1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES DE LA TESORERIA

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT001
(Nombre del sistema A1) *	**Padrón de Proveedores y Contratistas**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos de identificación**: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, RFC, CURP, cuenta bancaria y banco.
Responsable*:	
Nombre*:	**Arturo Martínez Alvarado**
Cargo*:	**Coordinador de Desarrollo**
Funciones*:	Dar soporte técnico al Padrón de Proveedores y Contratistas de la Universidad
Obligaciones*:	Mantener operativo el Padrón de Proveedores y Contratistas de la Universidad y atender los requerimientos y cambios solicitados por los usuarios.
	Encargados
(Nombre del Encargado 1*)	**Ma de los Angeles Carreón Rodríguez**
Cargo*:	**Líder de Proyecto**
Funciones*:	Validación de la información fiscal del proveedor.
Obligaciones*:	Verificar que la información que capturó el Proveedor es la misma que está contenida en la Constancia de Situación Fiscal emitida por el SAT, con una vigencia no mayor a 3 meses.
(Nombre del Encargado 2*)	**Lic. Carlos Méndez Hernández**
Cargo*:	**Auditor**
Funciones*:	Cotejar de datos bancarios proveedor
Obligaciones*:	Verificar que la información capturada por el proveedor o prestador de servicios coincida con el estado de cuenta bancario que anexa el proveedor, el cual no debe ser mayor a 3 meses con relación a la fecha de validación.
(Nombre del Encargado 3*)	**René Filemón Méndez González**
Cargo*:	**Auditor**
Funciones*:	Cotejar de datos bancarios proveedor
Obligaciones*:	Verificar que la información capturada por el proveedor o prestador de servicios coincida con el estado de cuenta bancario que anexa el proveedor, el cual no debe ser mayor a 3 meses con relación a la fecha de validación.
(Nombre del Encargado 4*)	**Jorge Alberto Rosado Ríos**
Cargo*:	**Auditor**
Funciones*:	Cotejar de datos bancarios proveedor
Obligaciones*:	Verificar que la información capturada por el proveedor o

	prestador de servicios coincida con el estado de cuenta bancario que anexa el proveedor, el cual no debe ser mayor a 3 meses con relación a la fecha de validación.
	Usuarios:
(Nombre del Usuario 1*)	**Proveedores de la UNAM**
Cargo*:	Encargado del registro
Funciones*:	Capturar información de personal y bancaria en el Padrón de Proveedores de la UNAM
Obligaciones*:	Capturar información de personal y bancaria tal como está registrada en el SAT y en su Banco.
(Nombre del Usuario 2*)	**Contratistas de la UNAM**
Cargo*:	Encargado del registro
Funciones*:	Capturar información de personal y bancaria en el Padrón de Proveedores de la UNAM
Obligaciones*:	Capturar información de personal y bancaria tal como está registrada en el SAT y en su Banco.

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT002
(Nombre del sistema A1) *	**Padrón de Prestadores de Servicios**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos de identificación**: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, RFC, CURP, cuenta bancaria y banco.
Responsable*:	
Nombre*:	**Arturo Martínez Alvarado**
Cargo*:	**Coordinador de Desarrollo**
Funciones*:	Dar soporte técnico al Padrón de Proveedores y Contratistas de la Universidad
Obligaciones*:	Mantener operativo el Padrón de Proveedores y Contratistas de la Universidad y atender los requerimientos y cambios solicitados por los usuarios.
	Encargados:
(Nombre del Encargado 1*)	**Ma de los Angeles Carreón Rodríguez**
Cargo*:	**Líder de Proyecto**
Funciones*:	Validación de la información fiscal del proveedor.
Obligaciones*:	Verificar que la información que capturó el Proveedor es la misma que está contenida en la Constancia de Situación Fiscal emitida por el SAT, con una vigencia no mayor a 3 meses.

	Usuarios:
(Nombre del Usuario 1*)	**Prestadores de Servicios de la UNAM**
Cargo*:	Encargado del registro
Funciones*:	Capturar información de personal y bancaria en el Padrón de Proveedores de la UNAM
Obligaciones*:	Capturar información de personal y bancaria tal como está registrada en el SAT y en su Banco.

