UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
ESCUELA NACIONAL PREPARATORIA
DIRECCIÓN GENERAL

Sistema de Gestión de Seguridad de Datos Personales

agosto de 2022

Responsable del desarrollo	Ing. Jesús Romero Martínez Coordinador General de Cómputo de la Escuela Nacional Preparatoria.
Revisó	Mtra. Araceli Pérez Hernández Coordinadora Jurídica de la Escuela Nacional Preparatoria.
Autorizó	Biol. María Dolores Valle Directora General de la Escuela Nacional Preparatoria.
Fecha de Aprobación 15/08/2022	

Presentación

La Escuela Nacional Preparatoria, desde su fundación, hace más de 150 años, ha sido una de las instituciones más importantes del bachillerato nacional, que ha marcado el rumbo de la educación en México. Tiene el reto educativo de ofrecer una educación integral de alto nivel, en la que prevalezcan los valores universitarios, éticos y cívicos: el respeto, la responsabilidad, la honestidad, la integridad académica, el compromiso, la solidaridad, la equidad de género, la disposición a la convivencia en un ambiente de tolerancia a diversas expresiones. Participa en la formación de jóvenes analíticos que logren transformar la información en conocimiento, que apliquen su pensamiento crítico para comprender los fenómenos de su entorno, que utilicen herramientas diversas para resolver problemas reales, que reflexionen para tomar decisiones. Que cuenten con herramientas para desenvolverse exitosamente en el ambiente académico, personal y ciudadano.

Una tarea importante de la UNAM y por consecuencia de la ENP es fomentar la transparencia y accesibilidad a la información, cuidando rigurosamente los datos personales de la comunidad preparatoriana.

El presente documento tiene como propósito mostrar las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales de la Dirección General de la Escuela Nacional Preparatoria, con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen. Medidas que se ven reflejadas en la metodología implementada en la DGENP para garantizar la seguridad de los datos (sensibles y no sensibles) de todas las personas que establecen alguna relación con la ENP y los datos propios de la institución.

La metodología se compone de:

- Identificar los activos y los recipientes de información como parte central, la información/datos es la parte más importante en las instituciones, por lo que se debe garantizar su seguridad.
- Posteriormente se identifica a los sistemas y procedimientos que manejan, almacenan, consultan y transforman a los datos. Una forma de tener acceso a la información de forma ilícita es a través de los medios y canales establecidos. Se identifican 2 medios, los sistemas y los procesos. Por lo que la metodología contempla identificar para cada grupo de datos el medio por el se tiene acceso, el área y/o personal responsable, encargados, usuarios que lo manejan y las medidas de seguridad implementadas para garantizar la integridad, confidencialidad y disponibilidad de los datos.
- Una vez identificados los activos, los procesos y sistemas y el área que los resguarda y administra, para cada forma (sistema o proceso) de manejar los datos se identifica el riesgo inherente por la forma en que se resguardan y manipulan los datos, así también se realiza un análisis, para saber qué hacer para mitigar o resolver los problemas de seguridad o riesgo identificados.

En la imagen 1 se observa:

- Los activos de la DGENP, que se encuentran resguardados en contenedores físicos y digitales.
- Los activos que son manejados/consultados por sistemas y procesos.
- Los sistemas y procesos son que son administrados por un área de la DGENP.
- Los puntos de vulnerabilidad, para que un agente malicioso pueda dañar, extraer, modificar a los activos.

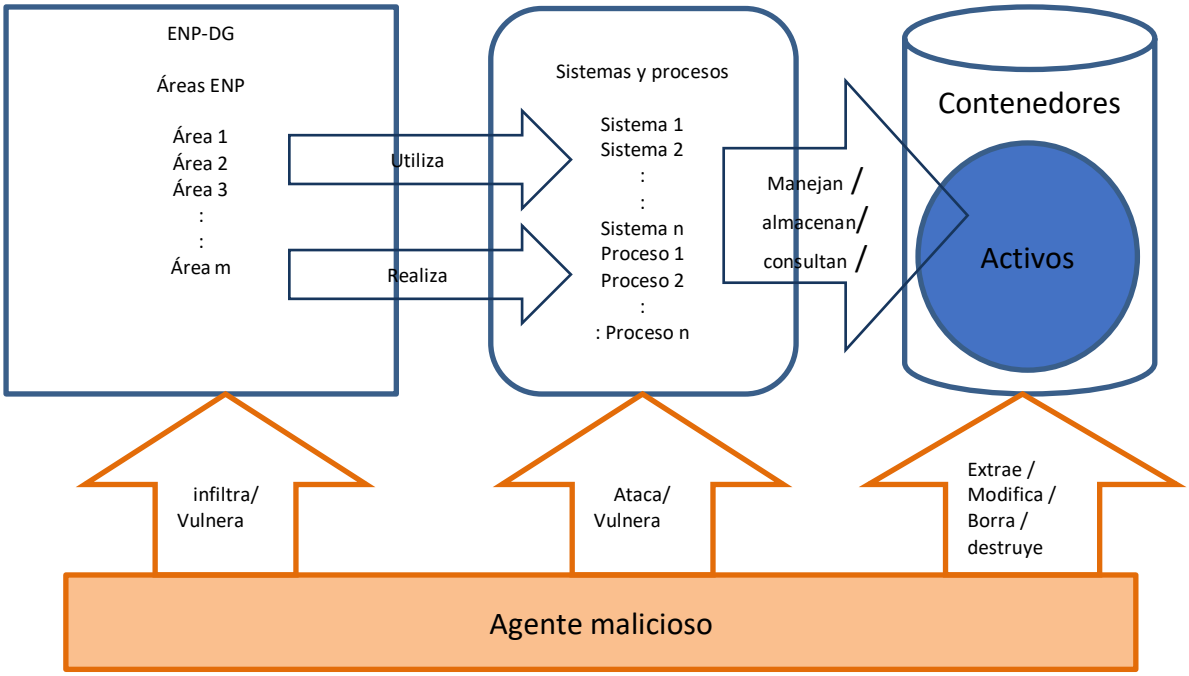

Figura 1. Manejo de la información y los puntos de vulnerabilidad.

La base del formato de 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, el formato considera el tamaño y estructura de esta área universitaria, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón a 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 20002:2013 “Tecnología de la información – Técnicas de seguridad – Código de práctica para los controles de seguridad de la información”.

Contenido

Introducción

A partir de la publicación del acuerdo a los lineamientos Generales de Protección de datos personales para el Sector Publico, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, y 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. Todas las dependencias de la UNAM se dieron a la tarea de implementar mecanismos, metodologías, nuevas formas de trabajo que nos permitiera recibir, almacenar, consultar y resguardar la información de la comunidad universitaria, así también la información de las personas que interactúan con la institución.

Por otra parte, el artículo 6, apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos, establece que toda la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
Por su parte, el artículo 16, párrafo segundo prevé que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación, cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
Bajo ese contexto, la Dirección General de la Escuela Nacional Preparatoria tiene bajo su resguardo diversa información de carácter de personal, tanto de alumnos, trabajadores, funcionarios, así como de persona externas al plantel, por lo que tiene la obligación de salvaguardar dicha información y protegerla en los términos de la normatividad aplicables vigente en la materia.
Por lo anterior, a fin de que La Dirección General de la Escuela Nacional Preparatoria dé cumplimiento a la obligación estipulada en el artículo 35 de la Ley General de Protección de Datos Personales, se crea el presente documento de seguridad, mismo que contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del mencionado, con la finalidad de asegurar la integridad, confidencialidad y disponibilidad personal en estos contenidos.

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.

En la Dirección general de la Escuela Nacional preparatoria, como muchas otras instituciones, se desarrolló una metodología para analizar y proponer los mecanismos de resguardo de los datos de los miembros de la comunidad.

La metodología se compone de varias fases, en cada una de ellas se tiene un objetivo.

La primera fase consiste en considerar a los activos como la parte central, debido a que es lo que queremos proteger, en la DGENP podemos decir que todas las áreas manejan activos, pero en muchos casos son los

mismos. Así que desde un punto de vista macro, se identifican a los activos más importantes, sin definir en qué áreas se manejan, ni la forma de manejarlos. De esta forma se obtiene el catálogo de activos.

La segunda fase consiste en identificar a todas las áreas de la DGENP que manejan a la información, de igual manera de forma general, no se describe la forma en que la manejan, sólo se enuncia las áreas, los roles, se describe la relación entre las áreas por medio la rendición de cuenta y su participación en el SGPDP.

La tercera fase consiste en identificar las áreas de impacto en general, clasificándolas de menor a mayor impacto.

La cuarta fase consistió en definir la forma para realizar el análisis de riesgo, el análisis de brecha y el plan de trabajo.

