como se restringe su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales del área involucrada.

**2. Listado de las personas que tienen acceso a los soportes físicos del sistema.**

<b>Secretaría del Tribunal Universitario</b>	
<b>Identificador único*</b>	SecTU
<b>(Nombre del sistema A1) *</b>	<u>Sistema de Gestión Documental de la Secretaría del Tribunal Universitario</u>
<b>Responsable*:</b>	Secretaría del Tribunal Universitario
<b>Nombre<sup>2</sup>:</b>	Janet Becerra Ramos
<b>Cargo*:</b>	Secretaria Suplente del Tribunal Universitario
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Suplir al Secretario del Tribunal Universitario en la gestión administrativa y operativa de los asuntos y trámites que son de su competencia.</li> <li>• Acceder, consultar y en su caso remitir la documentación recabada con motivo de los asuntos que en materia disciplinaria universitaria le sean turnados en el ámbito de su competencia, lo anterior a través del Sistema de Gestión Documental</li> <li>• Cuenta con voz, pero no voto ante dicho órgano.</li> </ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>

<sup>2</sup> **Responsable del Sistema de Datos Personales:** Persona funcionario universitario que decide sobre el tratamiento de los datos personales, su finalidad, la protección y las medidas de seguridad de los mismos.



## Documento de Seguridad de Datos Personales

	<p>Asignar el área física para el resguardo de los expedientes físicos que contienen datos personales.</p> <p>Concentrar e integrar la base de datos del Tribunal Universitario en que se contienen datos personales.</p> <p>Supervisar el espacio físico y el mobiliario destinados al resguardo de los expedientes en donde se pudieran contener datos personales.</p> <p>Emitir de manera inmediata el informe correspondiente al Responsable de Seguridad de Datos Personales sobre cualquier incidente que se presente en el acceso, resguardo, consulta o transmisión de los datos personales, y simultáneamente hacer el registro correspondiente.</p>
	<b>Usuarios:</b>
<b>(Nombre del Usuario 1*)</b>	Dr. José Maximo Carvajal Contreras
<b>Cargo*:</b>	Presidente del Tribunal Universitario
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario.</li><li>• Cuenta con voz y voto. En caso de empate en los votos de las resoluciones emitidas por el Tribunal Universitario en el marco de sus atribuciones, cuenta con voto de calidad.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental de este órgano colegiado.</li><li>• Emitir en el ámbito de sus atribuciones la documentación necesaria relacionada con los procedimientos disciplinarios de los que conoce el Tribunal.</li><li>• Instruir al personal asignado al Tribunal Universitario de no proporcionar información a personas no autorizadas o no consideradas como usuarias.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p>



## Documento de Seguridad de Datos Personales

	<p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 2*)</b>	Mtro. Hugo Alejandro Concha Cantú
<b>Cargo*:</b>	Secretario del Tribunal Universitario
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Coordina al personal operativo del Tribunal Universitario durante las diligencias de trámite de los asuntos. Cuenta con voz, pero no voto.</li><li>• Acceder, consultar y turnar al personal operativo del Colegiado por conducto de su Suplente los asuntos recibidos en materia de disciplina universitaria, lo anterior a través del Sistema de Gestión Documental de este órgano colegiado.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 3*)</b>	Mtra. Ana Beatriz Castrejón Díaz.
<b>Cargo*:</b>	Vocal permanente
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario. Cuenta con voz y voto.</li><li>• Acceder, consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.



## Documento de Seguridad de Datos Personales

	<p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 4*)</b>	Dra. María Patricia Kurczyn Villalobos.
<b>Cargo*:</b>	Vocal permanente
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario. Cuenta con voz y voto.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 5*)</b>	Lic. Miguel Mejía Sánchez
<b>Cargo*:</b>	Vocal permanente
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Formar parte del colegiado a fin de impartir justicia universitaria en cada uno de los asuntos de indisciplina remitidos al Tribunal Universitario. Cuenta con voz y voto.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la</p>



## Documento de Seguridad de Datos Personales

	<p>normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p>
<b>(Nombre del Usuario 6*)</b>	Abel Velázquez Cuevas
<b>Cargo*:</b>	Coordinador
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico</p>



## Documento de Seguridad de Datos Personales

	sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.
<b>(Nombre del Usuario 7*)</b>	Irvin Javier Espinosa Gutiérrez
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 8*)</b>	Brenda Cortés León
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>



## Documento de Seguridad de Datos Personales

<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 9*)</b>	Gustavo Brando Alonso Carrillo
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p>



Documento de Seguridad de Datos Personales

	<p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 10*)</b>	Laura Angélica Cruz Torres
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p>





## Documento de Seguridad de Datos Personales

	<p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 11*)</b>	Eduardo Vaca Cerón
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al Reglamento del Tribunal Universitario y de la Comisión de Honor.</li><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li></ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 12*)</b>	Adriana Cruz Hernández
<b>Cargo*:</b>	Jefe de Departamento
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Tramitar el procedimiento disciplinario conforme al</li></ul>