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

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT001
(Nombre del sistema A1*)	**Padrón de Proveedores y Contratistas**
Tipo de soporte:*	El sistema se encuentra únicamente en electrónico. No se tiene planificado contar con soporte físico.
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	El sistema y la base de datos, están alojados en un servidor virtual, mismo que se encuentra instalado sobre un servidor físico propiedad de la Tesorería de la UNAM, en las oficinas de la UTICT.

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT002
(Nombre del sistema A1*)	**Padrón de Prestadores de Servicios**
Tipo de soporte:*	El sistema se encuentra únicamente en electrónico. No se tiene planificado contar con soporte físico.
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	El sistema y la base de datos, están alojados en un servidor virtual, mismo que se encuentra instalado sobre un servidor físico propiedad de la Tesorería de la UNAM, en las oficinas de la UTICT.

3. ANÁLISIS DE RIESGOS

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT01	
(Nombre del sistema A1) *	**Padrón de Proveedores y Contratistas**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT002	
(Nombre del sistema A1) *	**Padrón de Prestadores de Servicios**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

4. ANÁLISIS DE BRECHA

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT01	
(Nombre del sistema A1) *	**Padrón de Proveedores y Contratistas**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT002	
(Nombre del sistema A1) *	**Padrón de Prestadores de Servicios**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

