Documento de Seguridad

DGDU-SGSDP-DS

Tabla de autorización

Elaboró y Revisó

Responsable de Seguridad de Datos Personales

Tel: 5622 0555 ext. 41761
aaron.altamirano@deporte.unam.mx

Mtro. Aarón Iván Altamirano García

Coordinadora Jurídica

Tel: 5622 0505
isabel.barragan@deporte.unam.mx

Lic. Isabel Barragán Isidro

Aprobó

Director General del Deporte Universitario

Tel: 5622-0047
afvarela@unam.mx

Lic. Alejandro Fernández Varela Jiménez

Fecha de emisión: 10 de agosto de 2022

Índice

0. Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Dirección General del Deporte Universitario con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta dependencia universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.

El formato de este documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, se considera la estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información".

1. Objetivo

Describir las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales de la Dirección General del Deporte Universitario de la Universidad Nacional Autónoma de México (DGDU), desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados mediante cualquiera de los siguientes tipos de soportes:

a) En soportes físicos.
b) En soportes electrónicos.
c) En redes de datos.

2. Términos, definiciones y abreviaturas

2.1 Términos y definiciones

2.1.1 Activo: Todo elemento de valor para la Universidad, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

2.1.2 Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el Responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de éstos.

2.1.3 Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

2.1.4 Borrado seguro: Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

2.1.5 Ciclo vital del documento: Las tres fases por las que atraviesan los documentos de archivo, sea cual sea su soporte, desde su recepción o generación hasta su conservación permanente o baja documental, a saber: archivo de trámite, archivo de concentración y archivo histórico.

2.1.6 Confidencialidad: Es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por el Área Universitaria respectiva.

2.1.7 Control de seguridad en la red: Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales.

2.1.8 Disponibilidad: Es el principio de seguridad de la información que consiste en ser accesible y utilizable a solicitud de personas o procesos autorizados por el Área Universitaria respectiva.

2.1.9 Documento de seguridad: 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.

2.1.10 Encargado: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

2.1.11. Evaluación de impacto en la protección de datos personales: Documento mediante el cual las Áreas Universitarias que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales sobre determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los Responsables y Encargados, previstos en la normativa aplicable.

2.1.12 Integridad: Es el principio de seguridad de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

2.1.13 Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales;

2.1.14 Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

2.1.15 Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma, asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

2.1.16 Medidas de seguridad técnicas: Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en formato digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

2.1.17 Red de datos: Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

2.1.18 Responsable: Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

2.1.19 Seguridad de la información: La preservación de la confidencialidad, integridad y disponibilidad de la información, que puede abarcar además otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

2.1.20 Servicios de nube privada: Modelo de servicio de tecnología de información proporcionados bajo demanda a las Áreas Universitarias, en infraestructura propiedad de la Universidad y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

2.1.21 Servicios de nube pública: Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena a la Universidad.

2.1.22 Sistema de Gestión de Seguridad de Datos Personales: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales.

2.1.23 Sistemas para el tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

2.1.24 Soporte: Medio, ya sea electrónico o físico, en el que se registra y guarda información, como lo es: el papel, así como los audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

2.1.25 Soportes electrónicos: Son los medios de almacenamiento accesibles sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs, DVDs y Blue-rays), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

2.1.26 Soportes físicos: Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías placas radiológicas, carpetas, expedientes, entre otros; XXXVII. Supresión: La erradicación del registro de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el Responsable.

2.1.27 Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del Responsable o del Encargado.

2.1.28 Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

2.1.29 Vulneración de seguridad: En cualquier fase del tratamiento de datos, se considera la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