Una vez definida la metodología, conociendo la lista de activos y áreas que manejan a los activos, se procedió a identificar a los sistemas y procesos que manejan, transforman y resguardan a los activos. Para cada sistema o proceso se documentó:

- El activo que maneja, el perfil del activo
- Las personas que la manejan, y el rol que juegan (encargado, usuario, responsable)
- La lista de procesos de la información, en mayor detalle, el área o subárea que lo realiza
- Los requerimientos de seguridad
- Análisis de riesgo
    - El entorno de riesgo del activo
    - El riesgo del activo
    - El impacto en cada una de las áreas de impacto
- Plan de trabajo

Inventario de activos

La Escuela Nacional Preparatoria tiene la tarea y responsabilidad de formar alumnos de bachillerato para que puedan continuar con una educación profesional de manera exitosa. De la tarea encomendada a la ENP, se desprenden los participantes de la institución:

- La comunidad
    - Alumnos
    - Profesores
    - Trabajadores
- Personal externo que tiene relación con la institución
    - Proveedores
    - Prestadores de servicios
- Activos físicos de infraestructura
    - Equipo de cómputo
    - Servidores
    - Infraestructura de red

En general para las personas que forman a la comunidad se manejan los datos:

- Nombre
- Domicilio
- Número telefónico

- Datos de familiares
- Teléfonos de familiares
- Padecimientos
- Género
- Sexo
- Fecha de nacimiento
- Etc.

Los participantes son vistos como activos en forma que residen en bases de datos, y son manipulados durante los procesos.

Activo	Descripción
Bases de datos	En general todos los sistemas que almacenan información hacer uso de un SMBD que permite guardar, consultar, borrar, actualizar y proteger los datos almacenados en una base de datos
procesos	Todos los datos se manipulan, consultan, transforman y almacenan de acuerdo con los procesos definidos en los manuales de procedimientos
Personal	Personal con amplia experiencia en el manejo y tratamiento de la información.
Hardware	La infraestructura que soporta las comunicaciones, medios de almacenamiento y procesos digitales. Tales como: red estructurada, servidores, computadoras personales
Software	La parte intangible de los sistemas que en combinación con el hardware da origen a los sistemas de información digitales.
Archivos	Se refiere a documentos digitales que contienen información.
Documentos	Se refiere a documentos físicos que contienen información.

Tabla 1. Lista de grupos de activos.

En general los activos se manejan en varios lugares, como activos compartidos o como copia de los activos. Por ejemplo, el activo alumno, se maneja en Servicios Escolares, y si el alumno se encuentra inscrito en los estudios técnicos especializados también se maneja en la Coordinación de Estudios Técnicos Especializados. Lo mismo sucede con los profesores y trabajadores, es un solo activo que se maneja/ manipula/almacena en varios lugares.

Catálogo de áreas y roles

La dirección General de la ENP cuenta con diversas áreas, la mayoría de ellas manejan a los activos, las áreas que manejan información sensible de los activos se listan a continuación.

Área	Siglas	Rol
Dirección General	DG	Director(a) General
Secretaria General	SG	Secretario(a) General
Secretaría Académica	SA	Secretario(a) Académico(a)
Secretaría Administrativa	SADMIN	Secretario(a) Administrativo(a)
Secretaría de Planeación	SP	Secretario(a) Planeación
Secretaria de Asuntos Estudiantiles	SAE	Secretario(a) de Asuntos Estudiantiles
Secretaría de Difusión Cultural	SDC	Secretario(a) de Difusión Cultural
Coordinación Jurídica	CJ	Coordinador(a) de la oficina Jurídica

Área	Siglas	Rol
Coordinación de Gestión	CG	Coordinador(a) de Gestión
Coordinación General de Cómputo	CGC	Coordinador(a) General de Cómputo
Coordinación General de Bibliotecas	CGB	Coordinador(a) de Bibliotecas
Coordinación General de Estudios Técnicos Especializados	ETE	Coordinador(a) General de Estudios Técnicos Especializados
Coordinación de Evaluación Educativa	CEE	Coordinador(a) de Evaluación Educativa
Jefatura de la Unidad de Investigación y Apoyo Pedagógico	UIAP	Jefe(a) de la Unidad de investigación y apoyo Pedagógico
Jefatura de la Unidad Administrativa	JUA	Jefe(a) de la Unidad Administrativa
Jefatura de Presupuesto	JPR	Jefe(a) del departamento de presupuesto
Jefatura de Bienes y Suministros	JBS	Jefe(a) del departamento de Bienes y Suministros
Jefatura de Personal	JPE	Jefe(a) del Personal
Jefatura de Servicios Generales	JSG	Jefe(a) del departamento de Servicios Generales
Jefatura de Desarrollo de Sistemas y Telecomunicaciones	JDSyT	Jefe(a) del departamento de Desarrollo de Sistemas y Telecomunicaciones
Jefatura de Evaluación y Control	JEyC	Jefe(a) del Departamento de Evaluación y Control

Tabla 2. Lista de áreas que manejan a los activos.

Algunas áreas además de manejar los datos personales tienen una función en el SGPDP, dichas áreas se listan a continuación.

Fase del SGPDP	Áreas de la DGENP					
	DG	SG	CGC	CJ	JEyC	JDyT
Definición de los objetivos	X	X	X	X		
Funciones y obligaciones	X	X				
Inventario de Datos Personales.		X	X	X	X	X
Análisis de Riesgo de los Datos Personales			X		X	X
Análisis de Brecha de las Medidas de Seguridad			X		X	X
Implementación de las Medidas de Seguridad			X		X	X
Capacitación			X		X	X
Creación de Políticas			X		X	X
Revisiones		X				

Tabla 3. Lista de áreas que participan en el SGPDP.

A su vez las áreas tienen una relación en función de la rendición de cuentas, dicha relación se muestra en la siguiente tabla.

Área en la DGENP	Área a la que rinde cuentas					
	DG	SG	CGC	CJ	JEyC	JDSyT
Dirección General						

Secretaria General	X					
Coordinación Jurídica	X	X				
Coordinación General de Cómputo	X	X				
Jefatura de Evaluación y Control			X			
Jefatura de Desarrollo de Sistemas y Telecomunicaciones			X			

Tabla 4. Relación de rendición de cuentas entre áreas.

A partir de procesos en que se da tratamiento a los datos, en cada uno de los sistemas se presenta un concentrado de estos procesos y el área que realiza dicho tratamiento.

Metodología

Para cada sistema de tratamiento de la información se realizó lo siguiente.

Identificación de Activos

En este apartado se describe particularmente cada activo o parte del activo que se maneja, se relaciona con las personas o figuras administrativas que tiene acceso a ellos, definiendo las funciones y obligaciones para con los activos.

Identificación de los procesos que dan tratamiento a los activos

Para cada uno de los activos identificados se listan los datos personales que se manejan y se enuncia el tratamiento de datos, así como el área que lo realiza.

Análisis de riesgo en el tratamiento de datos personales

El análisis se basa en identificar las áreas de mayor impacto, áreas de preocupación para la DG-ENP, a continuación, se listan las áreas de impacto y se asocian a un nivel de prioridad.

Área de impacto	Prioridad	Prioridad DGENP
Pérdida de confianza en el área universitaria y en la opinión pública (reputación)	9	9
Incumplimiento de obligaciones legales	8	8
Orden público	7	7
Persecución de delito	6	6
Interrupción del servicio	5	4
Amonestación pública y medidas de apremio (en multas) del INAI (art. 153 LGPDPPSO) / Sanciones (art. 163 LGPDPPSO) y procesos legales (1915 Código Civil Federal) (Multas / penas legales)	4	3

Área de impacto	Prioridad	Prioridad DGENP
Financiera	3	1
Productividad	2	5
Seguridad	1	2

Tabla 5. Áreas de impacto con prioridad de menor a mayor.

A continuación, se define un valor cuantitativo a los valores cualitativos de la probabilidad de impacto.

Medida	Puntaje
Alto	3
medio	2
Bajo	1

Tabla 6. Criterios cualitativos para evaluar el efecto del riesgo

Para cada área de impacto y criterio cualitativo se definen las características que definen a la combinación.

Criterio de medición de riesgo			
Área de impacto	**Bajo**	**Medio**	**Alto**
Pérdida de confianza en el área universitaria y en la opinión publica (reputación)	La información relacionada con un incidente de seguridad de datos personales sólo se conoce al interior de la DGENP	La información relacionada con un incidente de seguridad de datos personales es de conocimiento de la Universidad	La información relacionada con un incidente de seguridad de datos personales es conocida públicamente a través de medios de comunicación masivos y existe procedimiento de verificación por Violación o Incumplimiento a la LGPDPPSO ante el INAI.
Productividad	Se pierden de 1 a 50 registros o archivos electrónicos y físicos.	Se pierden de 50 a 250 registros o archivos electrónicos y físicos.	Se pierden más de 250 registros o archivos electrónicos y físicos.
Interrupción del servicio	Interrupción del servicio menor a 3 horas o el servicio se encuentra con un funcionamiento intermitente durante 24 horas.	Interrupción del servicio de 4 horas a 24 horas.	Interrupción del servicio mayor a 24 horas.
Orden público	La Entidad o dependencia se encuentra en paro de actividades o huelga durante 1 día.	La entidad o dependencia se encuentra en paro de actividades o huelga entre 2 o 4 días.	La entidad o dependencia se encuentra en paro de actividades o huelga por más de 5 días.
Financiera	Un incidente de seguridad de datos personales afecta a uno de los componentes de un servidor de la Unidad de Transparencia. Costo < 20,000	Un incidente de seguridad de datos personales que provoca pérdida de equipo por robo o inutilización completa del equipo. Costo >= 20,000 y < 80,000	Un incidente de seguridad de datos personales provoca pérdida equipo o extorsión por robo de información de bases de datos. Costo > 80,000
Seguridad	La seguridad del personal de la DGENP se ve cuestionada.	La seguridad del personal de la DGENP se ve afectada.	La seguridad del personal de la DGENP se ve violada.
Amonestación pública y medidas de apremio (en multas) del INAI (art. 153 LGPDPPSO) / Sanciones (art. 163 LGPDPPSO) y procesos legales (1915 Código Civil Federal) (Multas / penas legales)	Hay exposición de datos personales al interior de la Universidad, pero el área es proactiva y colabora con el INAI a fin de detener o reparar el daño.	Exposición de datos personales que provoca una multa de 150 a 1500 UMAS.	Exposición de datos personales son de tipo sensible o bien se expone información de un número considerable de titulares, reiteración en la exposición de datos personales. Se promueve en contra de la universidad una demanda por vía civil, laboral o una denuncia penal.