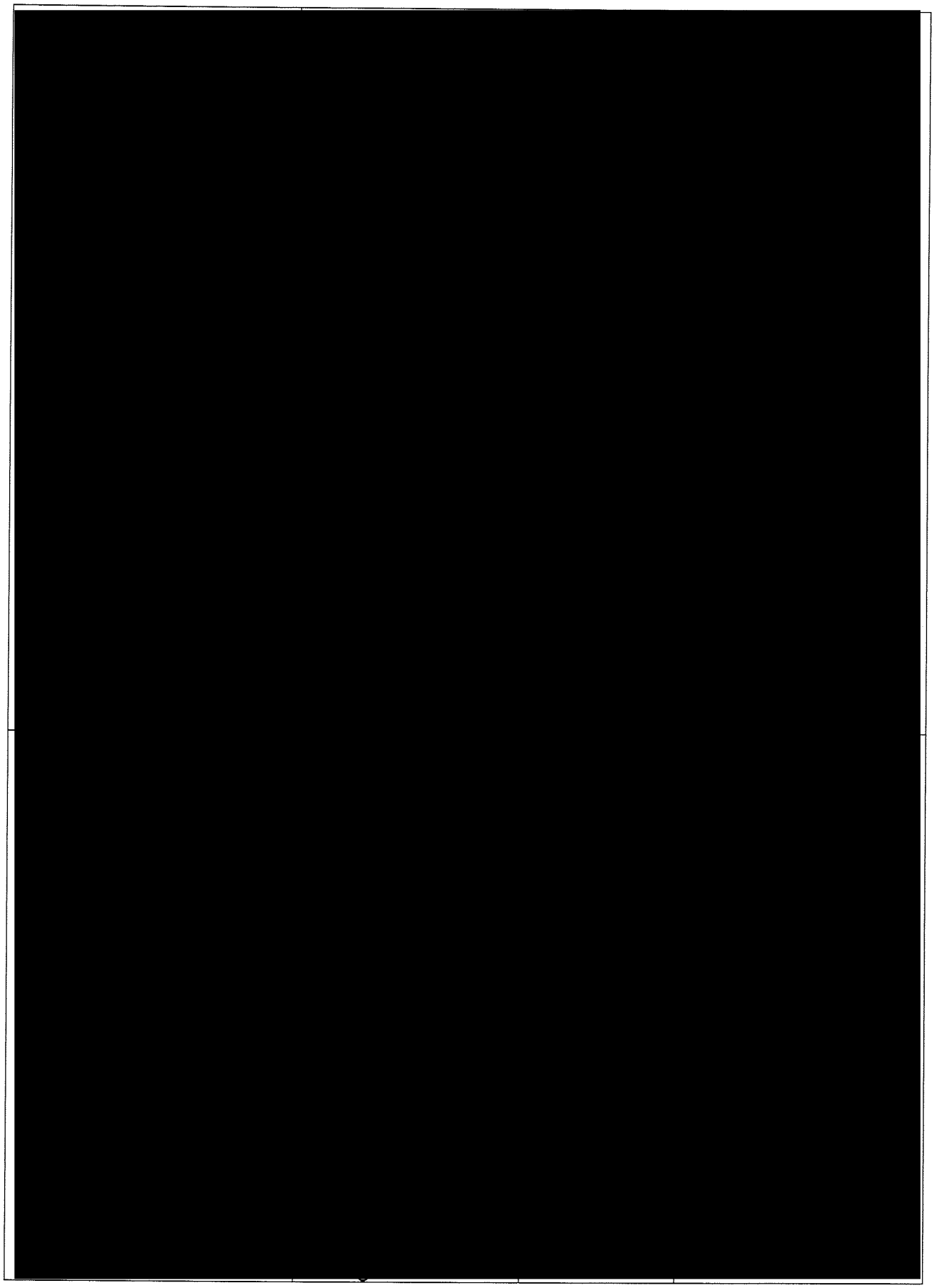
5. PLAN DE TRABAJO

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT01		
(Nombre del sistema A1) *	**Padrón de Proveedores y Contratistas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

[redacted]

[redacted]

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT002		
(Nombre del sistema A1) *	**Padrón de Prestadores de Servicios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			



[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT01
(Nombre del sistema A1)*	**Padrón de Proveedores y Contratistas**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	El sistema no entrega documentación física a otras entidades.
Transferencias mediante el traslado de soportes electrónicos:	El sistema no entrega ningún soporte electrónico a otras entidades.
Transferencias mediante el traslado sobre redes electrónicas:	**a)** El sistema no realiza ninguna transferencia de información a otras entidades.

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

Sistema UTICT01

1. La documentación que contiene los datos personales del sistema, no se recaba físicamente, por lo que no se requiere un espacio físico dedicado.

2. Al no contar con un espacio físico dedicado para el resguardo de la documentación, no existe tampoco un listado de personas con acceso a dicha área.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Sistema UTICT01

1. Los datos que se registran en las bitácoras:

a) No se cuenta con bitácoras electrónicas que registren la operación del sistema.

IV. REGISTRO DE INCIDENTES:

Sistema UTICT01

Se cuenta con una Mesa de ayuda, que registra los incidentes que pudieran surgir en la operación del sistema:

Sólo los usuarios de la propia UNAM, pueden solicitar el registro de un incidente.

El usuario que detecta que su información no aparece, escribe un correo a la Mesa de Ayuda de la UTICT (mesadeayuda@patronato.unam.mx), para la asignación de folio de atención.

1. Los datos que registra son:
   a) La persona que reporta el incidente;
   b) La dependencia a la que pertenece;
   c) Correo electrónico
2. Si el registro está en soporte electrónico, se carga nuevamente en el sistema
3. La recuperación de datos es autorizada de conformidad a los acuerdos de servicio (SLA) proporcionados por la Mesa de Ayuda de la UTICT.

V. ACCESO A LAS INSTALACIONES

Sistema UTICT01

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El edificio cuenta con un vigilante, que registra el nombre, la persona que visita, y la hora de entrada al edificio, de las personas que acceden a los diferentes pisos y oficinas.

Asimismo, el edificio cuenta con cámaras de videovigilancia.

2. **Seguridad perimetral interior** (centro de datos para soportes electrónicos):

1) Control biométrico para acceso a UTICT

2) Centro de Datos al interior de la UTICT, con acceso controlado por medios físicos (puerta y cerradura de seguridad).

3) Videovigilancia por detección de movimiento en áreas comunes de la UTICT y al interior del Centro de Datos.

4) No existe sistema de tratamiento de datos personales de videovigilancia

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

Sistema UTICT01

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema de tratamiento de datos personales.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Sistema UTICT01

El sistema tiene implementado un esquema de perfiles de usuario y contraseñas para control de acceso mediante una red electrónica.