TRIBUNAL UNIVERSITARIO



Documento de Seguridad de Datos Personales

	<p>Reglamento del Tribunal Universitario y de la Comisión de Honor.</p> <ul style="list-style-type: none"> <li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li> </ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Constatar que los expedientes contengan la documentación completa y actualizada sobre el tema</p> <p>Participar para que las condiciones ambientales y de seguridad física, administrativas o técnicas de los expedientes con que tenga contacto se cumplan.</p> <p>Resguardar los expedientes conforme a las políticas internas del Tribunal Universitario.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 13*)</b>	Alejandra Madrigal Rivera
<b>Cargo*:</b>	Abogada Auxiliar
<b>Funciones*:</b>	<ul style="list-style-type: none"> <li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li> </ul>
<b>Obligaciones*:</b>	<p>Proteger los datos personales a los que tenga acceso.</p> <p>Realizar actividades del tratamiento de los datos personales conforme a la normativa.</p> <p>Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Tribunal Universitario.</p> <p>Guardar confidencialidad respecto de los datos personales</p>



Documento de Seguridad de Datos Personales

	<p>tratados.</p> <p>Abstenerse de transferir sin autorización los datos personales relativos a su encargo.</p> <p>Reportar de manera inmediata a su superior jerárquico sobre cualquier incidente que se presente en el resguardo, consulta, acceso o transmisión de los datos personales y simultáneamente hacer el registro correspondiente.</p>
<b>(Nombre del Usuario 14*)</b>	Carolina Arellano Segoviano
<b>Cargo*:</b>	Asistente Ejecutiva
<b>Funciones*:</b>	<ul style="list-style-type: none"><li>• Acceder y consultar la documentación recabada a través del Sistema de Gestión Documental.</li><li>• Guardia y custodia del archivo del Tribunal Universitario y de su base de datos.</li></ul>
<b>Obligaciones*:</b>	<p>Dar cumplimiento a las obligaciones en materia de tratamiento de datos personales que se establecen en la normativa universitaria.</p> <p>Proteger los datos personales que se recaben.</p> <p>No modificar la información de datos personales.</p> <p>No difundir la información de datos personales.</p> <p>Confidencialidad sobre el tratamiento y resguardo de los datos personales.</p> <p>Supervisar el correcto resguardo de datos personales conforme a lo establecido en la normativa universitaria.</p> <p>Asignar el área física para el resguardo de los expedientes físicos que contienen datos personales.</p> <p>Concentrar e integrar la base de datos del Tribunal Universitario en que se contienen datos personales.</p> <p>Supervisar el espacio físico y el mobiliario destinados al resguardo de los expedientes en donde se pudieran contener datos personales.</p> <p>Vigilar que durante el desempeño de sus funciones, en el espacio físico destinado para el resguardo de los datos personales, no tengan acceso a ellos personas no autorizadas.</p>



### III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

El uso de bitácoras para el control o monitoreo de los sistemas de tratamiento de datos personales se desarrollarán, actualizarán o integrarán herramientas de software que nos permita contar con soportes electrónicos que registren los accesos del personal y las acciones realizadas en el uso o consulta de datos personales.

Las bitácoras se deberán almacenar en la nube privada del Tribunal Universitario y el tiempo de resguardo será de 3 años. El acceso y seguridad de la información estará controlada mediante la identificación de un usuario y contraseña, solo el área de informática correspondiente tendrá acceso a los respaldos de las bitácoras.

El responsable de seguridad de datos personales y el área de informática correspondiente serán los responsables de revisar y analizar la información de las bitácoras generadas en los soportes electrónicos cada semana mediante la herramienta desarrollada o implementada.

**Los datos que se registrarán en las bitácoras serán los siguientes:**

**a. Para la bitácora física.**

- I. Número consecutivo consulta
- II. Número de volante
- III. Nombre del trabajador universitarios solicitante
- IV. Área interna del solicitante
- V. Fecha y hora
- VI. Número de fojas
- VII. Seguimiento del préstamo

**b. Para la bitácora electrónica.**

- I. Número de transacción
- II. Id o nombre de usuario
- III. Host origen
- IV. Fecha y hora de ingreso
- V. Id o número de expediente consultado
- VI. Tipo de acción
  1. Trámite
  2. Consulta
  3. Conclusión



#### IV. REGISTRO DE INCIDENTES

Se establecerán registros de incidentes relativos a soportes físicos, como son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, se ofrecen detalles sobre el registro de incidentes en el cual se consignen los procedimientos realizados para la recuperación de los datos o permitir la disponibilidad del proceso.

- En el registro de incidentes, tanto en formato físico como electrónico, se elaborará un informe detallado, donde se señale lo ocurrido, así como la persona que resolvió el incidente.
- Se indicará los soportes físicos o electrónicos dañados y recuperados los cuales pueden ser: oficios, documentos, expedientes, estantes o archiveros, los campos, registros, tablas, bases de datos o archivos electrónicos, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor.
- Para el caso de robo o extravío de datos personales, el responsable del sistema dará vista al titular del área universitaria para su conocimiento, así como al responsable de seguridad de datos personales y al titular del área jurídica correspondiente para que, en el ámbito de sus atribuciones, determine lo conducente.
- Se informará a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información.