Criterio de medición de riesgo			
Área de impacto	**Bajo**	**Medio**	**Alto**
Incumplimiento de obligaciones legales	Se incumple una obligación en distintas materias legales o se cumple de forma mínima en un determinado lapso.	Incumplimiento de 1 a 3 obligaciones en distintas materias legales.	Incumplimiento de 4 o más obligaciones en distintas materias legales.
Persecución de delito	Existe impedimento o dificultad de la investigación de un delito (cadena de custodia).	Existe impedimento o dificultad de la investigación de un delito grave; o existe facilidad para la comisión de un delito.	Existe impedimento o dificultad de la investigación de 2 delitos graves; y 1 delito no grave. Existe facilidad para la comisión de 2 delitos.

Tabla 6. Criterios de medición de riesgo.

Puntaje máximo para la Valoración de riesgos

A partir de las áreas de impacto, la prioridad de cada área y considerando la máxima probabilidad, se calcula el puntaje máximo para la valoración de riesgo.

Área de impacto	Prioridad	Probabilidad	Puntaje
Pérdida de confianza en el área universitaria y en la opinión pública (reputación)	9	Alta (3)	27
Incumplimiento de obligaciones legales	8	Alta (3)	24
Orden público	7	Alta (3)	21
Persecución de delito	6	Alta (3)	18
Interrupción del servicio	5	Alta (3)	15
Amonestación pública y medidas de apremio (en multas) del INAI (art. 153 LGPDPPSO) / Sanciones (art. 163 LGPDPPSO) y procesos legales (1915 Código Civil Federal) (Multas / penas legales)	4	Alta (3)	12
Financiera	3	Alta(3)	9
Productividad	2	Alta(3)	6
Seguridad	1	Alta(3)	3
	Total (máximo)		153

Tabla 7. Áreas de impacto con puntaje máximo de riesgo.

En el caso de los sistemas, para cada uno de ellos se aplica el mismo método para calcular el riesgo del activo de información.

Análisis de Brecha

Una vez identificados los procesos necesarios en cada sistema que da tratamiento a los datos personales, se realiza el análisis de brecha.
Identificando la celda de la matriz de riesgos relativa cae el valor particular de sistema, activo, análisis de impacto.

Matriz de riesgo relativo			
Probabilidad	Puntuación de riesgo		
	135 a 90	89 a 44	0 a 42
Alta	Grupo 1	Grupo 2	Grupo 2
Media	Grupo 2	Grupo 2	Grupo 3
Baja	Grupo 3	Grupo 3	Grupo 4

Tabla 8. Matriz de riesgo relativo por grupo.

Grupo	Enfoque de mitigación
Grupo 1	Mitigar / transferir
Grupo 2	Mitigar/aplazar/Transferir
Grupo 3	Aplazar/Aceptar
Grupo 4	Aceptar

Tabla 9. Enfoque de mitigación por grupo.

En el ejercicio se decide no utilizar el enfoque de transferir, por lo que tenemos la matriz de riesgo relativo a utilizar

Matriz de riesgo relativo			
Probabilidad	Puntuación de riesgo		
	135 a 90	89 a 44	0 a 42
Alta	Mitigar	Mitigar o aplazar	Mitigar o aplazar
Media	Mitigar o aplazar	Mitigar o aplazar	Aplazar o Aceptar
Baja	Aplazar o Aceptar	Aplazar o Aceptar	Aceptar

Tabla 10. Enfoque de mitigación por grupo, a utilizar.

Mitigación y plan de trabajo

Una vez identificado el riesgo por sistema y activo, de acuerdo con la matriz de riesgo relativo se define que acción realizar (Mitigar, aplazar, aceptar).
Además, se definen las acciones inmediatas conforme al riesgo y un plan de trabajo para erradicar las vulnerabilidades que exponen al activo.

Formatos para cumplimiento de las MST

Para el caso particular de los Sistemas de Información, de acuerdo con el plan de trabajo se revisan los formatos para el cumplimiento de las MST, definidos por la DGTIC. En cada sistema se incorporan únicamente los formatos que aplican debido al plan de trabajo y forma de mitigar el riesgo.

Inventario de Sistemas de Tratamiento de la Información

SIEEL: Sistema de Inscripción a Exámenes Extraordinarios

DGENP/SAE/SIEEL - formato 1

Identificador único	DGENP/SAE/SIEEL
Nombre del sistema	Sistema de Inscripción de Exámenes Extraordinarios en Línea
Datos personales (sensibles o no) contenidos en el sistema	1) Datos personales en general: Información solicitada para realizar el proceso de registro del alumno: - Número de cuenta - Fecha de nacimiento - Correo electrónico personal Información que muestra el sistema: - Nombre completo del alumno - Plantel - Plan de estudios - Historial académico Información solicitada para registrar un usuario del sistema con perfil de Secretaria de Ventanilla: - Nombre completo - Número de trabajador - RFC con homoclave - Plantel 2) Datos laborales: Número de trabajador, plantel 3) Datos escolares o académicos: historial académico, plan de estudio, número de cuenta 4) Datos personales sensibles: Correo electrónico personal, fecha de nacimiento, RFC con homoclave
Responsables	
Nombre	Jefe de Desarrollo de Sistemas y Telecomunicaciones
Cargo	JDSyT (Jefatura de Desarrollo de Sistemas y Telecomunicaciones)
Funciones	Proporcionar los calendarios de inscripción y aplicación de exámenes extraordinarios al administrador del sistema (TAS) DGENP/SAE/SIEEL.

	Solicitar los Directorios e historias académicas de los alumnos del ciclo escolar correspondiente, a la Unidad de Registro Escolar para la ENP (URE).
Obligaciones	Verificar que los encargados cumplan con la protección de datos personales de acuerdo con las políticas de transferencia y recepción de archivos establecidas por la Coordinación. Garantizar la protección de los servidores de respaldo de la información generada por el sistema DGENP/SAE/SIEEL. Mantener actualizado el servidor donde se aloja el sistema DGENP/SAE/SIEEL.
Encargados	
Nombre del encargado 1	Jefe de la Unidad de Registro Escolar en la ENP
Cargo	URE (Unidad de Registro Escolar)
Funciones	- Solicitar los Directorios e historias académicas de los alumnos del ciclo escolar correspondiente, a la Dirección General de Administración Escolar (DGAE). - Proporcionar los Directorios e historias académicas de los alumnos del ciclo escolar correspondiente al Jefe del Departamento de Sistemas de la Coordinación de Cómputo de la DGENP. - Enviar a la DGAE los archivos de inscripción a exámenes extraordinarios.
Obligaciones	- Proteger los datos personales de los alumnos. - No modificar la información de datos personales contenidos en los archivos de inscripción de los alumnos. - No difundir la información de datos personales contenidos en los archivos de inscripción de los alumnos. - Mantener la información de datos personales en la Unidad del servidor privado configurado para ese propósito. - Utilizar únicamente el protocolo de seguridad definido para el envío y recepción de los datos personales contenidos en los archivos de inscripción de los alumnos.
Nombre del encargado 2	Técnico Académico Auxiliar
Cargo	TAS (Técnico Administrador del Sistema)
Funciones	- Cargar los calendarios de inscripción y aplicación de exámenes extraordinarios en el DGENP/SAE/SIEEL - Descargar los archivos de inscripción y entregarlos a la Unidad de Registro Escolar (URE).
Obligaciones	- Proteger los datos personales de los alumnos. - No modificar la información de datos personales contenidos en los archivos de inscripción de los alumnos. - No difundir la información de datos personales contenidos en los archivos de inscripción de los alumnos. - Mantener la información de datos personales en la Unidad del servidor privado configurado para ese propósito y en el servidor del sistema DGENP/SAE/SIEEL. - Utilizar únicamente el protocolo de seguridad definido para el envío y recepción de los datos personales contenidos en los archivos de inscripción de los alumnos.