1. El Modelo de control de acceso es obligatorio.

2. Los Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** Cuentan con un sistema operativo de red instalado en los equipos
- **b)** Proporcionan un manejo riguroso de perfiles de usuario y contraseñas
- **c)** Cifra los nombres de usuario y las contraseñas cuando los almacena

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** Dicho software tiene un manejo riguroso de perfiles de usuario y contraseñas
- **b)** Dicho software cifra las contraseñas cuando las almacena

4. Administración de perfiles de usuario y contraseñas:
- **a)** Los nuevos perfiles se dan de alta a través de la Mesa de Ayuda de la UTICT
- **b)** No existe el procedimiento para la autorización de creación de nuevos perfiles
- **c)** No se lleva a cabo registro de la creación de nuevos perfiles

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** Los usuarios no requieren acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema
- **b)** El administrador no requiere acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento
- **c)** El acceso remoto no autorizado, se mitiga al contar con una solicitud de acceso remoto que indica los sistemas que requiere conexión.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Sistema UTICT01

1. Si se realizan respaldos

   a) Completos e incrementales según el requerimiento

   b) Automáticos y bajo demanda manuales

   c) Diarios, semanales y anuales

2. El tipo de medios son cintas magnéticas y disco
3. Son archivados cifrados tanto en sitio (cintas magnéticas y disco) como fuera de sitio (copia remota a disco)
4. El responsable de realizar estas operaciones es la propia área universitaria.

IX. PLAN DE CONTINGENCIA

1. Se encuentra en desarrollo el Plan de Contingencia.

2. Está planificado una prueba de la puesta en marcha del Plan de Contingencia.

3. Para la ejecución del Plan de Contingencia se cuenta con un sitio alterno.
   a) Se trata de un sitio alterno caliente, que mantiene disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal, lo que supone tan solo unas cuantas horas para restaurar operaciones.
   b) El sitio alterno es propio y se encuentra instalado en una localización confidencial;

I. TRANSFERENCIAS DE DATOS PERSONALES

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT02
(Nombre del sistema A1)*	**Padrón de Prestadores de Servicios**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	Los Prestadores de Servicios de la UNAM, no entregan documentación física para su registro.
Transferencias mediante el traslado de soportes electrónicos:	Los Prestadores de Servicios de la UNAM, no entregan bajo ningún medio electrónico su información para su registro.
Transferencias mediante el traslado sobre redes electrónicas:	**a)** El sistema no realiza ninguna transferencia de información a otros sistemas.

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

Sistema UTICT02

1. La documentación que contiene los datos personales del sistema, no se recaba físicamente, por lo que no se requiere un espacio físico dedicado.

2. Al no contar con un espacio físico dedicado para el resguardo de la documentación, no existe tampoco un listado de personas con acceso a dicha área.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Sistema UTICT02

1. Los datos que se registran en las bitácoras:

a) No se cuenta con bitácoras electrónicas que registren la operación del sistema.

IV. REGISTRO DE INCIDENTES:

Sistema UTICT02

Se cuenta con una Mesa de ayuda, que registra los incidentes que pudieran surgir en la operación del sistema:

Sólo los usuarios de la propia UNAM, pueden solicitar el registro de un incidente.

El usuario que detecta que su información no aparece, escribe un correo a la Mesa de Ayuda de la UTICT (mesadeayuda@patronato.unam.mx), para la asignación de folio de atención.

1. Los datos que registra son:
   a) La persona que reporta el incidente;
   b) La dependencia a la que pertenece;
   c) Correo electrónico
2. Si el registro está en soporte electrónico, se carga nuevamente en el sistema
3. La recuperación de datos es autorizada de conformidad a los acuerdos de servicio (SLA) proporcionados por la Mesa de Ayuda de la UTICT.

V. ACCESO A LAS INSTALACIONES

Sistema UTICT02

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

El edificio cuenta con un vigilante, que registra el nombre, la persona que visita, y la hora de entrada al edificio, de las personas que acceden a los diferentes pisos y oficinas.

Asimismo, el edificio cuenta con cámaras de videovigilancia.

2. **Seguridad perimetral interior** (centro de datos para soportes electrónicos):

1) Control biométrico para acceso a UTICT

2) Centro de Datos al interior de la UTICT, con acceso controlado por medios físicos (puerta y cerradura de seguridad).

3) Videovigilancia por detección de movimiento en áreas comunes de la UTICT y al interior del Centro de Datos.

4) No existe sistema de tratamiento de datos personales de videovigilancia

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

Sistema UTICT02

No se cuenta con un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema de tratamiento de datos personales.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

Sistema UTICT02

El sistema tiene implementado un esquema de perfiles de usuario y contraseñas para control de acceso mediante una red electrónica.