#### V. ACCESO A LAS INSTALACIONES

##### 1. Seguridad perimetral exterior:

En la entrada principal del edificio del Centro Cultural Universitario Tlatelolco en el que se ubica el Tribunal Universitario (pisos 11 y 12), se cuenta con acceso controlado, donde personal de vigilancia de la UNAM es el encargado de permitir la entrada a las instalaciones. Se cuenta con video vigilancia las 24 horas en pasillos y cuya administración está a cargo de una dependencia universitaria externa al Tribunal Universitario.

Respecto a los pisos en los que se ubica el Tribunal Universitario, también se cuenta con personal de vigilancia de la UNAM, que entre sus principales actividades tiene la encomienda que, cuando personal externo o visitantes acudan al área universitaria, se le informará mediante radio de la presencia de la o las personas correspondientes y de manera personal, conducirá a las mismas con la o las personas que deban atenderles. Al finalizar su visita, también se encargará de acompañarlos a la salida.

##### 2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):



Documento de Seguridad de Datos Personales

El personal de vigilancia UNAM es el encargado de vigilar el acceso a los pisos 11 y 12 en que se ubica el Tribunal Universitario y quien da aviso de la visita de personas externas a un funcionario con quien se tiene cita o bien, a la titular de la oficialía de partes, son estas las personas las que dan la autorización para su acceso. El personal que labora para el Tribunal Universitario, cuenta con un registro de ingreso y egreso de las instalaciones a través de un control de acceso mediante un equipo biométrico habilitado para el personal autorizado.

Los registros electrónicos y documentación física se encuentran en cubículos cerrados, para su acceso se requiere pasar por una puerta de madera con cerradura cuya llave la detenta la persona que cuenta con el resguardo correspondiente. Así mismo, se cuenta con cajoneras con llave que resguarda los expedientes físicos. Por lo que hace a los registros electrónicos, se encuentran en equipos de cómputo resguardados dentro de los cubículos señalados y que cuentan con seguridad perimetral y clave de acceso.

#### **VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.**

Cualquier rectificación de datos personales se deberá ceñir a los procedimientos consignados en la normatividad universitaria aplicable en la materia.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos.

#### **VII. PERFILES DE USUARIO Y CONTRASEÑAS**

El modelo de control de acceso está basado en grupos o roles, configurada como una red privada y con la opción de uso compartido con protección de contraseña. Los sistemas operativos y aplicativos cuentan con todas las funcionalidades de seguridad para la administración de perfiles y se pueden establecer permisos por usuario.

El almacenamiento de las contraseñas se realiza por medio de un cifrado de datos y contraseñas fuertes que no se pueden invertir. La administración de los perfiles de usuario y contraseña las realiza área de informática correspondiente y se autoriza a través de la persona titular de la Presidencia o Secretaría del Tribunal Universitario.

No se permite el acceso a ninguna otra carpeta o aplicación del equipo donde se almacena el aplicativo para el tratamiento de datos personales. Los accesos para el mantenimiento de software se realizan de manera local.

Los accesos remotos son deshabilitados en los equipos de cómputo a través del sistema operativo.



## VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los procedimientos de respaldo y recuperación de datos se realizan conforme a las *Recomendaciones para el almacenamiento de datos* del Centro de datos de la UNAM, de la siguiente manera:

- Completos: todos,
- De forma automática: todos,
- Periodicidad con que los realiza: Semanal.

Las copias de seguridad se almacenan en la nube privada de Tribunal Universitario.

## IX. PLAN DE CONTINGENCIA

Las estrategias de prevención aplicables para recuperar y ejecutar operaciones de sistemas en caso de una contingencia se indican a continuación:

- a) Revisión en el medio de almacenamiento las últimas copias de respaldo de la información almacenada del aplicativo.
- b) Identificación de las carpetas que contenga las versiones de: sistema operativo, código fuente o propietario, software de la base de datos, actualizaciones, programas utilitarios, archivo con la estructura de la base y datos, etc.
- c) Contactos actualizados con los responsables del alojamiento alternativo para la recuperación de los servicios de tecnologías de información.
- d) Documentación técnica detallada de las especificaciones de hardware y software, habilitación o instalación de complementos, claves de acceso y guía de instalación.
- e) Entrenamiento del área de informática correspondiente en el proceso de recuperación de los servicios de Tecnología de la Información (TI).
- f) Evaluación del entrenamiento del personal de TI para verificar que se lograron los objetivos.
- g) Verificación y validación de acceso seguro a los sistemas y aplicativos web.
- h) Durante la contingencia se evaluará el alcance del desastre en el área.
- i) Proveer facilidades al personal encargado de la recuperación para asegurar que se lleven a cabo los procedimientos del plan de contingencia, y
- j) Finalmente evaluar la efectividad del plan de contingencia.

No se cuenta con un sitio redundante debido a que se realizan un estricto control de respaldos de los aplicativos, así como de sus bases de datos.