2.2 Abreviaturas

2.2.1 DGDU: Dirección General del Deporte Universitario de la UNAM

2.2.2 SGSDP: Sistema de Gestión de Seguridad de Datos Personales

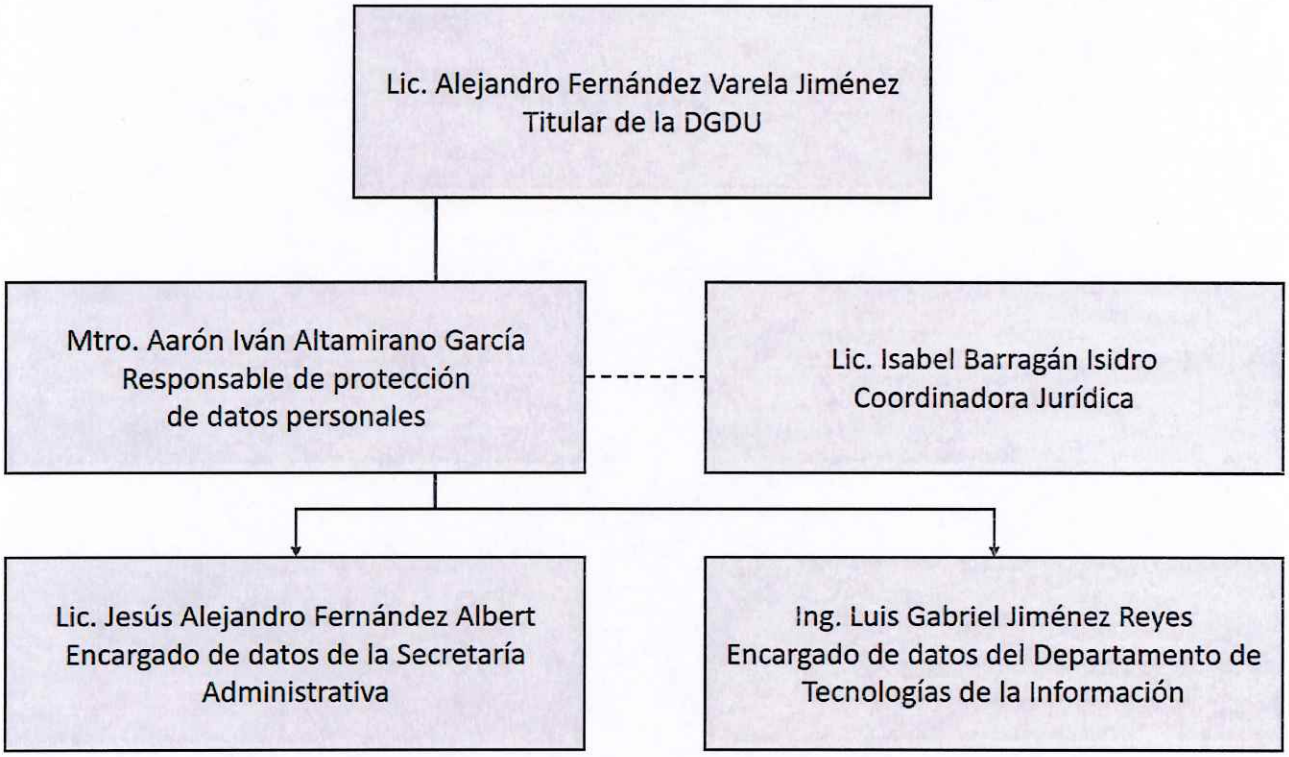
3. Alcance

Aplica a todas las áreas administrativas, académicas y de servicio que tienen en su poder datos personales y datos personales sensibles.

3.1 Funciones y Responsabilidades

En el SGSDP de la DGDU, la responsabilidad, autoridad e interrelaciones del personal que trata datos personales, se mantiene con la siguiente cadena de rendición de cuentas:

a) Organigrama del SGSDP



Las funciones y responsabilidades generales de los integrantes del SGSDP son:

Titular

Supervisar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla de acuerdo a éste Documento de Seguridad.

Responsables

Verificar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla en sus áreas específicas (administrativas, académicas y/o de servicio) de acuerdo a éste Documento de Seguridad.

Encargados:

Mantener el Sistema de Gestión de Seguridad de Datos Personales en sus áreas específicas (administrativas, académicas y/o de servicio) de acuerdo a éste Documento de Seguridad.

Usuarios:

Utilizar el Sistema de Gestión de Seguridad de Datos Personales en sus áreas específicas (administrativas, académicas y/o de servicio) de acuerdo a éste Documento de Seguridad.

En la Dirección General del Deporte Universitario, los roles son:

Rol	Figura
Titular	Titular de la DGDU
Responsable	Responsable designado por el Titular de la DGDU
Encargado	De acuerdo al uso de los datos personales definidos en el **Anexo 1**: Secretario Administrativo Departamento de Tecnologías de la Información
Usuarios	Definido en el **Anexo 1** de acuerdo al uso de datos personales

3.2 Sistema de Gestión de Seguridad de Datos Personales

3.2.1 La DGDU establece y mantiene un Sistema de Gestión de Seguridad de Datos Personales y documenta sus políticas, sistemas, programas, procedimientos e instrucciones necesarias para asegurar la integridad, confidencialidad y disponibilidad de los datos personales, según el REGLAMENTO DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO publicado el 26 de agosto de 2016 y a las NORMAS COMPLEMENTARIAS SOBRE MEDIDAS DE SEGURIDAD TÉCNICAS, ADMINISTRATIVAS Y FÍSICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD publicadas el 10 de enero de 2020.

Política del Sistema de Seguridad de Datos Personales El Instituto de Física se compromete a cumplir con las medidas de seguridad para la protección de datos personales desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados mediante soportes físicos, electrónicos o en redes de datos.

Objetivo del SGSDP

El objetivo del SGSDP es: Asegurar la integridad, confidencialidad y disponibilidad de la información que contengan datos personales.

3.2.2 El SGSDP cuenta con un inventario con información sobre el tratamiento de datos personales por área administrativa, académica o de servicio responsable, que se encuentra en el **Anexo 1** y que considera:

I. El catálogo de recursos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales;
III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. La lista de funcionarios o empleados universitarios que tienen acceso a los sistemas de tratamiento; VI. Los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estas.

3.2.3 En dicho inventario se incluye el ciclo de vida de los datos personales conforme a las siguientes etapas:

- La obtención de los datos personales;
- El almacenamiento de los datos personales;
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- El bloqueo de los datos personales, en su caso, y
- La cancelación, supresión o destrucción de los datos personales.

3.2.4 Cada Sistema de Tratamiento sirve para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos. El detalle de cada sistema de tratamiento de datos personales por área administrativa, académica o de servicio responsable se encuentra en el **Anexo 1** de éste documento.

3.3 Análisis de Riesgos

3.3.1 La DGDU realiza un análisis de riesgos del tratamiento de los datos personales que se encuentra en el **Anexo 2** y de acuerdo a la siguiente metodología:

3.3.2 Los riesgos sobre el tratamiento de datos personales se detectan por área administrativa, académica o de servicio y por cualquier persona que dé tratamiento de datos personales.

3.3.3 Se realiza la "Matriz de Riesgos Por Tratamiento de Datos Personales donde se identifica:

Tratamiento de datos personales
Clave de tratamiento de datos personales conforme al inventario.

Riesgo probable
Enunciado del riesgo identificado, tomando en cuenta:

- Los requerimientos regulatorios, legales y reglamentarios.
- El valor de los datos personales de acuerdo a si son sensibles
- no y su ciclo de vida;
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- Los siguientes factores:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;
- El número de titulares;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Causa probable

La causa probable del riesgo. Pueden usarse las herramientas del análisis de causa raíz como los 5 por qué's, diagrama de Ishikawa, entre otros.

Probabilidad

La probabilidad subjetiva de que ocurra el riesgo. Es la posibilidad de que ocurra una vulneración de seguridad a los datos personales. Para determinar su probabilidad se toma en cuenta el número de áreas en las que se ha identificado el riesgo. Criterio cuya escala es:

Probabilidad	Escala
De 1 a 3 áreas	Bajo
De 4 a 5 áreas	Medio
De 6 a 7 áreas	Alto

Tabla 1. Escala de Probabilidad.

Impacto

El impacto del riesgo se refiere al impacto a las consecuencias negativas, daño o afectación para los titulares que pudieran derivar de una vulneración de seguridad ocurrida en los datos personales. Criterio cuya escala es:

Impacto	Escala
No impacta a la integridad, confidencialidad ni disponibilidad de datos personales.	Bajo
Impacta a la integridad, confidencialidad o disponibilidad de datos personales.	Medio
Impacta a la integridad, confidencialidad y disponibilidad de datos personales.	Alto

Tabla 2. Escala de Impacto.