	- Generar los respaldos de la información contenida en el sistema y almacenarlos en la unidad de Respaldos de la Coordinación de Cómputo.
Usuarios	
Nombre del usuario 1	Técnico Académico Auxiliar
Cargo	Administrador
Funciones	- Configurar fechas de registro de exámenes extraordinarios. - Configurar calendario de aplicación de exámenes extraordinarios. - Configurar horarios de acceso al sistema DGENP/SAE/SIEEL. - Descargar los archivos de inscripción correspondientes al periodo activo.
Obligaciones	- Proteger los datos personales de los alumnos. - No modificar la información de datos personales contenidos en los archivos de inscripción de los alumnos. - No difundir la información de datos personales contenidos en los archivos de inscripción de los alumnos. - Generar los respaldos de la información contenida en el sistema.
Nombre del usuario 2	Secretario Escolar de Plantel
Cargo	SAE (Secretaría de Asuntos Estudiantiles)
Funciones	- Consultar Situación Académica del alumno - Realizar cambios de plan de estudios cuando lo amerite la situación académica del alumno. - Consultar inscripciones. - Registrar al alumno las asignaturas solicitadas en el periodo activo. - Imprimir comprobantes de inscripción. - Registrar alumnos bajo planes no vigentes (Plan 1964) - Dar de alta usuarios con el rol de secretaria de ventanilla.
Obligaciones	- Proteger los datos personales de los alumnos. - No modificar la información de datos personales de los alumnos. - No difundir la información de datos personales contenidos en los archivos de inscripción de los alumnos. - Proteger los datos personales de los trabajadores responsables del registro en ventanillas. - No difundir información de los trabajadores responsables del registro en ventanillas.
Nombre del usuario 3	Secretaria/o Oficinista
Cargo	OSE (Oficinista de Servicios Escolares)
Funciones	- Consultar inscripciones - Imprimir comprobantes de inscripción - Registrar al alumno las asignaturas solicitadas en el periodo activo.

SIEEL

Obligaciones	- Proteger los datos personales de los alumnos. - No difundir la información de datos personales contenidos en los archivos de inscripción de los alumnos.	
Nombre del usuario 4		
Cargo	ALU (Alumno)	
Funciones	- Consultar inscripción - Registrar las asignaturas que así considere en el periodo activo. - Imprimir comprobante de inscripción.	
Obligaciones	- Realizar su inscripción de manera personal, a través del personal de ventanilla o el Secretario Escolar de su plantel. - No proporcionar su información personal a otro compañero para que realice su inscripción. - Verificar que su información sea correcta al realizar su inscripción.	
Estructura		
Tipo de soporte	Electrónico	
Descripción	Base de datos, archivos de registro, directorio de alumnos e historiales académicos.	
Características del lugar donde se resguardan los soportes	- Servidor virtual contenido en un servidor rack dentro el Cuarto de Servidores de la Coordinación de Cómputo de la DGENP. Cuenta con aire acondicionado, luz artificial, aislado de humedad y cableado de red estructurado. - Acceso restringido a la Coordinación de cómputo. - Acceso restringido al Cuarto de Servidores de la DGENP.	
Análisis de Riesgo		
Riesgo	Impacto	Mitigación
[redacted]		
Análisis de brecha		
Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación

SIEEL

[redacted]

Plan de trabajo			
Actividad	Descripción	duración	Cobertura

[redacted]

DGENP/SAE/SIEEL - formato 2

De acuerdo con el catalogo de áreas y roles llenar las funciones asociadas al sistema, enunciar el procedimiento, párrafo corto.

Tratamiento de datos personales	**Área (siglas)**
Solicitar Directorios de alumnos activos e Historias Académicas a la DGAE.	URE
Depositar Directorios de alumnos e Historias Académicas en la Unidad del Servidor Privado	URE
Cargar los datos del directorio de alumnos e historias académicas a la base de datos del SIEEL	JDSyT
Consultar situación académica de alumnos y realizar cambios de plan de estudios.	SAE
Registrar exámenes extraordinarios.	SAE, OSE, ALU
Consultar e imprimir comprobantes de alumnos inscritos a los exámenes extraordinarios.	SAE, OSE, ALU
Descargar la lista de alumnos inscritos a los exámenes extraordinarios	TAS
Depositar la lista de alumnos inscritos a exámenes extraordinarios en la Unidad del Servidor Privado	TAS
Entregar la lista de alumnos inscritos a exámenes extraordinarios a la DGAE.	URE

DGENP/SAE/SIEEL - formato 3

Activos asociados al sistema

Perfil de activo de información		
Activo de información critico	Motivo de la selección	Descripción
Base de datos del SIEEL	En esta base de datos se almacena información sobre la situación académica del alumno y la información solicitada para inscribir al alumno a los exámenes extraordinarios. Esta información contiene datos personales.	La base de datos contiene información requerida para realizar el proceso de inscripción de exámenes extraordinarios de los alumnos. Derivado de este proceso se concentran los siguientes datos: • Nombre completo del alumno • Plan de estudios • Historial Académico • Correo electrónico • Inscripción de exámenes

SIEEL

		• RFC de los directores de plantel.
Propietario(s)		
Requerimientos de seguridad		
Confidencialidad	Solo el siguiente personal autorizado puede consultar el activo	Sólo los secretarios escolares y oficinistas de servicios escolares encargados del registro de exámenes extraordinarios deberán acceder a la base de datos.
Integridad	Solo el siguiente personal autorizado puede modificar el activo	Sólo los Secretarios Escolares encargado de realizar cambios de plan de estudios podrá modificar la Situación Académica de los alumnos.
Disponibilidad	El activo debe estar disponible para el personal	Solo el personal encargado de la inscripción de exámenes extraordinarios deberá acceder al sistema para consultar y modificar la base de datos, en las fechas señaladas por el calendario oficial de la ENP de exámenes extraordinarios.
	Los horarios en que debe estar disponible la información	La base de datos del SIEEL deberá estar disponible en el horario de inscripción de exámenes extraordinarios definido en el sistema, durante las fechas señaladas en el Calendario Oficial de la ENP de exámenes extraordinarios.
Otros	La carga de información necesaria para la inscripción de exámenes la deberá realizar sólo el personal autorizado.	El activo debe contar con los directorios e historias académicas de los alumnos para realizar el proceso de inscripción. Sólo el responsable de la carga, Técnico Administrador de esta información podrá acceder a la base de datos en fechas previas al calendario de exámenes extraordinarios, para realizar la carga.
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo		
Confidencialidad **Sí**	Integridad **Sí**	Disponibilidad **Sí** / Otros No
Entorno del riesgo del activo de la información (contenedor)		

SIEEL

Tipo de contenedor	Interno	
Categoría	Descripción	Propietario(s)
Técnico	Aplicativo web Base de datos del SIEEL	• CGC • JDSyT
Física	Servidor rack de la Coordinación de Cómputo de la DGENP Unidad del Servidor Privado	• CGC • JDSyT
Administrativo		
Entorno del riesgo del activo de la información (contenedor)		
Tipo de contenedor	Externo	
Categoría	Descripción	Propietario(s)
Técnico	No aplica	No aplica
Físico	No aplica	No aplica
Administrativo	No aplica	No aplica
Riesgo del Activo de información		
Área de preocupación	[redacted]	
Actor		
Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?		
Motivo		
Resultados	( ) Relevancia	( ) Destrucción

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad q que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

SIEEL

¿Qué efecto tendría la vulneración del activo de información?	(X) Modificación	( ) Interrupción	
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	[redacted]		
Probabilidad	(X) baja	( ) Media	( ) Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	Valor	Puntaje
Se revelan datos de personales de los proveedores y estos ya no querrán darse de alta ante la Universidad	[redacted]		
Puede existir denuncia por parte de los proveedores para resarcir el daño causado por la revelación de los datos personales			

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

SIEEL

	[redacted]		
Puntaje del valor relativo			47
Mitigación del riesgo Acción a tomar para mitigar el riesgo			
( ) aceptar	**( ) aplazar**	**(X) Mitigar**	**( ) Transferir**
Indicar las mediadas a realizar conforme al riesgo			
JDSyT	[redacted]		
SAE, OSE			

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Plan de trabajo

Control	Actividad a realizar	Duración	Prioridad	Áreas responsables
[redacted]				

Plataforma Contacto-ENP

DGENP/CGC/ContactoENP - formato 1

Identificador único	DGENP/CGC/ContactoENP
Nombre del sistema	ContactoENP
Datos personales (sensibles o no) contenidos en el sistema	1) Datos personales en general: a) Datos de identificación: número de trabajador, RFC, CURP, número de cuenta, nombre, fecha de nacimiento b) Datos laborales: lugar de trabajo d) Datos académicos: correo electrónico institucional, grado de estudios 2) Datos personales sensibles: género
Responsables	
Nombre	Coordinación General de Cómputo de la ENP
Cargo	Coordinador General de Cómputo
Funciones	- Designar al personal responsable para la manipulación de la información
Obligaciones	- Salvaguardar los datos personales que se reciben en la plataforma. - No difundir la información de datos personales a personas no autorizadas.
Encargados	
Nombre del encargado 1	Departamento de Sistemas y Telecomunicaciones
Cargo	Jefe de Sistemas y Telecomunicaciones
Funciones	- Realizar las actividades de administración y mantenimiento de la B.D. - Realizar las actividades de administración y mantenimiento del servidor de aplicaciones.
Obligaciones	- Proteger el entorno donde viven los datos personales de accesos no autorizados. - No modificar la información de datos personales almacenada en los servidores. - No difundir la información de datos personales contenidos en los servidores.
Nombre del encargado 2	Desarrollador del sistema
Cargo	Técnico(a) Académico(a)
Funciones	- Agregar y administrar la información de datos personales - Respaldar y actualizar la información de datos personales
Obligaciones	- Prevenir el acceso de usuarios a módulos o funcionalidades no autorizadas. - Prevenir el daño a los datos personales. - No modificar sin la autorización del responsable, la información de datos personales. - No difundir la información de datos personales.
Usuarios	
Nombre del usuario 1	Soporte técnico de plantel
Cargo	Secretario(a) Académico(a) de Plantel
Funciones	- Consulta y seguimiento de las búsquedas de profesores(as) realizadas por las y los alumnos
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Nombre del usuario 2	Soporte técnico DG
Cargo	Técnico(a) Académico(a)
Funciones	- Consulta y seguimiento de los tickets generados por las y los profesores
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Nombre del usuario 3	Profesores(as)
Cargo	Académico(a)
Funciones	- Envío de mensajes a sus alumnos(as) - Generación y consulta de tickets - Visualización de listados y evaluaciones de las y los alumnos de sus grupos - Carga de evaluaciones
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Nombre del usuario 4	Alumnos(as)
Cargo	No aplica