## **7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD**





## 7. MONITOREO DE LAS MEDIDAS DE SEGURIDAD

La supervisión de las medidas de seguridad técnicas y físicas es un elemento importante para la mejora continua, puesto que permite definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo con los que cuenta el Tribunal Universitario se encuentran las siguientes y aplican para:

### 7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1)*	Sistema de Gestión Documental del Tribunal Universitario

Recurso*	Descripción*	Control*
Software de administración Router/Firewall.	Utilización de la interfase del Router/Firewall para realizar una revisión trimestral de las actualizaciones del firmware para solucionar vulnerabilidades de seguridad.	Registrar en una bitácora la fecha y versión del firmware instalado del fabricante, así como el responsable de llevar a cabo la revisión. El área de informática correspondiente analiza los registros de la actividad.
Software para el diagnóstico de hardware y software en los equipos de cómputo y servidores.	Utilización de herramientas de software para diagnosticar y controlar funcionalidades de hardware y software.	Registrar en una bitácora los diagnósticos suministrados por el software, indicando la fecha, resultados, tipo de corrección realizada y responsable de la revisión. El área de informática correspondiente analiza los registros de la actividad.
Software de administración de la nube privada.	Utilización de la interfase de la nube privada para realizar diagnósticos trimestrales del funcionamiento de los discos de respaldo donde se encuentran las copias de seguridad (backups).	Verificar a través de un muestreo si la integridad de las copias de seguridad no ha sido alterada y registrar en una bitácora, la fecha, resultados obtenidos y responsable de la revisión. El área de informática correspondiente analiza los registros de la actividad.



Recurso*	Descripción*	Control*
Cumplimiento de protocolos.	Mantener actualizada la documentación derivada de cambios en las operaciones técnicas o actualizaciones tecnológicas.	Realizar actualizaciones y versionado de la documentación técnica de los sistemas en operación. El área de informática correspondiente analiza los registros de la actividad.
Controles de roles y permisos.	Validar que los accesos, baja o cambio a sistemas físicos o electrónicos se realicen conforme al proceso de administración de usuarios.	Vigilar y registrar en un medio electrónico que el ingreso del personal sea a través de los accesos correspondientes y plenamente identificados. El área de informática correspondiente analiza los registros de la actividad.

### 7.2 Procedimiento para la revisión de las medidas de seguridad

Los procedimientos para la revisión de las medidas de seguridad de encuentran en elaboración.

### 7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Los resultados de la evaluación de pruebas a las medidas de seguridad se registrarán y analizarán una vez que se cuente con los procedimientos para la revisión de las medidas de seguridad.

### 7.4 Acciones para la corrección y actualización de las medidas de seguridad

Las acciones para la corrección y actualización de las medidas de seguridad se obtendrán una vez que se cuenten con los resultados de las evaluaciones y los procedimientos de revisión correspondiente.



## **8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN**



## 8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

### 8.1 Programa de capacitación a los responsables de seguridad de datos personales

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1)*	Sistema de Gestión Documental del Tribunal Universitario

Actividad*	Descripción*	Duración*	Cobertura*
Programa universitario de capacitación en protección de datos personales.	Impartido en conjunto por la DGTIC y la Unidad de Transparencia.	Una semana.	A todo el personal responsable de seguridad de datos personales e informática.

### 8.2 Programa de difusión de la protección a los datos personales

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1)*	Sistema de Gestión Documental del Tribunal Universitario

Actividad*	Descripción*	Duración*	Cobertura*
Difusión de actualizaciones a medidas sobre la protección de datos personales.	<ul style="list-style-type: none"> <li>Difusión de material que apoye la actualización a los usuarios que operan y dan tratamiento sobre las políticas y mecanismos de seguridad en el tratamiento de datos personales que se vayan implementando.</li> <li>Cursos de capacitación que se efectúen conforme se programen por la Unidad de Transparencia.</li> </ul>	Semestral (de acuerdo a las modificaciones o adecuaciones a las medidas de seguridad implementadas)	Personal involucrado en el tratamiento de datos personales



## 9. MEJORA CONTINUA



## 9. MEJORA CONTINUA

En este apartado se muestran las acciones que se llevan a cabo para mantener y mejorar los procesos y el sistema de protección de datos personales.

Tribunal Universitario	
Identificador único*	SecTU
(Nombre del sistema A1)*	Sistema de Gestión Documental del Tribunal Universitario

### 9.1 Actualización y mantenimiento de sistemas de información

Actividad*	Descripción*	Duración*	Cobertura*
Identificación de cambios o mejoras a los aplicativos.	Se identifica que parte del aplicativo se requiere actualizar o modificar a solicitud de los usuarios del sistema o por identificación del área de informática correspondiente por una falla técnica.	Dos semanas.	En caso de falla del sistema o su base de datos, se cuenta con el soporte técnico para su reparación parcial o total.

### 9.2. Actualización y mantenimiento de equipo de cómputo

Actividad*	Descripción*	Duración*	Cobertura*
Actualización de software y hardware	Los equipos están configurados para recibir de forma automática las actualizaciones de software y son instaladas de acuerdo a las horas activas del equipo, aunado a esto, el área de informática correspondiente realiza búsquedas manuales y periódica de ellas. En caso de requerir componentes para los equipos de cómputo o servidores se hará el requerimiento correspondiente.	Actividad permanente	Total



Documento de Seguridad de Datos Personales

Mantenimiento preventivo o correctivo	Los servicios se realizan trimestralmente. El área de informática correspondiente realiza una revisión interna del CPU y se determina si el mantenimiento es preventivo o correctivo. La fecha de mantenimiento se coordina con el área y se determina el momento adecuado para realizarlo.	1 día	Total
---------------------------------------	---	-------	-------

**9.3 Procesos para la conservación, preservación y respaldos de información**

Proceso*	Descripción*	Responsable*
Respaldos de las bases de datos	Los respaldos se llevan a cabo semanalmente y se almacenan en un medio diferente al equipo de cómputo. El resguardo se realiza en el servicio de nube privada del Tribunal Universitario.	El área de informática correspondiente.