Cálculo de Nivel de valor de Riesgo

Para éste caso, se asume que el Impacto y la Probabilidad tienen el mismo valor para la valuación del riesgo.
Se identifica en la gráfica Probabilidad vs Impacto la zona en la que se encuentra el riesgo identificado para asignarle su nivel de valor de riesgo, que definirá la prioridad con la que se tratarán los riesgos, de la siguiente manera:

Gráfica 1. Probabilidad vs Impacto.

Nivel de Riesgo	Prioridad
Bajo	Planificar acción y documentar en no más de 20 días hábiles desde su detección.
Medio	Planificar acción y documentar en no más de 10 días hábiles desde su detección.
Alto	Planificar acción y documentar inmediatamente.

Tabla 3. Nivel de prioridad del riesgo.

3.3.3 Una vez identificados los riesgos y su prioridad, se define el tratamiento del riesgo, el cual puede ser:

- **Mitigar:** acciones que minimicen los efectos que pudieran surgir por los riesgos.
- **Eliminar:** acciones que desaparezcan los efectos del riesgo.
- **Transferir:** acciones que trasladen el riesgo. Generalmente ocurre cuando no se tiene control total sobre la situación.
- **Aceptar:** Generalmente ocurre cuando no se tiene control total sobre la situación.

3.3.4. Una vez identificado el tratamiento del riesgo se plantean acciones para mitigar, eliminar, transferir o aceptar el riesgo, debiendo considerar los controles de seguridad física, administrativa y técnica para la protección de datos personales.

3.3.5 Cuando se identifique algún riesgo se debe notificar al Responsable de Seguridad de Datos Personales para que lo integre a la Matriz de Riesgos.

3.4 Análisis de Brecha

La DGDU realiza un análisis de brecha que se encuentra en el **Anexo 3** considerando:

- Las medidas de seguridad existentes y efectivas;
- El nivel óptimo de medidas de seguridad y
- Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

3.5 Plan de Trabajo

3.5.1 La DGDU cuenta con un plan de trabajo que 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 detectado.

Lo anterior, considerando los recursos asignados, el personal interno y externo al área, así como las fechas establecidas para la implementación de los controles de seguridad nuevos o faltantes.

El Plan de Trabajo se encuentra en el **Anexo 4** de este documento.

3.6 Medidas de seguridad para la protección de datos personales

3.6.1 La DGDU implementa medidas de seguridad técnicas, administrativas y físicas para asegurar la protección de los datos personales presentadas en el **Anexo 4**.

3.7 Capacitación

Dentro de la capacitación para la comunidad de la DGDU, se estarán estableciendo:

- Charlas informativas sobre temas de protección de datos personales
- Correos masivos con información del tema
- Generación de elementos gráficos con información de protección de datos personales.
- La capacitación debe de incluir los siguientes temas:
  i. Los requerimientos y actualizaciones del sistema de gestión;
  ii. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;
  iii. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
  iv. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

4. Anexos

Anexos	Descripción
Anexo 1	Inventario
Anexo 2	Análisis de Riesgos
Anexo 3	Análisis de Brecha
Anexo 4	Planes de Trabajo

Tabla 4. Lista de anexos.

5. Identificación de los cambios

Fecha de revisión	Versión	Descripción de la modificación	Página/Sección
10 de agosto de 2022	1.0	Versión Inicial	

Tabla 5. Control de cambios del Documento de Seguridad.

ANEXO 1

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Departamento de Tecnologías de la Información de la DGDU	
Identificador único	**REDP-01**
Nombre del sistema A1	**REDPUMA**
Datos personales (sensibles o no) contenidos en el sistema:	CURP, Apellido paterno, Apellido materno, Nombres, Fecha de nacimiento, Peso, Estatura, Calle, Colonia, CP, Estado civil, Celular, Tipo de usuario, Número de cuenta, Plantel, Tipo de sangre, Alergias, tipo de servicio médico, número de póliza, avisar en caso de emergencia, teléfono en caso de accidente, Fecha del registro, Edad.
Responsable:	Departamento de Tecnologías de la Información
Nombre:	Ing. Luis Gabriel Jiménez Reyes.
Cargo:	**Jefe de Tecnologías de la Información**
Funciones:	**Desarrollar el sistema de información de forma segura para proteger la integridad de los datos personales**
Obligaciones:	Mantener actualizados los sistemas operativos del servidor, así como llevar a cabo revisiones periódicas para mantenimientos de acceso a la información.
	Encargados:
Nombre del Encargado 1	Ing. Brian Belmontes Botello
Cargo:	**Desarrollo de sistemas y página web**
Funciones:	**Desarrollar el sistema de información de forma segura para proteger la integridad de los datos personales**
Obligaciones:	Diseñar sistemas de información seguros para proteger la integridad de los datos del sistema REDPUMA.
Nombre del Encargado 2	
Cargo:	
Funciones:	
Obligaciones:	
	Usuarios:
Nombre del Usuario 1	VALETÍN ALBARRÁN ULLOA
Cargo:	Director de Cultura Física
Funciones:	Supervisar el registro de carreras y cursos
Obligaciones:	Llevar a cabo actividades recreativas como carreras y cursos
Nombre del Usuario 2	LUIS BOLAÑOS
Cargo:	Coordinador de Deporte Representativo
Funciones:	Registro de deportistas a eventos nacionales
Obligaciones:	Proporcionar vigencia a deportistas para competencias

Nombre del sistema A2	SIEM
Datos personales contenidos en el sistema:	Antecedentes heredofamiliares, antecedentes heredofamiliares patológicos, antecedentes ginecológicos, antecedentes genito-urinarios, antecedentes deportivos, antecedentes personales patológicos.
Responsable:	Dirección de Medicina del Deporte
Nombre:	Dra. María Cristina Rodríguez Gutiérrez
Cargo:	Directora
Funciones:	Ingresar información de los usuarios que desean hacer una evaluación morfofuncional
Obligaciones:	Administrar los datos médicos registrados de cada paciente
	Encargados:
Nombre del Encargado 1	Fabiola Núñez Zurita
Cargo:	Coordinadora de Evaluación
Funciones:	Coordinar el registro de los pacientes a evaluarse y darlos de alta en el sistema
Obligaciones:	Coordinar que cada médico ingrese al módulo correspondiente para ingresar la información médica.
Nombre del Encargado 2	Ana Rosa Becerra Pérez
Cargo:	Diagnóstico Integral
Funciones:	Revisar cada expediente y toda la evaluación morfofuncional para emitir un diagnóstico final
Obligaciones:	Se envía por correo electrónico al destinatario su resultado o se entrega en físico al mismo.