Plataforma de contacto-ENP

Funciones	- Consulta de mensajes enviados por las y los profesores - Generación y consulta de búsqueda de profesores(as) - Consulta de evaluaciones - Registro a eventos académicos
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Estructura	
Tipo de soporte	Electrónico
Descripción	Base de datos
Características del lugar donde se resguardan los soportes	Servidor de bases de datos

Análisis de Riesgo		
Riesgo	Impacto	Mitigación
[redacted]		

Análisis de brecha		
Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación
[redacted]		

Plan de trabajo			
Actividad	Descripción	duración	Cobertura
[redacted]			

Plataforma de contacto-ENP

DGENP/CGC/ContactoENP - formato 2

De acuerdo con el catalogo de áreas y roles llenar las funciones asociadas al sistema, enunciar el procedimiento, párrafo corto.

Tratamiento de datos personales	Área (siglas)
Designar al personal responsable de la manipulación de los datos personales.	CGC
Realizar las actividades de administración y mantenimiento de la B.D.	JDSyT
Realizar las actividades de administración y mantenimiento del servidor de aplicaciones.	JDSyT
Agregar y administrar la información de datos personales.	JDSyT
Respaldar y actualizar la información de datos personales.	JDSyT
Dar seguimiento a los tickets de las y los profesores. Consultar y dar seguimiento a las solicitudes de soporte técnico que realizan las y los profesores a través de la plataforma. Parte del seguimiento se realiza a través del correo electrónico proporcionado por el/la profesor(a)	JDSyT
Dar seguimiento a las consultas de alumnos(as) de su plantel. Consultar y dar seguimiento a las solicitudes de las y los alumnos para contactar a sus profesores(as).	SAP
Enviar información a las y los alumnos. El/la profesor(a) puede enviar información sobre su clase a sus grupos. Esta información puede contener datos personales de las y los profesores.	SAP/Profesores(as)
Generar y consultar tickets. El/la profesor(a) puede levantar tickets referentes a dudas técnicas o de los procesos realizados en la ENP. Esta información puede contener datos personales de las y los profesores.	SAP/Profesores(as)
Consultar información de sus grupos. El/la profesor(a) puede consultar y descargar el listado de las y los alumnos de sus grupos con sus evaluaciones.	SAP/Profesores(as)
Cargar evaluaciones. El/la profesor(a) puede cargar (agregar o modificar) evaluaciones de las y los alumnos de sus grupos	SAP/Profesores(as)
Consultar información enviada por las y los profesores al grupo. Las y los alumnos pueden consultar la información que las y los profesores publican para sus grupos. Esta información puede contener datos personales de las y los profesores	SAP/Alumnos(as)
Generar búsquedas de profesores(as). Las y los alumnos pueden realizar búsquedas de sus profesores(as), así como revisar el estatus de dichas solicitudes.	SAP/Alumnos(as)
Consultar evaluaciones. Las y los alumnos pueden realizar consultas de las evaluaciones publicadas por sus profesores(as).	SAP/Alumnos(as)
Registrar participación a eventos académicos. Las y los alumnos pueden realizar su registro a diferentes eventos académicos publicados en el sistema. La información de registro contiene datos personales y académicos de las y los alumnos.	SAP/Alumnos(as)

DGENP/CGC/ContactoENP - formato 3

Activos asociados al sistema

Perfil de activo de información			
Activo de información crítico	Motivo de la selección		Descripción
Base de datos	Recurso que almacena datos personales, laborales, sensibles y académicos de miembros de la comunidad de la ENP.		La base de datos almacena datos de las y los profesores y de las y los alumnos de la ENP. Almacena número de trabajador, RFC, CURP, número de cuenta, nombre, fecha de nacimiento, nombramiento, lugar de trabajo, género, correo electrónico institucional, grado de estudios
Propietario(s)			
Coordinación General de Cómputo de DG			
Requerimientos de seguridad			
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo		Sólo puede acceder directamente a la base de datos el personal de la Coordinación General de Cómputo que la administra y los encargados del servidor de la base de datos
Integridad	Solo el siguiente personal autorizado puede modificar el activo		Sólo puede acceder directamente a la base de datos el personal de la Coordinación General de Cómputo que la administra, previa solicitud o autorización del propietario
Disponibilidad	El activo debe estar disponible para el personal		El personal autorizado podrá acceder a la información de la base de datos todos los días excepto cuando se realice mantenimiento de los servidores
	Los horarios en que debe estar disponible la información		La información de la base de datos debe estar disponible todos los días a cualquier hora, excepto cuando se realice mantenimiento de los servidores
Otros	Indicar si se debe de tener si el activo debe de contar con algún requerimiento diferente a los anteriores		No aplica
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (/ No)	Integridad (Si/No)	Disponibilidad (Si/No)	Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)			
Tipo de contenedor	Interno		
Categoría	Descripción		Propietario(s)
Técnico	Base de datos		Coordinación General de Cómputo
Física	Servidor ubicado en la Coordinación General de Cómputo		Coordinación General de Cómputo
Administrativo			
Tipo de contenedor	Externo		
Categoría	Descripción		Propietario(s)
Técnico	No se cuenta con contenedor técnico externo		
Física	No se cuenta con contenedor físico externo		
Administrativo			
Riesgo del Activo de información			
Área de preocupación	Divulgación de datos personales de las y los profesores y alumnos(as) almacenados en la base de datos		
Actor	Personas no autorizadas que ingresen a la base de datos		

Plataforma de contacto-ENP

Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Obtención de las credenciales de acceso a la base de datos por divulgación por parte de los administradores		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados ¿Qué efecto tendría la vulneración del activo de información?	(X) Revelación	( ) Destrucción	
	( ) Modificación	( ) Interrupción	
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Uso de credenciales de autenticación del usuario administrador por usuarios no autorizados		
Probabilidad	(X) baja	( ) Media	() Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	Valor	Puntaje
Se revelan datos de personales de las y los profesores o alumnos(as), quienes perderán la confianza en el proceso y en el sistema	[redacted]		
Pueden existir quejas por parte de las y los profesores o alumnos(as) afectados			
Puntaje del valor relativo			63

Mitigación del riesgo Acción a tomar para mitigar el riesgo			
(X) aceptar	**( ) aplazar**	**() Mitigar**	**( ) Transferir**
Indicar las medidas a realizar conforme al riesgo			
Base de datos	Debido a la acción seleccionada, no se aplicarán medidas		

Perfil de activo de información		
Activo de información critico	Motivo de la selección	Descripción
Sistema Contacto-ENP	Mediante el sistema se puede ingresar a la información personal de las y los profesores o alumnos(as) de la ENP	Mediante el sistema se realiza tratamiento de datos personales de profesores(as) y alumnos(as) de la ENP: número de trabajador, RFC, número de cuenta, nombre, fecha de nacimiento, lugar de trabajo, correo electrónico institucional
Propietario(s)		
Coordinación General de Cómputo de DG		
Requerimientos de seguridad		

Confidencialidad	Solo el siguiente personal autorizado puede ver el activo		Sólo puede visualizar los datos personales a través del sistema: - El personal encargado del seguimiento de búsquedas de profesores(as) realizadas por las y los alumnos - El personal encargado del seguimiento de tickets realizados por las y los profesores - Las y los profesores (su información personal y la información personal de identificación de las y los alumnos de sus grupos) - Las y los alumnos (su información personal y la información personal de identificación de las y los profesores de sus grupos)
Integridad	Solo el siguiente personal autorizado puede modificar el activo		Sólo las y los alumnos pueden realizar modificaciones de sus datos académicos
Disponibilidad	El activo debe estar disponible para el personal		Todas y todos los profesores, alumnos y usuarios del sistema pueden acceder a este todos los días excepto cuando se realice mantenimiento de los servidores
	Los horarios en que debe estar disponible la información		Todas y todos los profesores, alumnos y usuarios del sistema pueden acceder a este todos los días a cualquier hora, excepto cuando se realice mantenimiento de los servidores
Otros	Indicar si se debe de tener si el activo debe de contar con algún requerimiento diferente a los anteriores		No aplica
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (/ No)	Integridad (Si/No)	Disponibilidad (/No)	Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)			
Tipo de contenedor	Interno		
Categoría	Descripción		Propietario(s)
Técnico	Aplicativo web		Coordinación General de Cómputo
Física	Servidor ubicado en la Coordinación General de Cómputo		Coordinación General de Cómputo
Administrativo			
Tipo de contenedor	Externo		
Categoría	Descripción		Propietario(s)
Técnico	No se cuenta con contenedor técnico externo		
Física	No se cuenta con contenedor físico externo		
Administrativo			
Riesgo del Activo de información			
Área de preocupación	Divulgación de datos personales de las y los profesores o alumnos(as) de la ENP		
Actor	Profesores(as) que accedan a la sesión de otro profesor(a) Alumnos(as) que ingresen con los datos de autenticación de otro(a) alumno(a) Personas no autorizadas que ingresen a la sesión de algún(a) profesor(a)		
Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Uso de información de fácil conocimiento para autenticación de las y los profesores y alumnos(as) de la ENP		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados	( ) Revelación		( ) Destrucción
	( ) Modificación		( ) Interrupción