**9.4 Procesos de borrado seguro y disposición final de equipos y componentes informáticos**

Proceso*	Descripción*	Responsable*
Borrado seguro	Utilización de herramientas que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura en medios magnéticos o electrónicos.	El área de informática correspondiente.
Baja de equipo	Previo a la baja de un equipo de cómputo o componente informático se realiza el proceso de borrado seguro. Si no es posible una destrucción lógica, se realiza una destrucción física.	El área de informática correspondiente.



# **10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES**





## 10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Cuando la totalidad de los datos personales contenidos en los aplicativos hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades para la que fueron recolectados, de acuerdo con las disposiciones legales aplicables, se realizarán los siguientes pasos:

1. Datos del sistema de tratamiento de datos personales que será cancelado.
2. Plazos y condiciones para el bloqueo del sistema de tratamiento de datos personales.
3. Medidas de seguridad para el bloqueo y posterior supresión del sistema de tratamiento de datos personales:
4. Procedimiento para la supresión del sistema de tratamiento de datos personales.
5. Mecanismos para la supresión del sistema de tratamiento de datos personales.



11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

		Nombre y firma de quienes revisaron el presente documento:
<b>Elaboraron y revisaron:</b>	<p>Adriana Cruz Hernández Jefa de Departamento Teléfono 5551172818, Ext. 49655 Correo electrónico: <a href="mailto:adrianach@tribunaluniversitario.unam.mx">adrianach@tribunaluniversitario.unam.mx</a></p> <p>Janet Becerra Ramos Secretaria Suplente del Tribunal Universitario Teléfono 5551172818, Ext. 49640 Correo electrónico: <a href="mailto:janet.becerra@tribunaluniversitario.unam.mx">janet.becerra@tribunaluniversitario.unam.mx</a></p>	 
<b>Autorizó:</b>	<p>Dr. José Maximo Carvajal Contreras Presidente del Tribunal Universitario Teléfono 5551172818, Ext. 49657</p>	
<b>Fecha de aprobación por el Comité de Transparencia de la UNAM:</b>	12 de agosto de 2022	



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública, que someten el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, el **Programa Universitario de Bioética**, la **Dirección General de Bibliotecas y Servicios Digitales de Información**, el **Centro de Enseñanza para Extranjeros**, el **Instituto de Ciencias Aplicadas y Tecnología**, el **Centro de Investigaciones sobre América Latina y el Caribe**, la **Facultad de Estudios Superiores Aragón**, la **Coordinación Universitaria para la Sustentabilidad**, el **Tribunal Universitario**, la **Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”**, la **Escuela Nacional de Estudios Superiores, Unidad León**, la **Dirección General de Administración Escolar** y la **Oficina de la Abogacía General**, en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

### ANTECEDENTES

- I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.
- II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/528/2022

- IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los “Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”.
- V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado “V. Reglas de Generales de Evaluación” del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

Por otra parte, en el apartado “VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia”, Capítulo II. Criterios y formatos, **Vertiente 2: Deberes, Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.

- VI. En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.
- VII. La Presidencia del Comité de Transparencia recibió diversos oficios, mediante los cuales las Áreas Universitarias sometieron a consideración de este Cuerpo Colegiado, la clasificación de reserva total de una parte de la información de sus Documentos de Seguridad, mismos que se enlistan a continuación:



**COMITÉ DE TRANSPARENCIA DE LA  
UNIVERSIDAD NACIONAL AUTÓNOMA DE  
MÉXICO**

**RESOLUCIÓN: CTUNAM/528/2022**

<b>Oficio</b>	<b>Área Universitaria</b>	<b>Fecha de presentación</b>
CH/PUED/COORD/0058/2022	Programa Universitario de Estudios del Desarrollo	18/08/2022
DGAC/CoNTI/018/2022	Dirección General de Actividades Cinematográficas	
DGPYFE/DG/487/2022	Dirección General de Publicaciones y Fomento Editorial	
ICF/139/2022	Instituto de Ciencias Físicas	
CRAI/232/2022	Coordinación de Relaciones y Asuntos Internacionales	
COHU/PUEAA/128/2022	Programa Universitario de Estudios sobre Asia y África	
DGPU/1806/2022	Dirección General del Patrimonio Universitario	
CJHA/357/2022	Consejo Académico del Área de las Humanidades y las Artes	
IAST/DIR/798/248/590-22	Instituto de Astronomía	
ENP/P9/DIR/048/R/2022	Escuela Nacional Preparatoria, Plantel 9 "Pedro de Alba"	
ENP/PL2/D205/2022	Escuela Nacional Preparatoria 2, "Erasmus Castellanos Quinto"	
ENP7/D/107/22	Escuela Nacional Preparatoria 7, "Ezequiel A. Chávez"	19/08/2022
CAAUCA/241/2022	Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área	
FESI/DIR/MCAA/0387/2022	Facultad de Estudios Superiores, Iztacala	
FMVZ/D/FSG/193/2022	Facultad de Medicina Veterinaria y Zootecnia	
ETR/003/2022	Coordinación de Vinculación con el Consejo Universitario	
SADM/294/2022	Secretaría Administrativa	
IIE/D/159/2022	Instituto de Investigaciones Estéticas	
CEII/D/0265/2022	Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades	22/08/2022
PUB/DIR/105/2022	Programa Universitario de Bioética	
DGBSDI/640/2022	Dirección General de Bibliotecas y Servicios Digitales de Información	
CEPE/D*CPO/270/2022	Centro de Enseñanza para Extranjeros	
Oficio sin número	Instituto de Ciencias Aplicadas y Tecnología	