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

Departamento de Tecnologías de la Información de la DGDU	
Identificador único	REDP-01
Nombre del sistema A1	REDPUMA
Tipo de soporte:	Electrónico
Descripción:	Base de datos relacional en sqlserver
Características del lugar donde se resguardan los soportes:	[redacted]
Nombre del sistema A2	SIEM
Tipo de soporte:	Electrónico
Descripción:	Base datos relacional en sqlserver
Características del lugar donde se resguardan los soportes:	[redacted]
Nombre del sistema A3	

ANEXO 2

3. ANÁLISIS DE RIESGOS

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	*REDPUMA*	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	*SIEM*	
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

ANEXO 3

4. ANÁLISIS DE BRECHA

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	*REDPUMA*	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

Denominación del área específica del Área Universitaria A		
Identificador único	*REDP-01*	
Nombre del sistema A2	*SIEM*	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]	[redacted]	[redacted]

ANEXO 4

5. PLAN DE TRABAJO

Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A1	*REDPUMA*		
Actividad	**Descripción**	**Duración**	Cobertura
[redacted]	[redacted]	[redacted]	[redacted]
Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A2	*SIEM*		
Actividad	**Descripción**	**Duración**	Cobertura
[redacted]	[redacted]	[redacted]	[redacted]

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Departamento de Tecnologías de la Información de la DGDU	
Identificador único	*REDP-01*
Nombre del sistema A1	*REDPUMA*
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	[redacted]
Transferencias mediante el traslado de soportes electrónicos:	[redacted]
Transferencias mediante el traslado sobre redes electrónicas:	[redacted]
Nombre del sistema A2	*SIEM*
Transferencias mediante el traslado de soportes físicos:	[redacted]

Transferencias mediante el traslado de soportes electrónicos:	[redacted]
Transferencias mediante el traslado sobre redes electrónicas:	[redacted]

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

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
2. Si las bitácoras están en soporte físico o en soporte electrónico;
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
4. La manera en que asegura la integridad de las bitácoras, y
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

III. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;

3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

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

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica? [redacted]
b) ¿Cómo las autentifica? [redacted]
c) ¿Cómo les autoriza el acceso? [redacted]

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

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica? [redacted]
2. ¿Cómo las autentifica? [redacted]
3. ¿Cómo les autoriza el acceso? [redacted]

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

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

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

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?
c) ¿Está basado en roles (perfiles) o grupos? Está basado en roles.
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? [redacted]
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? [redacted]
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? [redacted]

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? [redacted]
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? [redacted]

4. Administración de perfiles de usuario y contraseñas:
- **a)** ¿Quién da de alta nuevos perfiles? [redacted]
- **b)** ¿Quién autoriza la creación de nuevos perfiles? [redacted]
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? [redacted]

5. Acceso remoto al sistema de tratamiento de datos personales:
- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? [redacted]
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? [redacted]
- **c)** ¿Cómo se evita el acceso remoto no autorizado? [redacted]

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos_x_, diferenciales ___ o incrementales___;
   - **b)** De forma automática _x___ o Manual _____,
   - **c)** Periodicidad con que los realiza: _lunes a viernes_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad. En discos duros se respaldan las bases de datos.

3. Cómo y dónde archiva esos medios. Se hacen tareas automatizadas y el servidor las ejecuta en los días y horarios indicados. [redacted]
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). [redacted]

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío); [redacted]
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

PLAN DE CONTINGENCIA.

Para el sistema A1 y A2, se tiene una imagen del servidor Windows y respaldos de los sistemas, bases de datos y contamos con un servidor alterno. El sitio es propio y el tiempo de restauración podría ser de 3 días.

Continuar los mismos pasos con el siguiente SISTEMA A2. SIEM.

I. Transferencias de datos personales
II. Resguardo de sistemas de tratamiento de datos personales con soportes físicos
III. Bitácoras para accesos y operación cotidiana
IV. Registro de incidentes
V. Acceso a las instalaciones
VI. Actualización del sistema de tratamiento de datos personales
VII. Perfiles de usuario y contraseñas
VIII. Procedimientos de respaldo y recuperación de datos
IX. Plan de contingencia

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

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

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	*REDPUMA*	
Recurso	Descripción	Control
[redacted]	[redacted]	[redacted]
Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	*SIEM*	
Recurso	Descripción	Control
[redacted]	[redacted]	[redacted]

7.2. Procedimiento para la revisión de las medidas de seguridad

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	**REDPUMA**	
Medida de seguridad	Procedimiento	Responsable
[redacted]	[redacted]	[redacted]

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	**SIEM**	
Medida de seguridad	Procedimiento	Responsable
[redacted]	[redacted]	[redacted]

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

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	**REDPUMA**	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]
Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	**SIEM**	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]

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

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	**REDPUMA**	
Medida de seguridad	Acciones	**Responsable**
[redacted]	[redacted]	[redacted]
Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	**SIEM**	
Medida de seguridad	Acciones	**Responsable**
[redacted]	[redacted]	[redacted]

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A1	REDPUMA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Por parte de la DGP se tomó el curso correspondiente	*Curso de protección de los datos personales en la UNAM*	*Duración: 20 horas.*	*Cada año se publica en línea por parte de la DGTIC*

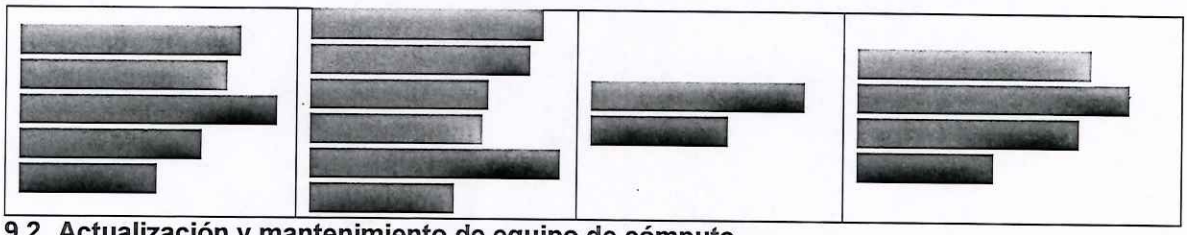
8.2. Programa de difusión de la protección a los datos personales

Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A1	REDPUMA		
Actividad	**Descripción**	**Duración**	**Cobertura**
Se envía por correo a los involucrados, la liga para inscripción al curso de protección de datos personales	*Videos tutoriales en la plataforma Moodle*	*Duración: 20 horas*	*Cada año se publica en línea por parte de la DGTIC*

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A1	**REDPUMA**		
Actividad	Descripción	**Duración**	**Cobertura**
[redacted]	[redacted]	[redacted]	[redacted]
Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A2	*SIEM*		
Actividad	**Descripción**	**Duración**	**Cobertura**



9.2. Actualización y mantenimiento de equipo de cómputo

Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A1	**REDPUMA**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Departamento de Tecnologías de la Información de la DGDU			
Identificador único	*REDP-01*		
Nombre del sistema A2	**SIEM**		
Actividad	**Descripción**	**Duración**	**Cobertura**

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

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	**REDPUMA**	
Proceso	**Descripción**	**Responsable**
Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	**SIEM**	
Proceso	**Descripción**	**Responsable**

[redacted]	[redacted]	[redacted] b)

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

Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A1	**REDPUMA**	
Proceso	**Descripción**	**Responsable**
[redacted]	[redacted]	[redacted] b)
Departamento de Tecnologías de la Información de la DGDU		
Identificador único	*REDP-01*	
Nombre del sistema A2	*SIEM*	
Proceso	**Descripción**	**Responsable**
[redacted]	[redacted]	[redacted]

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

En caso de una cancelación de un sistema de tratamiento de datos personales, se nos dará la instrucción por escrito y procedemos a eliminar del disco duro, así como respaldos que tuviéramos de las bases de datos. Usaremos herramientas de borrado con el software Acronis o en su momento con el más actual.

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

a) Denominación
b) Motivo de la cancelación

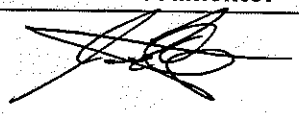
B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:
El periodo de bloque del tratamiento de datos personales se nos dará por escrito por parte de la Dirección General y su fecha y hora de restablecimiento en caso de ser necesario.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

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

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

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Luis Gabriel Jiménez Reyes Jefe de Tecnologías Teléfono: 5622 2222 ext 40086 Correo electrónico:gabel@unam.mx	
Revisó:	Luis Gabriel Jiménez Reyes Jefe de Tecnologías Teléfono: 5622 2222 ext 40086 Correo electrónico:gabel@unam.mx	
Autorizó:	Alejandro Fernández Varela Jiménez Director General del Deporte Universitario. Teléfono: 5622 2222 ext 20047 Correo electrónico: afvarela@unam.mx	
Fecha de aprobación:	10 agosto 2022	
Fecha de actualización:	10 agosto 2022	

REDPUMA			**REDP-01**	
Formato	**1**	**Verificación anual**	**Acción concluida**	(X)
Medida de seguridad técnica:	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.			
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.			
Mejores prácticas, referencias:	**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.			

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ **BRIAN BELMONTES BOTELLO**	02/01/2022
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**2**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**	30 de marzo 2022
Nombre y firma Administrador del sistema de información	**Fecha término** 31 de marzo 2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**3**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		
Ejecución			**Fecha inicio**	
BRIAN BELMONTES BOTELLO			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			20/01/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**		
Formato:	4	**Verificación anual**	**Acción concluida**	(X)	
Medidas de seguridad técnicas:	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**				
Aplicable en:	I. Bases de datos y sistemas de tratamiento.				
Tiempo estimado:	Dos días hábiles.				
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.				
Proceso recomendado:	**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.				
Mejores prácticas, referencias:	**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.				
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.				
Ejecución			**Fecha inicio**		
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**			01/01/2022		
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 15/12/2022		
Observaciones / anotaciones	[redacted]				

REDPUMA			**REDP-01**	
Formato:	**5**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.			
Proceso recomendado:	**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.			
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.			

Ejecución	**Fecha inicio**
GABINO ROCHA CORTES	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 12/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**6**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.			
Proceso recomendado:	**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.			
Conocimientos requeridos:	Administración de sistema operativo.			
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 15/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**7**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.			
Proceso recomendado:	**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENES REYES	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 15/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**8**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:		**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			15/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**9**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	16/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 19/03/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**10**	**Verificación anual**	**Acción concluida**	(X)
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:		**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	18/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 19/03/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**11**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:		**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			22/03/2021	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 23/03/2021	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**12**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.			
Proceso recomendado:	**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.			
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.			
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			22/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 22/03/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**13**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.			
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy)*. **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. **2.-** El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.			
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			18/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			22/03/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**14**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. **D)** En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **E)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			24/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 26/03/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**15**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.			
Proceso recomendado:	**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP*. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES			02/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 15/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**16**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:		**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**	02/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 15/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**17**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:		**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	05/04/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 08/04/2022
Observaciones / anotaciones	

REDPUMA			**REDP-01**	
Formato:	**18**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnica:		**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:		**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			05/04/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			14/04/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**19**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:		**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			05/04/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			30/04/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**20**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:		**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			27/04/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			30/04/2022	
Observaciones / anotaciones				

REDPUMA			**REDP-01**	
Formato:	**21**	**Verificación anual**	**Acción concluida**	(X)
Norma Complementaria Técnica		**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:		**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:		Administración de redes de datos.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	22/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 25/03/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**22**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:		**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			22/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	25/03/2022
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**23**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:		**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.		
Conocimientos requeridos:		Administración de sistema de información. Desarrollo de aplicaciones.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	02/02/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**24**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:		**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:		Administración de aplicaciones. Administración de sistema operativo.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ REYES	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 15/12/2022
Observaciones / anotaciones	[redacted]