Plataforma de contacto-ENP

¿Qué efecto tendría la vulneración del activo de información?			
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Mediante el uso de datos de autenticación de las y los profesores de la ENP		
Probabilidad	( ) baja	([redacted]) Media	( ) Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	Valor	Puntaje
Se revelan datos de personales de las y los profesores o alumnos(as), quienes perderán la confianza en el proceso y en el sistema	[redacted]		
Pueden existir quejas por parte de las y los profesores o alumnos(as) afectados			
Algún(a) alumno(a) puede ingresar con los datos de otro(a) alumno(a) para registrarlo en algún evento académico, pudiendo modificar algún dato académico, pe. Su cuenta de correo institucional.			
Puntaje del valor relativo			

Mitigación del riesgo Acción a tomar para mitigar el riesgo			
( ) aceptar	**( ) aplazar**	**([redacted]) Mitigar**	**( ) Transferir**

Indicar las mediadas a realizar conforme al riesgo	
Aplicativo web	[redacted]
Profesores(as) y alumnos(as)	

Plataforma de contacto-ENP

DGENP/CGC/ContactoENP - formato 4

Plan de trabajo

Control	Actividad a realizar	Duración	Prioridad	Áreas responsables

Sistema de boletines

DGENP/SG/Boletines - formato 1

Identificador único	DGENP/SG/Boletines
Nombre del sistema	Sistema de Administración de Boletines
Datos personales (sensibles o no) contenidos en el sistema	1) Datos personales en general: a) Datos de identificación: número de trabajador, RFC, nombre b) Datos laborales: documentos de reclutamiento, puesto d) Datos académicos: títulos/cédulas profesionales 2) Datos sensibles: género
Responsables	
Nombre	Secretaría General de la ENP
Cargo	Secretario General de la ENP
Funciones	- Designar al personal responsable para la manipulación física de la información recibida. - Designar al personal responsable de la manipulación de la información dentro del sistema.
Obligaciones	- Salvaguardar los datos personales que recibe la Secretaría. - No difundir la información de datos personales a personas no autorizadas.
Encargados	
Nombre del encargado 1	Departamento de Sistemas y Telecomunicaciones
Cargo	Jefe de Sistemas y Telecomunicaciones
Funciones	- Realizar las actividades de administración y mantenimiento de la B.D. - Realizar las actividades de administración y mantenimiento del servidor de aplicaciones.
Obligaciones	- Proteger el entorno donde viven los datos personales de accesos no autorizados. - No modificar la información de datos personales almacenada en los servidores. - No difundir la información de datos personales contenidos en los servidores.
Nombre del encargado 2	Desarrollador del sistema
Cargo	Técnico(a) Académico(a)
Funciones	- Agregar y administrar la información de datos personales - Respaldar y actualizar la información de datos personales
Obligaciones	- Prevenir el acceso de usuarios a módulos o funcionalidades no autorizadas. - Prevenir el daño a los datos personales. - No modificar sin la autorización del responsable, la información de datos personales almacenada en los servidores. - No difundir la información de datos personales contenidos en los servidores.
Usuarios	
Nombre del usuario 1	Administrador de boletines DG
Cargo	Departamento de Asignaciones. Secretaría General de la ENP
Funciones	- Digitalizar y cargar información personal, laboral y académica. - Agregar y consultar información personal. - Archivar información laboral.
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Nombre del usuario 2	Administrador de boletines Plantel
Cargo	Secretario(a) General de Plantel
Funciones	- Consultar información laboral. - Agregar y consultar información personal.
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Nombre del usuario 3	Consultor de información DG
Cargo	Unidad Administrativa
Funciones	- Consultar información personal y laboral.
Obligaciones	- No difundir la información de datos personales a personas no autorizadas. - Utilizar el sistema únicamente con el perfil asignado.
Nombre del usuario 4	Profesores
Cargo	Académicos
Funciones	- Consulta de su información personal y laboral.

Sistema de boletines

Obligaciones	- Utilizar el sistema únicamente con el perfil asignado.		
Estructura			
Tipo de soporte	Físico y electrónico		
Descripción	Soporte físico: expedientes Soporte electrónico: Base de datos, repositorio digital		
Características del lugar donde se resguardan los soportes	Soporte físico: archiveros en las oficinas con puerta y llave, bajo el resguardo del personal de la Secretaría General de la DG Soporte electrónico: servidor de bases de datos y servidor de respaldos		
Análisis de Riesgo			
Riesgo	Impacto	Mitigación	
[redacted]			
Análisis de brecha			
Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación	
[redacted]			
Plan de trabajo			
Actividad	Descripción	duración	Cobertura
[redacted]			

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema de boletines

[redacted]

DGENP/SG/Boletines - formato 2

De acuerdo con el catalogo de áreas y roles llenar las funciones asociadas al sistema, enunciar el procedimiento, párrafo corto.

Tratamiento de datos personales	**Área (siglas)**
Ejemplo: Cargar los datos del directorio a la base de datos del SIEEL	JDSyT
Ejemplo: Descargar la lista de alumnos inscritos a los exámenes extraordinarios	SecEsc
Designar al personal de la Secretaría General de la DG responsable de la manipulación de los datos personales.	SG
Asignar profesores de nuevo ingreso a vacantes de grupo: Digitalizar y cargar información de reclutamiento.	SG
Consultar información personal, laboral y académica de los profesores de la ENP.	SG
Manipular de expedientes físicos: archivar información de reclutamiento.	SG
Realizar las actividades de administración y mantenimiento de la B.D.	JDSyT
Realizar las actividades de administración y mantenimiento del servidor de aplicaciones.	JDSyT
Agregar y administrar la información de datos personales.	JDSyT
Respaldar y actualizar la información de datos personales.	JDSyT
Consultar información personal de los profesores adscritos al plantel.	SGP
Consultar la información de reclutamiento de los profesores que ingresan al plantel a cubrir alguna vacante	SGP
Asignar profesores del plantel a las vacantes del mismo: Agregar información personal de los profesores	SGP
Consultar los datos personales de los profesores de la ENP	JUA
Consultar la información de reclutamiento de los profesores de la ENP	JUA

Sistema de boletines

DGENP/SG/Boletines - formato 3

Activos asociados al sistema

Perfil de activo de información			
Activo de información crítico	Motivo de la selección		Descripción
Base de datos	Recurso que almacena los datos personales de los profesores de la ENP y datos personales y sensibles de los responsables del proceso de asignaciones		La base de datos almacena datos de los profesores de la ENP, los responsables de la asignación de candidatos, y de los usuarios del Sistema de Administración de Boletines. Almacena número de trabajador, RFC, nombre, puesto y género de los responsables
Propietario(s)			
Secretaría General de DG			
Requerimientos de seguridad			
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo		Sólo puede acceder directamente a la base de datos el personal de la Coordinación General de Cómputo que la administra y los encargados del servidor de la base de datos
Integridad	Solo el siguiente personal autorizado puede modificar el activo		Sólo puede acceder directamente a la base de datos el personal de la Coordinación General de Cómputo que la administra, previa solicitud o autorización del propietario
Disponibilidad	El activo debe estar disponible para el personal		El personal autorizado podrá acceder a la información de la base de datos todos los días excepto cuando se realice mantenimiento de los servidores
	Los horarios en que debe estar disponible la información		La información de la base de datos debe estar disponible todos los días a cualquier hora, excepto cuando se realice mantenimiento de los servidores
Otros	Indicar si se debe de tener si el activo debe de contar con algún requerimiento diferente a los anteriores		No aplica
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (/ No)	Integridad (Si/No)	Disponibilidad (/No)	Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)			
Tipo de contenedor	Interno		
Categoría	Descripción		Propietario(s)
Técnico	Base de datos		Secretaría General de DG
Física	Servidor ubicado en la Coordinación General de Cómputo		Coordinación General de Cómputo
Administrativo			
Tipo de contenedor	Externo		
Categoría	Descripción		Propietario(s)
Técnico	No se cuenta con contenedor técnico externo		
Física	No se cuenta con contenedor físico externo		
Administrativo			
Riesgo del Activo de información			
Área de preocupación	Divulgación de datos personales de los profesores y usuarios almacenados en la base de datos		
Actor	Personas no autorizadas que ingresen a la base de datos		

Sistema de boletines

Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Obtención de las credenciales de acceso a la base de datos por divulgación por parte de los administradores		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados ¿Qué efecto tendría la vulneración del activo de información?	(X) Revelación	( ) Destrucción	
	( ) Modificación	( ) Interrupción	
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Uso de credenciales de autenticación del usuario administrador por usuarios no autorizados		
Probabilidad	(X) baja	( ) Media	() Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	Valor	Puntaje
Se revelan datos de personales de los profesores, quienes perderán la confianza en el proceso y en el sistema	[redacted]		
Pueden existir quejas por parte de los profesores afectados			
Puntaje del valor relativo			
Mitigación del riesgo Acción a tomar para mitigar el riesgo			
(X) aceptar	**( ) aplazar**	**() Mitigar**	**( ) Transferir**
Indicar las medidas a realizar conforme al riesgo			
[redacted]			