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

CIAL/DIR/333/22	Centro de Investigaciones sobre América Latina y el Caribe	23/08/2022
FESAR/DIRA/OJUR/907/2022	Facultad de Estudios Superiores, Aragón	
COUS/087/2022	Coordinación Universitaria para la Sustentabilidad	
T-22/023/01	Tribunal Universitario	
ENP 1/D/147/2022	Escuela Nacional Preparatoria, Plantel 1 "Gabino Barreda"	
ENES-León/OJ/099/2022	Escuela Nacional de Estudios Superiores, Unidad León	
SG/DGAE/1018/2022	Dirección General de Administración Escolar	
OAG/ST/1729/2022	Oficina de la Abogacía General	

En dichos oficios, las Áreas Universitarias informaron lo siguiente:

*“Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados<sup>1</sup>; exige elaborar versión pública del documento de seguridad de esta área universitaria.*

*Una vez analizada la información que se solicitó en el primer punto del ‘Documento de seguridad’, se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

*En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos*

<sup>1</sup> DOF: 26 de noviembre de 2021



**COMITÉ DE TRANSPARENCIA DE LA  
UNIVERSIDAD NACIONAL AUTÓNOMA DE  
MÉXICO**

**RESOLUCIÓN: CTUNAM/528/2022**

*Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales ... El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:*

<b>Anexos o Políticas</b>	<b>Contenido y su afectación</b>	<b>Páginas</b>
<i>a) Análisis de riesgos</i>	<i>El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica ... y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.</i>	<i>...</i>
<i>b) Análisis de brecha</i>	<i>El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.</i>	<i>...</i>
<i>c) Plan de Trabajo</i>	<i>El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.</i>	<i>...</i>

*Los fundamentos y motivos se exponen a continuación:*

- Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información*





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/528/2022

*exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo ... evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*
- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

*La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*

*En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

*En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de*





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

*la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.*

*Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

*En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda ...” (sic).*

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

### CONSIDERACIONES

**PRIMERA.** Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Oficina de la Abogacía General**, en este acto, el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y Secretario Técnico del Comité de Transparencia, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

**SEGUNDA.** De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y**



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

Humanidades, el Programa Universitario de Bioética, la Dirección General de Bibliotecas y Servicios Digitales de Información, el Centro de Enseñanza para Extranjeros, el Instituto de Ciencias Aplicadas y Tecnología, el Centro de Investigaciones sobre América Latina y el Caribe, la Facultad de Estudios Superiores Aragón, la Coordinación Universitaria para la Sustentabilidad, el Tribunal Universitario, la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, la Escuela Nacional de Estudios Superiores, Unidad León, la Dirección General de Administración Escolar y la Oficina de la Abogacía General, y determinar, en consecuencia, si la confirma, modifica o revoca.

**TERCERA.** De conformidad con lo dispuesto en los artículos 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, esa clasificación.

En tal virtud el Programa Universitario de Estudios del Desarrollo, la Dirección General de Actividades Cinematográficas, la Dirección General de Publicaciones y Fomento Editorial, el Instituto de Ciencias Físicas, la Coordinación de Relaciones y Asuntos Internacionales, el Programa Universitario de Estudios sobre Asia y África, la Dirección General del Patrimonio Universitario, el Consejo Académico del Área de las Humanidades y las Artes, el Instituto de Astronomía, la Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”, la Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área, la Facultad de Estudios Superiores Iztacala, la Facultad de Medicina Veterinaria y Zootecnia, la Coordinación de Vinculación con el Consejo Universitario, la Secretaría Administrativa, el Instituto de Investigaciones Estéticas, el Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades, el Programa Universitario de Bioética, la Dirección General de Bibliotecas y Servicios Digitales de Información, el Centro de Enseñanza para Extranjeros, el Instituto de Ciencias Aplicadas y Tecnología, el Centro de Investigaciones sobre América Latina y el Caribe, la Facultad de Estudios Superiores Aragón, la Coordinación Universitaria para la Sustentabilidad, el Tribunal Universitario, la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, la Escuela Nacional de Estudios Superiores, Unidad León. la Dirección General de Administración Escolar y la Oficina de la Abogacía General, clasificaron como información reservada, por un periodo de **cinco años**, la relativa al **Análisis de Riesgo**, al **Análisis de Brecha** y al **Plan de Trabajo**, conforme a lo expuesto en el antecedente VII de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente.