1. El Modelo de control de acceso es obligatorio.

2. Los Perfiles de usuario y contraseñas en el sistema operativo de red:
- a) Cuentan con un sistema operativo de red instalado en los equipos
- b) Proporcionan un manejo riguroso de perfiles de usuario y contraseñas
- c) Cifra los nombres de usuario y las contraseñas cuando los almacena

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) Dicho software tiene un manejo riguroso de perfiles de usuario y contraseñas
b) Dicho software cifra las contraseñas cuando las almacena

4. Administración de perfiles de usuario y contraseñas:
a) Los nuevos perfiles se dan de alta a través de la Mesa de Ayuda de la UTICT
b) No existe el procedimiento para la autorización de creación de nuevos perfiles
c) No se lleva a cabo registro de la creación de nuevos perfiles

5. Acceso remoto al sistema de tratamiento de datos personales:
a) Los usuarios no requieren acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema
b) El administrador no requiere acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento
c) El acceso remoto no autorizado, se mitiga al contar con una solicitud de acceso remoto que indica los sistemas que requiere conexión.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Sistema UTICT02

1. Si se realizan respaldos

   a) Completos e incrementales según el requerimiento

   b) Automáticos y bajo demanda manuales

   c) Diarios, semanales y anuales

2. El tipo de medios son cintas magnéticas y disco
3. Son archivados cifrados tanto en sitio (cintas magnéticas y disco) como fuera de sitio (copia remota a disco)
4. El responsable de realizar estas operaciones es la propia área universitaria.

IX. PLAN DE CONTINGENCIA

1. Se encuentra en desarrollo el Plan de Contingencia.

2. Está planificado una prueba de la puesta en marcha del Plan de Contingencia.

3. No se tiene actualizado el ejercicio de puesta en marcha de los Planes de Contingencia.

a) Para la ejecución del Plan de Contingencia se cuenta con un sitio alterno.
b) Se trata de un sitio alterno caliente, que mantiene disponibles en todo momento la infraestructura, el equipo y el software; lo único que hace falta para iniciar operaciones son los datos y el personal, lo que supone tan solo unas cuantas horas para restaurar operaciones.
c) El sitio alterno es propio y se encuentra instalado en una localización confidencial;

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

Sistema UTICT01

No se cuenta con herramientas para el monitoreo de la protección de datos personales.

Sistema UTICT02

No se cuenta con herramientas para el monitoreo de la protección de datos personales.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Sistema UTICT01

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

Este ejercicio de 2024 se tiene planificado llevar a cabo una capacitación presencial a los responsables de la seguridad de los datos personales de nuestras dependencias.

Fecha: Segundo semestre de 2024
Lugar: Aula de Capacitación de la Dirección General de Control Presupuestal
Duración: 3 días
Cobertura: Responsables de la seguridad de los datos personales de la Tesorería y las Direcciones Generales de Control Presupuestal y de Finanzas.

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

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT01		
(Nombre del sistema A1)*	**Padrón de Proveedores y Contratistas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Elaborar una publicación para sensibilizar al personal de la importancia de la protección de los datos personales	*Uno o varios posters para publicar de forma física en los pizarrones de las áreas y su envío por correo electrónico*	*Inicia 2 de agosto 2024* *Termina 11 diciembre 2024*	*Bimestral* *Envío de las publicaciones por correo electrónico al personal de la Tesorería, DGCP y DGF* *En instalaciones físicas: Tesorería, DGCP y DGF*

Sistema UTICT02

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

Este ejercicio de 2024 se tiene planificado llevar a cabo una capacitación presencial a los responsables de la seguridad de los datos personales de nuestras dependencias.

Fecha: Segundo semestre de 2024
Lugar: Aula de Capacitación de la Dirección General de Control Presupuestal
Duración: 3 días
Cobertura: Responsables de la seguridad de los datos personales de la Tesorería y las Direcciones Generales de Control Presupuestal y de Finanzas.