Perfil de activo de información		
Activo de información crítico	Motivo de la selección	Descripción
Documentación laboral y de reclutamiento	Documentación que contiene información personal, laboral y académica	Expediente de los profesores de nuevo ingreso
Propietario(s)		
Secretaría General de DG		
Requerimientos de seguridad		
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo	Sólo puede visualizar los datos personales a través del sistema: - El personal encargado de las asignaciones de profesores a las vacantes de grupos

			(con los expedientes físicos y a través del sistema a los expedientes digitalizados) - El personal que consulta las asignaciones de profesores a las vacantes de grupos (sólo a través del sistema a los expedientes digitalizados) - Los profesores que fue asignado a las vacantes de grupos (sólo su información personal a través del sistema)
Integridad	Solo el siguiente personal autorizado puede modificar el activo		Sólo puede modificar los expedientes: - El personal encargado de las asignaciones de profesores de nuevo ingreso a las vacantes de grupos (expediente físico) - el personal de la Coordinación General de Cómputo que la administra, previa solicitud o autorización del propietario (expediente digital)
Disponibilidad	El activo debe estar disponible para el personal		Los expedientes digitales deberán estar disponibles todos los días, a través del sistema Los expedientes físicos deberán estar disponibles sólo en horario laboral
	Los horarios en que debe estar disponible la información		Excepto cuando se realicen actividades de soporte en los servidores, los expedientes digitales deberán estar disponibles todos los días y en cualquier horario, a través del sistema Los expedientes físicos deberán estar disponibles sólo en días y horas laborales
Otros	Indicar si se debe de tener si el activo debe de contar con algún requerimiento diferente a los anteriores		No aplica
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (/ No)	Integridad (Si/No)	Disponibilidad (/No)	Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)			
Tipo de contenedor	Interno		
Categoría	Descripción		Propietario(s)
Técnico	Documentos digitalizados		Secretaría General de DG
Física	Oficina y archiveros con los expedientes físicos Servidor ubicado en la Coordinación General de Cómputo		Secretaría General de DG Coordinación General de Cómputo
Administrativo			
Tipo de contenedor	Externo		
Categoría	Descripción		Propietario(s)
Técnico	El manejo de los expedientes en planteles es ajeno al proceso realizado en DG		Secretaría General de Plantel
Física	El manejo de los expedientes en planteles es ajeno al proceso realizado en DG		Secretaría General de Plantel
Administrativo			
Riesgo del Activo de información			
Área de preocupación	Divulgación de datos personales de los profesores y usuarios almacenados en la base de datos		
Actor	Personas no autorizadas que ingresen a la base de datos		

Sistema de boletines

Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Acceso no autorizado al espacio donde se almacenan los expedientes físicos		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados ¿Qué efecto tendría la vulneración del activo de información?	(X) Revelación	( ) Destrucción	
	( ) Modificación	( ) Interrupción	
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	En alguna toma de la dependencia personal no autorizado podría violentar el espacio físico donde se encuentran los expedientes		
Probabilidad	( ) baja	(X) Media	() Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
Se revelan datos de personales de los profesores, quienes perderán la confianza en el proceso y en el sistema	[redacted]		
Pueden existir quejas por parte de los profesores afectados			
Puntaje del valor relativo			
Mitigación del riesgo Acción a tomar para mitigar el riesgo			
( ) aceptar	**(X) aplazar**	**() Mitigar**	**( ) Transferir**
Indicar las medidas a realizar conforme al riesgo			
[redacted]			

Perfil de activo de información		
Activo de información critico	Motivo de la selección	Descripción
Sistema de Administración de Boletines	Mediante el sistema se puede ingresar a la información personal de identificación, laboral y de reclutamiento de los profesores de la ENP	Mediante el sistema se realiza tratamiento de datos personales de profesores y funcionarios de la ENP: número de trabajador, RFC, nombre y puesto de los responsables, así como de los archivos digitales de reclutamiento
Propietario(s)		
Secretaría General de DG		

Sistema de boletines

Requerimientos de seguridad			
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo		Sólo puede visualizar los datos personales a través del sistema: - El personal encargado de las asignaciones de profesores a las vacantes de grupos - El personal que consulta las asignaciones de profesores a las vacantes de grupos - Los profesores que fue asignado a las vacantes de grupos (sólo su información personal)
Integridad	Solo el siguiente personal autorizado puede modificar el activo		Sólo el personal encargado de las asignaciones de profesores a las vacantes de grupos puede modificar la información a través del sistema
Disponibilidad	El activo debe estar disponible para el personal		Todos los profesores y usuarios del sistema pueden acceder a este todos los días excepto cuando se realice mantenimiento de los servidores
	Los horarios en que debe estar disponible la información		Todos los profesores y usuarios del sistema pueden acceder a este todos los días a cualquier hora, excepto cuando se realice mantenimiento de los servidores
Otros	Indicar si se debe de tener si el activo debe de contar con algún requerimiento diferente a los anteriores		No aplica
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (/ No)	Integridad (Si/No)	Disponibilidad (/No)	Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)			
Tipo de contenedor	Interno		
Categoría	Descripción		Propietario(s)
Técnico	Aplicativo web		Secretaría General de DG
Física	Servidor ubicado en la Coordinación General de Cómputo		Coordinación General de Cómputo
Administrativo			
Tipo de contenedor	Externo		
Categoría	Descripción		Propietario(s)
Técnico	No se cuenta con contenedor técnico externo		
Física	No se cuenta con contenedor físico externo		
Administrativo			
Riesgo del Activo de información			
Área de preocupación	Divulgación de datos personales de los profesores		
Actor	Profesores que accedan a la sesión de otro profesor Personas no autorizadas que ingresen a la sesión de algún profesor		
Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Uso de información de fácil conocimiento para autenticación de los profesores de la ENP		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados ¿Qué efecto tendría la vulneración del activo de información?	( ) Revelación	( ) Destrucción	
	( ) Modificación	( ) Interrupción	
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Mediante el uso de datos de autenticación de los profesores de la ENP		
Probabilidad	( ) baja	( ) Media	( ) Alta

Sistema de boletines

Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	Valor	Puntaje
Se revelan datos de personales de los profesores, quienes perderán la confianza en el proceso y en el sistema	[redacted]		
Pueden existir quejas por parte de los profesores afectados			
Puntaje del valor relativo			

Mitigación del riesgo Acción a tomar para mitigar el riesgo			
( ) aceptar	**( ) aplazar**	**( ) Mitigar**	**( ) Transferir**

Indicar las mediadas a realizar conforme al riesgo	
Aplicativo web	Realización de un módulo para que los profesores puedan modificar su contraseña para evitar el uso de contraseñas de conocimiento público
Profesores	Uso de contraseñas personales y robustas

DGENP/SG/Boletines - formato 4

Plan de trabajo

Control	Actividad a realizar	Duración	Prioridad	Áreas responsables
[redacted]				

Sistema Integral de Personal (SIP)

DGENP/Sistema Integral de Personal (SIP)- formato 1

Identificador único	DGENP/ SADMIN /SIP
Nombre del sistema	Sistema Integral de Personal (SIP)
Datos personales (sensibles o no) contenidos en el sistema	**Datos de identificación** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, fotografía, idioma o lengua. **Datos laborales** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros. **Datos académicos** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos.
Responsables	
Nombre	
Cargo	Secretario Administrativo
Funciones	Solicita usuario y contraseñas para los usuarios del SIP Autoriza el uso e instalación del SIP en equipos Consulta de movimientos y de información
Obligaciones	Control de las personas y equipos con acceso al SIP Asegurar el buen uso y la correcta captura de información
Encargados	
Nombre del encargado 1	
Cargo	Jefe de personal Académico
Funciones	Coordinar el trabajo de los supervisores para la captura de información del personal académico

Sistema Integral de Personal (SIP)

Obligaciones	Asegurar el buen uso y la correcta captura de información tanto de él como de su personal a cargo (supervisores)
Nombre del encargado 2	
Cargo	Jefa de Personal Administrativo
Funciones	Captura de información y movimientos del personal administrativo
Obligaciones	Asegurar el buen uso y la correcta captura de información
Nombre del encargado 3	
Funciones	
Obligaciones	

Usuarios	
Nombre del usuario 1	
Cargo	Supervisor
Funciones	Captura de información de los movimientos del personal
Obligaciones	Asegurar el buen uso y la correcta captura de información
Nombre del usuario 2	
Cargo	Director(a) General de la ENP
Funciones	Autoriza movimientos mediante la firma electrónica
Obligaciones	Asegurar el buen uso y la correcta captura de información
Nombre del usuario 3	
Cargo	
Funciones	
Obligaciones	
Nombre del usuario 4	

Sistema Integral de Personal (SIP)

Cargo	
Funciones	
Obligaciones	

Estructura

Tipo de soporte	Físico/Electrónico
Descripción	PC/Archivos PDF / Formatos / Expedientes
Características del lugar donde se resguardan los soportes	(Físico 3 oficinas con mobiliario similar, pero tamaños diferentes) Puertas con cristal y cerraduras con llaves, archiveros de 3 cajones con cerraduras. Electrónico: 12 equipos de cómputo para el uso del sistema

Análisis de Riesgo

Riesgo	Impacto	Mitigación
[redacted]		

Análisis de brecha

Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación
[redacted]		

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema Integral de Personal (SIP)

[redacted]

Actividad	Descripción	Plan de trabajo duración	Cobertura
[redacted]			

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema Integral de Personal (SIP) - formato 2

De acuerdo con el catalogo de áreas y roles llenar las funciones asociadas al sistema, enunciar el procedimiento, párrafo corto.