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

*“... Como información reservada podrá clasificarse aquella cuya publicación:*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

[...]

**VII. Obstruya la prevención o persecución de los delitos;**

[...]”.

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:

***“Vigésimo sexto. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, **aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.*****

...”.

### Énfasis añadido.

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Al respecto, cabe tener en consideración lo establecido en el documento de trabajo del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: *“La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad...”*.

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

Desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/528/2022

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Asimismo, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981, publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De igual forma, de conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/528/2022

disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrá pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

En ese sentido, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que los sujetos obligados deben elaborar un documento de seguridad, entendiéndose como tal, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Ahora bien, de conformidad con los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los numerales 55 al 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, el análisis de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En tal orden de ideas, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Además de lo anterior, de conformidad con el artículo 19, fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

Por ende, de difundirse la información contenida en los apartados relativos al **Análisis de Riesgos, al Análisis de Brecha, al Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en el **Análisis de Riesgos**, en el **Análisis de Brecha**, en **Plan de Trabajo**, así como de **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o que revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

*“Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

*Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa”.*

*“Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*

*Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

*...”*

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean o no propiedad del Estado**, o bien, conozca o copie dicha información; conductas que de igual manera se pueden materializar en los archivos físicos, ya que es factible **sustraer, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, los datos personales contenidos en los documentos bajo custodia de las Áreas Universitarias**, por lo que la misma protección deberá otorgarse a los sistemas electrónicos, así como a los archivos físicos con los que se cuenta.



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

### RESOLUCIÓN: CTUNAM/528/2022

Por lo que de darse a conocer la información relativa al **Análisis de Riesgos**, al **Análisis de Brecha**, al **Plan de Trabajo**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal del responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las Áreas Universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la publicación de esa información revelaría elementos que de manera concatenada con otra información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica de las Áreas Universitarias, ya que la información relativa a las medidas físicas, administrativas y técnicas puede ser utilizada para propiciar, entre otros, actos vandálicos, o bien, ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a los documentos físicos y/o electrónicos que obran en los archivos, así como a la infraestructura informática, programas y desarrollos tecnológicos de las Áreas Universitarias, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, tales como las relacionadas en párrafos anteriores.

Por lo anterior, se concluye que la información solicitada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

*“Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*

*I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

*II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*

*III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio”.*

**I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.**

De difundirse la información contenida en el **análisis de riesgos**, en el **análisis de brecha** y en el **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

En ese sentido la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

**II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.**

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **análisis de riesgos**, en el **análisis de brecha** y en el **plan de trabajo**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se limitaría la capacidad de las Áreas Universitarias para prevenir la comisión de conductas ilícitas.

De ahí resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda.

**III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.**

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, a cambio de garantizar la capacidad de las Áreas Universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.





## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

En ese sentido, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la versión pública propuesta por el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, el **Programa Universitario de Bioética**, la **Dirección General de Bibliotecas y Servicios Digitales de Información**, el **Centro de Enseñanza para Extranjeros**, el **Instituto de Ciencias Aplicadas y Tecnología**, el **Centro de Investigaciones sobre América Latina y el Caribe**, la **Facultad de Estudios Superiores Aragón**, la **Coordinación Universitaria para la Sustentabilidad**, el **Tribunal Universitario**, la **Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”**, la **Escuela Nacional de Estudios Superiores, Unidad León**, la **Dirección General de Administración Escolar** y por la **Oficina de la Abogacía General**, por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

**CUARTA.** Este Comité considera pertinente orientar a las Áreas Universitarias, a efecto de que en la elaboración de la versión pública de sus respectivos documentos de seguridad, tengan en cuenta lo siguiente:

- Deberán testar las secciones o información correspondientes al “Análisis de Riesgo”, al “Análisis de Brecha”, al “Plan de Trabajo”, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Deberán insertar un cuadro de texto en el cual se indiquen:
  - Las partes o secciones reservadas.
  - El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentran indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

Lo anterior, de conformidad con lo dispuesto en los numerales Quincuagésimo Noveno, Sexagésimo y Sexagésimo Primero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

### RESUELVE

**PRIMERO.** Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN de RESERVA** total de una parte la información para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por el **Programa Universitario de Estudios del Desarrollo**, la **Dirección General de Actividades Cinematográficas**, la **Dirección General de Publicaciones y Fomento Editorial**, el **Instituto de Ciencias Físicas**, la **Coordinación de Relaciones y Asuntos Internacionales**, el **Programa Universitario de Estudios sobre Asia y África**, la **Dirección General del Patrimonio Universitario**, el **Consejo Académico del Área de las Humanidades y las Artes**, el **Instituto de Astronomía**, la **Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”**, la **Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área**, la **Facultad de Estudios Superiores Iztacala**, la **Facultad de Medicina Veterinaria y Zootecnia**, la **Coordinación de Vinculación con el Consejo Universitario**, la **Secretaría Administrativa**, el **Instituto de Investigaciones Estéticas**, el **Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades**, el **Programa Universitario de Bioética**, la **Dirección General de Bibliotecas y Servicios Digitales de Información**, el **Centro de**



## COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/528/2022

**Enseñanza para Extranjeros, el Instituto de Ciencias Aplicadas y Tecnología, el Centro de Investigaciones sobre América Latina y el Caribe, la Facultad de Estudios Superiores Aragón, la Coordinación Universitaria para la Sustentabilidad, el Tribunal Universitario, la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, la Escuela Nacional de Estudios Superiores, Unidad León, la Dirección General de Administración Escolar y por la Oficina de la Abogacía General, en relación con el Análisis de Riesgos, el Análisis de Brecha y el Plan de Trabajo, así como toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias, por un periodo de cinco años, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.**

Lo anterior, en términos de la consideración **TERCERA** de la presente resolución.