8.2 Programa de difusión de la protección a los datos personales

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT02		
(Nombre del sistema A1)*	**Padrón de Prestadores de Servicios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Elaborar una publicación para sensibilizar al personal de la importancia de la protección de los datos personales	*Uno o varios posters para publicar de forma física en los pizarrones de las áreas y su envío por correo electrónico*	*Inicia 2 de agosto 2024* *Termina 11 diciembre 2024*	*Bimestral* *Envío de las publicaciones por correo electrónico al personal de la Tesorería, DGCP y DGF* *En instalaciones físicas: Tesorería, DGCP y DGF*

9. MEJORA CONTINUA

Sistema UTICT01

9.1 Actualización y mantenimiento de sistemas de información

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT01		
(Nombre del sistema A1)*	**Padrón de Proveedores y Contratistas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Migración del padrón de proveedores a la plataforma tecnológica Odoo.	Desarrollo de un nuevo padrón de proveedores, desarrollado bajo la tecnología Odoo. Alineado con los	Pendiente la fecha de implementación	Actualización de la plataforma tecnológica con la que está construido el Padrón de Proveedores y Contratistas.

	objetivos de la Tesorería.		En esta plataforma, permitirá identificar los usuarios y las tareas que realizan, haciendo más sencillo la auditoria del Padrón.

9.2 Actualización y mantenimiento de equipo de cómputo

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT01		
(Nombre del sistema A1)*	**Padrón de Proveedores y Contratistas**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sustitución de equipo de cómputo	*El equipo de cómputo tiene una vida útil de 3 años. Después de este tiempo, se sustituye por uno nuevo.*	*Bajo demanda. El tiempo de duración de la actividad es de 2 días.*	*Se mitiga el riesgo por tener equipo de cómputo obsoleto*
Actualización de software de los equipos de cómputo	*El equipo de cómputo es actualizado con los parches que libera el fabricante.*	*Cada que el fabricante libera una actualización*	*Se resuelven los incidentes de seguridad identificados por el fabricante.*
Mantenimiento a servidores físicos	*Se realiza mantenimiento preventivo a servidores físicos*	*2hrs, cada 6 meses*	*Se mantienen 3 servidores físicos productivos en condiciones operativas*

9.3 Procesos para la conservación, preservación y respaldos de información

745.01 Unidad de Coordinación Tesorería	
Identificador único*	UTICT01

(Nombre del sistema A1)*	Padrón de Proveedores y Contratistas	
Proceso*	**Descripción***	**Responsable***
Respaldo diario de BD	*Se realiza respaldo de la BD a disco localmente, posteriormente a cinta y a almacenamiento remoto*	*a) Alvaro Reyes Cervantes* *b) 1 día*
Respaldo semanal de BD	*Se realiza respaldo de la BD a disco localmente, posteriormente a cinta y a almacenamiento remoto*	*a) Alvaro Reyes Cervantes* *b) 1 día*

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

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT01	
(Nombre del sistema A1)*	Padrón de Proveedores y Contratistas	
Proceso*	**Descripción***	**Responsable***
Desinstalación de software con licenciamiento	Se desinstala el software que cuenta con licenciamiento activo, (MS Office, Antivirus, etc) a fin de liberar correctamente la licencia.	a) Responsable informático del área a la que pertenece el equipo b) 1 día
Borrado seguro del disco	Se realiza formato a bajo nivel del disco duro del equipo a dar de baja, mediante herramientas de software libre.	a) Responsable informático del área a la que pertenece el equipo b) 1 día

9.1 Actualización y mantenimiento de sistemas de información

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT02		
(Nombre del sistema A1)*	**Padrón de Prestadores de Servicios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Migración del padrón de proveedores a la plataforma tecnológica Odoo.	Desarrollo de un nuevo padrón de proveedores, desarrollado bajo la tecnología Odoo. Alineado con los objetivos de la Tesorería.	Pendiente la fecha de implementación	Actualización de la plataforma tecnológica con la que está construido el Padrón de Prestadores de Servicio. En esta plataforma, permitirá identificar los usuarios y las tareas que realizan.