	[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA			**REDP-01**	
Formato:	**25**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 15/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA			**REDP-01**	
Formato:	**26**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			15/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA			**REDP-01**	
Formato:	**27**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Seis días hábiles.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:		Administración de infraestructura.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	19/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 26/03/2022
Observaciones / anotaciones	[redacted]

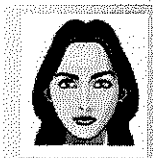
REDPUMA			**REDP-01**	
Formato:	**28**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**		
Aplicable en:		Servicios en la nube pública.		
Tiempo estimado:		Hito.		
Importancia de la acción:		No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:		**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:		**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:		Administración de respaldos. Administración de sistema operativo.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	24/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

REDPUMA-SIEM			**REDP-01**	
Formato	**1**	**Verificación anual**	**Acción concluida**	(X)
Medida de seguridad técnica:		**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de tablas.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ **BRIAN BELMONTES BOTELLO**	02/01/2022
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

[redacted]



[redacted]

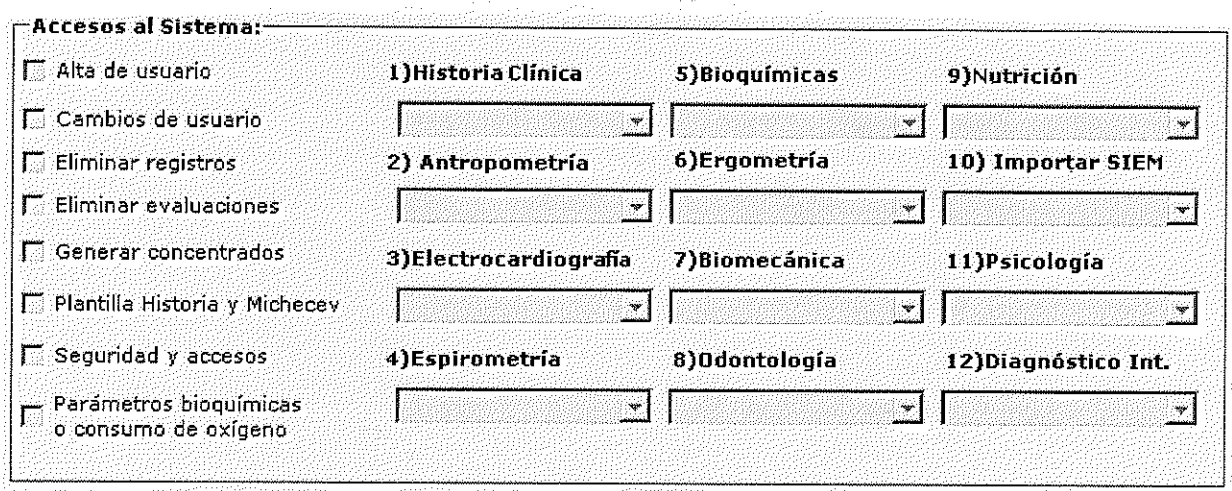
[redacted]

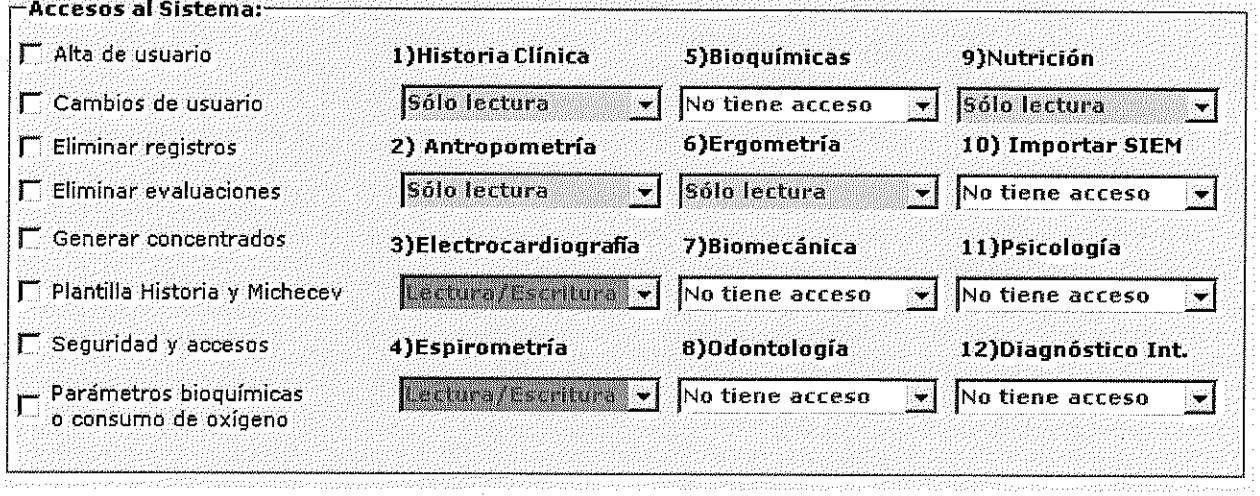
Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y desclasificación de la información, así como para la elaboración de versiones públicas. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/S25/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA -SIEM			**REDP-01**	
Formato:	**2**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**			30/03/2022	
Nombre y firma Administrador del sistema de información			**Fecha término**	
			31/03/2022	
Observaciones / anotaciones	[redacted]			

Se restringen los privilegios de cada usuario de acuerdo a su cargo, los permisos son:

- No tiene acceso(no puede visualizar la información dentro de esa sección)
- Solo lectura (el usuario solo tiene permiso de lectura en esa sección)
- Lectura y Escritura (el usuario puede revisar, modificar y/o eliminar datos dentro de la sección)