**SEGUNDO.** Se instruye a las Áreas Universitarias a efecto de que elaboren la versión pública en términos de lo dispuesto en la consideración **CUARTA**.

**TERCERO.** Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional al **Programa Universitario de Estudios del Desarrollo, a la Dirección General de Actividades Cinematográficas, a la Dirección General de Publicaciones y Fomento Editorial, al Instituto de Ciencias Físicas, a la Coordinación de Relaciones y Asuntos Internacionales, al Programa Universitario de Estudios sobre Asia y África, a la Dirección General del Patrimonio Universitario, al Consejo Académico del Área de las Humanidades y las Artes, al Instituto de Astronomía, a la Escuela Nacional Preparatoria, Planteles 9 “Pedro de Alba”, 2 “Erasmus Castellanos Quinto” y 7 “Ezequiel A. Chávez”, a la Unidad Coordinadora de Servicios de Apoyo Administrativo a los Consejos Académicos de Área, a la Facultad de Estudios Superiores Iztacala, a la Facultad de Medicina Veterinaria y Zootecnia, a la Coordinación de Vinculación con el Consejo Universitario, a la Secretaría Administrativa, al Instituto de Investigaciones Estéticas, al Centro de Investigaciones Interdisciplinarias en Ciencias y Humanidades, al Programa Universitario de Bioética, a la Dirección General de Bibliotecas y Servicios Digitales de Información, al Centro de Enseñanza para Extranjeros, al Instituto de Ciencias Aplicadas y Tecnología, al Centro de Investigaciones sobre América Latina y el Caribe, a la Facultad de Estudios Superiores Aragón, a la Coordinación Universitaria para la Sustentabilidad, al Tribunal Universitario, a la Escuela Nacional Preparatoria, Plantel 1 “Gabino Barreda”, a la Escuela Nacional de Estudios Superiores, Unidad León, a la Dirección General de Administración Escolar, a la Oficina de la Abogacía General, así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.**



## **COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**RESOLUCIÓN: CTUNAM/528/2022**

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

**POR MI RAZA HABLARÁ EL ESPÍRITU”  
Ciudad Universitaria, Cd. Mx., 24 de agosto de 2022**

<b>Archivo</b>	02-ctunam-528-2022-docto-seg-3.pdf		
<b>Identificador único (hash)</b>	07de6833b5ddfb06d59dfe05ffc9ae1d6e0e12f253c84b4590303ce195d20cd		
<b>Fecha y hora de cierre</b>	24/08/2022 19:14:44	<b>Fecha y hora de emisión</b>	24/08/2022 19:35:48
<b>Número de páginas</b>	18	<b>Firmantes</b>	5



#### Firmantes

<b>Nombre</b>	Lic. MARIA ELENA GARCIA MELENDEZ	<b>Fecha y hora de firma</b>	24/08/2022 16:01:41
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
<b>Hash Firma</b>	a5b9499d7fd52fa3c184565d34d68700d725eea53a83224d5cb7a84fc5e3e39e1d35df5ae8294a7d46ae8e8b731e1394		

<b>Nombre</b>	Dra. Guadalupe Barrena Nájera	<b>Fecha y hora de firma</b>	24/08/2022 16:36:33
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
<b>Hash Firma</b>	730f1857908c13c686920a2766995f4f29d88309feb74c45dcb8753ce300799dd8962ec4863776556b971bd808c63e3f		

<b>Nombre</b>	Ing. Ricardo Ramírez Ortiz	<b>Fecha y hora de firma</b>	24/08/2022 15:52:42
Director General de Servicios Generales y Movilidad			
<b>Hash Firma</b>	d56f4af1a2aa91be862c6200037618c973a7a494330be4015b65e14ba73b7f814dd8e8c370d1f428753896438442afcd		

<b>Nombre</b>	JOSE MELJEM MOCTEZUMA	<b>Fecha y hora de firma</b>	24/08/2022 17:57:01
Titular de la Unidad de Transparencia			
<b>Hash Firma</b>	ee57713fb4e324026815ba61dec8c010cbbe4089ba52a484dff0d1953af31654d371b4b621a363f2c110c521fe492397		

<b>Nombre</b>	Dra. Jacqueline Peschard Mariscal	<b>Fecha y hora de firma</b>	24/08/2022 19:14:44
Especialista			
<b>Hash Firma</b>	6c01e40a8ac66d63d19efa430d0cc5a32750a74bd853ee40d2d3d8571a5c6ed4e483274029997b22c3c45cd4ba2dc82c		