9.2 Actualización y mantenimiento de equipo de cómputo

745.01 Unidad de Coordinación Tesorería			
Identificador único*	UTICT02		
(Nombre del sistema A1)*	**Padrón de Prestadores de Servicios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Sustitución de equipo de cómputo	*El equipo de cómputo tiene una vida útil de 3 años. Después de este tiempo, se sustituye por uno nuevo.*	*Bajo demanda. El tiempo de duración de la actividad es de 2 días.*	*Se mitiga el riesgo por tener equipo de cómputo obsoleto*

Actualización de software de los equipos de cómputo	*El equipo de cómputo es actualizado con los parches que libera el fabricante.*	*Cada que el fabricante libera una actualización*	*Se resuelven los incidentes de seguridad identificados por el fabricante.*
Mantenimiento a servidores físicos	*Se realiza mantenimiento preventivo a servidores físicos*	*2hrs, cada 6 meses*	*Se mantienen 3 servidores físicos productivos en condiciones operativas*

9.3 Procesos para la conservación, preservación y respaldos de información

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT02	
(Nombre del sistema A1)*	**Padrón de Prestadores de Servicios**	
Proceso*	**Descripción***	**Responsable***
Respaldo diario de BD	*Se realiza respaldo de la BD a disco localmente, posteriormente a cinta y a almacenamiento remoto*	*c) Alvaro Reyes Cervantes* *d) 1 día*
Respaldo semanal de BD	*Se realiza respaldo de la BD a disco localmente, posteriormente a cinta y a almacenamiento remoto*	*c) Alvaro Reyes Cervantes* *d) 1 día*

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

745.01 Unidad de Coordinación Tesorería		
Identificador único*	UTICT02	
(Nombre del sistema A1)*	**Padrón de Prestadores de Servicios**	
Proceso*	**Descripción***	**Responsable***
Desinstalación de software con licenciamiento	*Se desinstala el software que cuenta con licenciamiento activo, (MS Office, Antivirus, etc) a fin de liberar correctamente la licencia.*	*b) a) Responsable informático del área a la que pertenece el equipo b) 1 día*
Borrado seguro del disco	*Se realiza formato a bajo nivel del disco duro del equipo a dar de baja, mediante herramientas de software libre.*	*a) Responsable informático del área a la que pertenece el equipo b) 1 día*

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

Sistema UTICT01

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Los datos personales que podrían ser cancelados, se refieren a la información de ubicación de la persona, o los datos bancarios de la cuenta a la que se realizan los pagos, la cual a petición de un Proveedor o Contartista podrían ser eliminados del Sistema de tratamiento de datos personales.

La información fiscal de la persona a la que se está realizando los pagos, no pueden ser eliminadas del Sistema, ya que es utilizada por un periodo de al menos 15 años, para la emisión de reportes solicitados por las entidades fiscalizadoras.

b) El motivo de la petición de cancelación de la guarda de los datos personales, debe ser plenamente justificado por el dueño de la información a través de una solicitud entregada a esta Dependencia o mediante la orden de una autoridad judicial.

La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que esta Dependencia conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.

Bajo este contexto, la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos, en el cual no se podrá disponer de tales datos en la misma medida en que la podría hacerse por el área universitaria de estar en operación el Sistema de tratamiento de datos personales.

La cancelación de sistema de tratamiento de datos personales debe considerar lo establecido en los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México, así como el Catálogo de disposición documental de la Universidad del año respectivo, a fin de atender al valor documental de la información contenida en el mismo.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Una vez que se cuenta con un dictamen a favor del interesado, de forma inmediata se procede al bloqueo de la información señalada, misma que se encontrará en un estado de bloqueo por un periodo de hasta 15 años de conformidad con la normatividad de esta área Universitaria.

El bloqueo se realizará en el sistema informático de padrón de Proveedores y Contratistas de la UNAM, en donde no permitirá el despliegue de la información solicitada, sin que esto, ocasione la pérdida de información del Proveedor o Contratista, ni la integridad del propio sistema.

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

Una vez aplicado el procedimiento de bloqueo de la información, el área informática de esta Dependencia, a través del área de Calidad, verificará el bloqueo de la información solicitada, a través de una prueba focalizada al momento de la aplicación del bloqueo y anualmente a través de verificaciones rutinarias.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Una vez cumplido 15 años más un día de la última utilización (registro nuevo o consulta para integración en algún reporte) del dato bloqueado del Proveedor o Contratista de la UNAM, podrá ser eliminado en forma definitiva de los registros del sistema.

El proceso de identificación de los registros que caen en el supuesto del párrafo anterior, se correrá una vez al año, previo a la puesta en marcha de un nuevo ejercicio fiscal, a través de algún procedimiento sistemático, que al efecto desarrolle el área informática de esta Dependencia.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se lleva a cabo la sobreescritura con espacios vacíos de la información objeto de la solicitud de cancelación de datos personales, en la tabla que proporciona la información. Con esta acción se asegura la consistencia de la base de datos y la operabilidad de cualquier funcionalidad del propio Sistema.