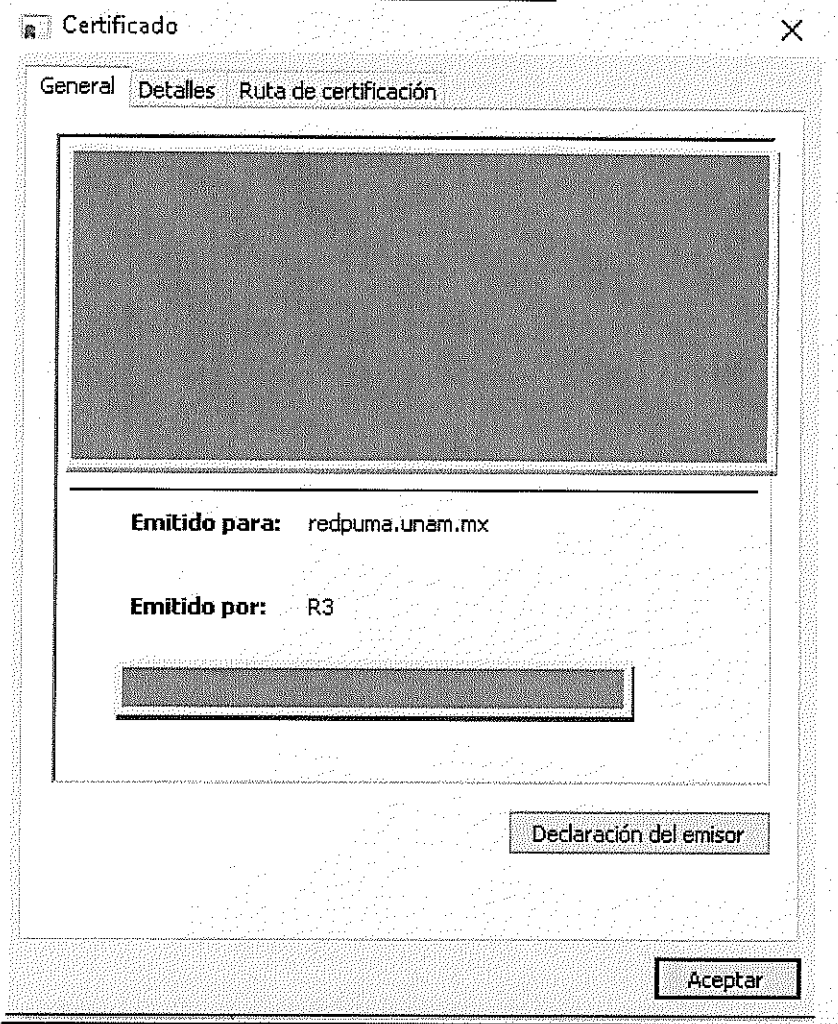




REDPUMA -SIEM			**REDP-01**	
Formato:	**3**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		

Ejecución	**Fecha inicio**
BRIAN BELMONTES BOTELLO	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

[redacted]



[redacted]

REDPUMA -SIEM			**REDP-01**	
Formato:	**4**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un periodo de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA -SIEM			**REDP-01**	
Formato:	5	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:		**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M.*		
Conocimientos requeridos:		Administración de sistema operativo. Comandos de borrado.		
Ejecución			**Fecha inicio**	
GABINO ROCHA CORTES			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			31/12/2022	
Observaciones / anotaciones	[redacted]			

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación**: Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación**: En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA -SIEM			**REDP-01**	
Formato:	**6**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:		**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			31/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA-SIEM			**REDP-01**	
Formato:	7	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.			
Proceso recomendado:	**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			

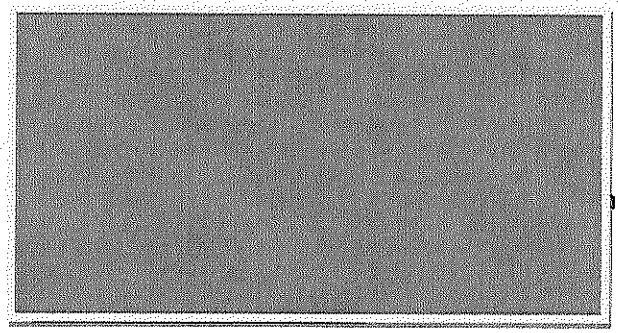
Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENES REYES	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación**: Con fundamento 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 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. Dicha información será reservada por un periodo de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación**: En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**8**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.			
Proceso recomendado:	**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMENEZ REYES	01/01/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]



[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**		
Formato:	**9**	**Verificación anual**	**Acción concluida**	(X)	
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**			
Aplicable en:		I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:		Cuatro días hábiles.			
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.			
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.			
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución			**Fecha inicio**		
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			16/03/2022		
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**		
			19/03/2022		
Observaciones / anotaciones	[redacted]				

[redacted]

Accesos al Sistema:

☑ Alta de usuario	**1)Historia Clínica**	**5)Bioquímicas**	**9)Nutrición**
☑ Cambios de usuario	Lectura/Escritura	Lectura/Escritura	Lectura/Escritura
☐ Eliminar registros	**2) Antropometría**	**6)Ergometría**	**10) Importar SIEM**
☐ Eliminar evaluaciones	Sólo lectura	Sólo lectura	Sólo lectura
☑ Generar concentrados	**3)Electrocardiografía**	**7)Biomecánica**	**11)Psicología**
☐ Plantilla Historia y Michecev	Sólo lectura	Sólo lectura	Sólo lectura
☑ Seguridad y accesos	**4)Espirometría**	**8)Odontología**	**12)Diagnóstico Int.**
☐ Parámetros bioquímicas o consumo de oxígeno	Sólo lectura	Sólo lectura	Lectura/Escritura

REDPUMA-SIEM			**REDP-01**	
Formato:	**10**	**Verificación anual**	**Acción concluida**	(X)
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:		**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	18/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 19/03/2022
Observaciones / anotaciones	[redacted]

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un periodo de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**11**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:		**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			22/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 23/03/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA-SIEM			**REDP-01**	
Formato:	**12**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:		**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.		
Conocimientos requeridos:		Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			22/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 22/03/2022	
Observaciones / anotaciones	[redacted]			

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**13**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.			
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy)*. **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-getinstallopenssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctlenablessh*. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. **2.-** El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.			