Sistema UTICT02

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Los datos personales que podrían ser cancelados, se refieren a la información de ubicación de la persona, o los datos bancarios de la cuenta a la que se realizan los pagos, la cual a petición de un Prestador de Servicio podrían ser eliminados del Sistema de tratamiento de datos personales.

La información fiscal de la persona a la que se está realizando los pagos, no pueden ser eliminadas del Sistema, ya que es utilizada por un periodo de al menos 15 años, para la emisión de reportes solicitados por las entidades fiscalizadoras.

b) El motivo de la petición de cancelación de la guarda de los datos personales, debe ser plenamente justificado por el dueño de la información a través de una solicitud entregada a esta Dependencia o mediante la orden de una autoridad judicial.

La cancelación da lugar al bloqueo de los datos, esto es, el periodo en el que esta Dependencia conservará los datos para efectos de responsabilidades, el cual será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad de aplicable y, cumplido este plazo, deberá procederse a la supresión del dato que implica el borrado físico del mismo.

Bajo este contexto, la cancelación no supone automáticamente la supresión o borrado físico de los datos, sino que se debe determinar un período o fase previa de bloqueo de los datos, en el cual no se podrá disponer de tales datos en la misma medida en que la podría hacerse por el área universitaria de estar en operación el Sistema de tratamiento de datos personales.

La cancelación de sistema de tratamiento de datos personales debe considerar lo establecido en los Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México, así como el Catálogo de disposición documental de la Universidad del año respectivo, a fin de atender al valor documental de la información contenida en el mismo.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Una vez que se cuenta con un dictamen a favor del interesado, de forma inmediata se procede al bloqueo de la información señalada, misma que se encontrará en un estado de bloqueo por un periodo de hasta 15 años de conformidad con la normatividad de esta área Universitaria.

El bloqueo se realizará en el sistema informático de padrón de Prestadores de Servicio de la UNAM, en donde no permitirá el despliegue de la información solicitada, sin que esto, ocasione la pérdida de información del Proveedor o Contratista, ni la integridad del propio sistema.

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

Una vez aplicado el procedimiento de bloqueo de la información, el área informática de esta Dependencia, a través del área de Calidad, verificará el bloqueo de la información solicitada, a través de una prueba focalizada al momento de la aplicación del bloqueo y anualmente a través de verificaciones rutinarias.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

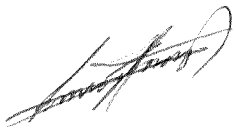
Una vez cumplido 15 años más un día de la última utilización (registro nuevo o consulta para integración en algún reporte) del dato bloqueado del Prestador de Servicio de la UNAM, podrá ser eliminado en forma definitiva de los registros del sistema.

El proceso de identificación de los registros que caen en el supuesto del párrafo anterior, se correrá una vez al año, previo a la puesta en marcha de un nuevo ejercicio fiscal, a través de algún procedimiento sistemático, que al efecto desarrolle el área informática de esta Dependencia.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Se lleva a cabo la sobreescritura con espacios vacíos de la información objeto de la solicitud de cancelación de datos personales, en la tabla que proporciona la información. Con esta acción se asegura la consistencia de la base de datos y la operabilidad de cualquier funcionalidad del propio Sistema.

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Firma de quienes revisaron el presente documento:
Responsable del desarrollo:	**Juan Mariano López López** Coordinador de Infraestructura y Comunicaciones Tel. 55 5622 6435 Mariano.lopez@patronato.unam.mx	
Revisó:	**Jesús Alberto Ojeda Arévalo** Jefe del Departamento de Redes y Comunicaciones Tel. 55 56226393 Ext. 48238 Jesus.Ojeda@patronato.unam.mx	
Autorizó:	**Mtro. Luis Arturo López Caballero** Director de la Unidad de Tecnologías de la Información y Comunicaciones de la Tesorería Tel. 55 56226393 Luis.lopez@patronato.unam.mx	
Fecha de aprobación:	15 de enero de 2024	
Fecha de actualización:	31 de enero de 2024 Ver. 1.2	