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	18/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 22/03/2022
Observaciones / anotaciones	[redacted]

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**14**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 20.Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. **D)** En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **E)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	24/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 26/03/2022
Observaciones / anotaciones	[redacted]

REDPUMA-SIEM			**REDP-01**	
Formato:	**15**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas		**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:		**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP*. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES			02/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	31/12/2022
Observaciones / anotaciones				

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación**: Con fundamento 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 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. Dicha información será reservada por un periodo de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación**: En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**16**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:		**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**			02/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			31/12/2022	
Observaciones / anotaciones	[redacted]			

[redacted]

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un periodo de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**17**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:		**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			05/04/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 08/04/2022	
Observaciones / anotaciones	[redacted]			

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación**: Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación**: En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**18**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnica:		**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:		**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			05/04/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			14/04/2022	
Observaciones / anotaciones	[redacted]			

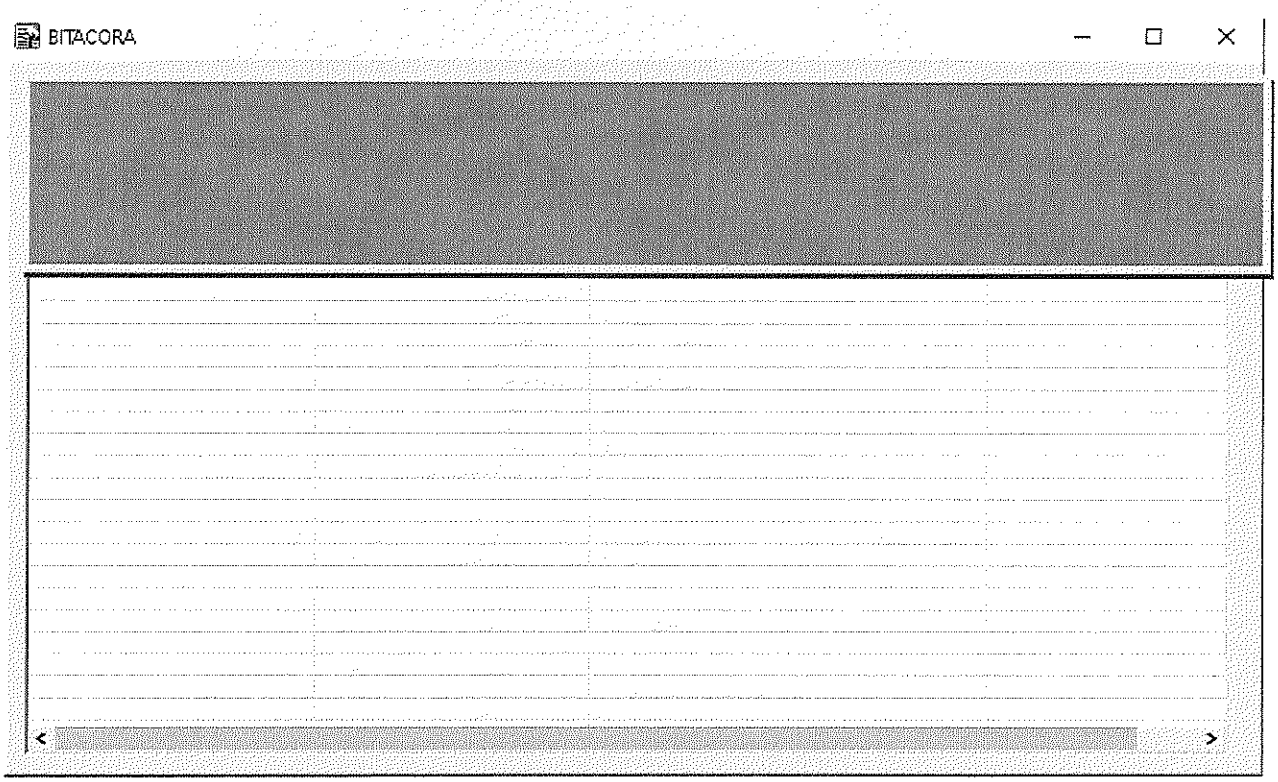
[redacted]

REDPUMA-SIEM			**REDP-01**	
Formato:	**19**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:		**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	05/04/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 30/04/2022
Observaciones / anotaciones	[redacted]

REDPUMA-SIEM			**REDP-01**	
Formato:	**20**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:		**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	27/04/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 30/04/2022
Observaciones / anotaciones	[redacted]



REDPUMA-SIEM			**REDP-01**	
Formato:	**21**	**Verificación anual**	**Acción concluida**	(X)
Norma Complementaria Técnica		**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:		**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:		Administración de redes de datos.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	22/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 25/03/2022
Observaciones / anotaciones	[redacted]

REDPUMA-SIEM			**REDP-01**	
Formato:	**22**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:		**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			22/03/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	25/03/2022
Observaciones / anotaciones	[redacted]			

[redacted]

Eliminado: Observaciones/anotaciones. **Fundamentación:** Con fundamento 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 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. Dicha información será reservada por un período de cinco años de conformidad con la Resolución CTUNAM/525/2022 de 19 de agosto de 2022. **Motivación:** En virtud de tratarse de información que pudiera revelar vulnerabilidades en la protección de los datos personales en poder de la Dirección General del Deporte Universitario, evitando o previniendo la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática.

REDPUMA-SIEM			**REDP-01**	
Formato:	**23**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**			02/02/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			31/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA-SIEM		**REDP-01**	
Formato:	**24**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:	**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:	**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.		
Ejecución		**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES		01/01/2022	
Nombre y firma Administrador del sistema de información o servidor		**Fecha término**	
		31/12/2022	
Observaciones / anotaciones	[redacted]		

REDPUMA-SIEM			**REDP-01**	
Formato:	**25**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.			
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES **BRIAN BELMONTES BOTELLO**			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 31/12/2022	
Observaciones / anotaciones	[redacted]			

REDPUMA-SIEM			**REDP-01**	
Formato:	**26**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
LUIS GABRIEL JIMENEZ REYES			01/01/2022	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			31/12/2022	
Observaciones / anotaciones		[redacted]		

REDPUMA-SIEM			**REDP-01**	
Formato:	**27**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Seis días hábiles.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:		Administración de infraestructura.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	19/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 26/03/2022
Observaciones / anotaciones	[redacted]

REDPUMA-SIEM			REDP-01	
Formato:	**28**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 21.Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**		
Aplicable en:		Servicios en la nube pública.		
Tiempo estimado:		Hito.		
Importancia de la acción:		No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:		**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:		**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:		Administración de respaldos. Administración de sistema operativo.		

Ejecución	**Fecha inicio**
LUIS GABRIEL JIMÉNEZ REYES **BRIAN BELMONTES BOTELLO**	24/03/2022
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** 31/12/2022
Observaciones / anotaciones	[redacted]