Tratamiento de datos personales	Área (siglas)
Capturar la información del personal y archivar los documentos físicos	SADMIN, UA
Escaneo de documentos con información del personal	SADMIN, UA
Descarga e impresión de relaciones, Kardex, y rechazos	SG

Sistema Integral de Personal (SIP) - formato 3

Activos asociados al sistema

Activo de información critico	Perfil de activo de información Motivo de la selección	Descripción
Equipo de cómputo con acceso al SIP	En estos equipos se encuentra instalado el sistema SIP y se resguardan documentos obtenidos del mismo	Los documentos descargados del sistema pueden contener los siguientes datos: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, fotografía, idioma o lengua. Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
Archiveros	Los documentos impresos desde el sistema SIP se resguardan e diferentes archiveros	Los documentos impresos desde el sistema pueden contener los siguientes datos:

		Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, fotografía, idioma o lengua. Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
Propietario(s)		
Los propietarios son todos los usuarios encargados de la atención a los movimientos de personal		
Requerimientos de seguridad		
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo	Solo el personal encargado por los titulares de cada área interna de la Secretaría General, Secretaría Administrativa y Unidad Administrativa podrá acceder al activo.
Integridad	Solo el siguiente personal autorizado puede modificar el activo	Solo el personal encargado por los titulares de cada área interna de la Secretaría General, Secretaría Administrativa y Unidad Administrativa y Coordinación de Cómputo podrá acceder, agregor y/o modificar el activo.
Disponibilidad	El activo debe estar disponible para el personal	Solo el personal encargado por los titulares de cada área interna de la Secretaría General, Secretaría Administrativa y Unidad Administrativa podrá acceder, al activo. En días laborables para la UNAM
	Los horarios en que debe estar disponible la información	El activo deberá estar disponible en el Horario laborable de la DGENP, el cual es: Lunes a viernes de 8 am a 9 pm. En días laborables para la UNAM
Otros		El activo debe de contar con la trazabilidad de la actividad realizada por el personal.

Sistema Integral de Personal (SIP)

Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (**X**)	Integridad ( )	Disponibilidad ( )	Otros ( )

Entorno del riesgo del activo de la información (contenedor)		
Entorno Interno		
Categoría	Descripción del contenedor	Propietario(s)
Técnico	Equipo de cómputo de la DGENP	Titular de la DGENP Jefa de la Unidad Administrativa Jefa de Compras Jefa de la Bienes y Suministros
Física	Archiveros	Titular de la DGENP Jefa de la Unidad Administrativa Jefa de Compras Jefa de la Bienes y Suministros
Administrativo		
Entorno Externo		
Categoría	Descripción del contenedor	Propietario(s)
Técnico	Aplicativo de escritorio	Dirección General de Personal
	Firma electrónica	DGTIC
Física	Servidores de alojamiento de la base de datos	DGP
Administrativo	Se desconoce el personal involucrado al ser un contendor externo	

Riesgo del Activo de información	
Área de preocupación	Divulgación de datos personales de personal de la Universidad.
Actor	Personal no autorizado para el manejo del Sistema Integral de Personal y/o archiveros

Sistema Integral de Personal (SIP)

Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Ingeniería social para con el personal de la Unidad Administrativa o Titular de la Entidad o Dependencia Acceso al equipo de cómputo y/o documentos impresos Contaminación de equipo de cómputo con virus o malware.		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados ¿Qué efecto tendría la vulneración del activo de información?	(**X**) Revelación	(**X**) Destrucción	
	(**X**) Modificación	(**X**) Interrupción	
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Mediante el uso de contraseñas del personal autorizado de la DGENP. Falta de revocación de credenciales de un extrabajador. Falta de aplicación de buenas practicas en ciberseguridad.		
Probabilidad	( ) baja	(**X**) Media	( ) Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	**Valor**	**Puntaje**
Se revelan datos de personales de los proveedores y estos ya no querrán darse de alta ante la Universidad	[redacted]		
Puede existir denuncia por parte de los proveedores para resarcir el daño causado por la revelación de los datos personales			

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL:** Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema Integral de Personal (SIP)

	[redacted]
Puntaje del valor relativo	

Mitigación del riesgo

Acción a tomar para mitigar el riesgo

( ) aceptar	**( ) aplazar**	**(X) Mitigar**	**( ) Transferir**

Indicar las medidas a realizar conforme al riesgo

Contenedor en el que se aplicarán las medidas	[redacted]
Titular de la DGENP SG SADMIN UA	

Sistema Integral de Personal (SIP) - formato 4

Plan de trabajo

Control	Actividad a realizar	Duración	Prioridad	Áreas responsables
[redacted]				

Sistema Integral de Personal (SIP)

[redacted]	[redacted]

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema Integral de Personal (SIP)

[redacted]	[redacted]

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema Informe Anual

DGENP/SP/Informe Anual de Actividades - formato 1

Identificador único	DGENP/SP/INFORME_ANUAL	
Nombre del sistema	Informe Anual de Actividades	
Datos personales (sensibles o no) contenidos en el sistema	Datos de identificación: RFC, CURP, domicilio, fecha de nacimiento, estado civil, celular, correo, nombre.	
Responsables		
Nombre		
Cargo	Jefatura de Evaluación y Seguimiento	
Funciones	Gestión de información, monitoreo de la captura de datos, elaboración de consultas y reportes.	
Obligaciones	Resguardo de bases, empleo de contraseñas para acceder al equipo y a la información.	
Encargados		
Nombre del encargado 1		
Cargo	Técnico Académico	
Funciones	Soporte técnico y mantenimiento del sistema.	
Obligaciones	Procesar bases de datos, alimentar el sistema y manejo de los datos recabados.	
Nombre del encargado 2		
Cargo		
Funciones		
Obligaciones		
Nombre del encargado 3		
Funciones		
Obligaciones		
Usuarios		
Nombre del usuario 1	Personal académico y docente de la ENP.	
Cargo	Personal académico y docente de la ENP.	
Funciones	Ingreso al sistema y reporte de informes anual de actividades.	
Obligaciones	Resguardar sus credenciales de acceso, así como la información recabada y realizar buenas prácticas en el manejo de datos sensibles.	
Nombre del usuario 2		
Cargo		
Funciones		
Obligaciones		
Nombre del usuario 3		
Cargo		
Funciones		
Obligaciones		
Nombre del usuario 4		
Cargo		
Funciones		
Obligaciones		
Estructura		
Tipo de soporte	Electrónico	
Descripción	Base de datos.	
Características del lugar donde se resguardan los soportes	Servidor dentro de la DGENP.	
Análisis de Riesgo		
Riesgo	Impacto	Mitigación
[redacted]		

Sistema informe Anual

[redacted]			
Análisis de brecha			
Medida de seguridad actual	Medida de seguridad necesaria		Acciones para remediación
[redacted]			
Plan de trabajo			
Actividad	Descripción	duración	Cobertura
[redacted]			

DGENP/SP/Informe Anual de Actividades - formato 2

De acuerdo con el catalogo de áreas y roles llenar las funciones asociadas al sistema, enunciar el procedimiento, párrafo corto.

Tratamiento de datos personales	**Área (siglas)**
Cargar los datos de los académicos nuevos.	CGC
Monitorear proceso.	CGC
Generación de documentos.	CGC

DGENP/SP/Informe Anual de Actividades - formato 3

Activos asociados al sistema

Perfil de activo de información

Sistema informe Anual

Activo de información critico	Motivo de la selección	Descripción
Datos de los académicos de la ENP y las actividades realizadas en el año	Son datos sensibles.	Contienen datos personales que identifican a los académicos de la ENP y la captura de sus actividades en el año.
Propietario(s)		
Requerimientos de seguridad		
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo	Sólo el personal de la CGC y el encargado de la SP tienen acceso a dicho activo.
Integridad	Solo el siguiente personal autorizado puede modificar el activo	Sólo el personal de la CGC y el encargado de la SP tienen acceso a la modificación y actualización dicho activo.
Disponibilidad	El activo debe estar disponible para el personal	La base de datos debe estar disponible para el personal del área de la CGC y al encargado de la SP.
	Los horarios en que debe estar disponible la información	En el horario laboral.
Otros	N/A	N/A
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo		
Confidencialidad (Si / No)	Integridad (Si/No)	Disponibilidad (Si/No) / Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)		
Entorno Interno		
Categoría	Descripción del contenedor	Propietario(s)
Técnico	Base de datos de MySQL	Jefe de la CGC
Física	Servidor de la CGC.	Jefe de la CGC
Administrativo		
Entorno Externo		
Categoría	Descripción del contenedor	Propietario(s)
Técnico	N/A	N/A
	N/A	N/A
Física	N/A	N/A
Administrativo	N/A	N/A
Riesgo del Activo de información		
Área de preocupación	Divulgación de datos personales de los académicos.	
Actor	Personal no autorizado consultando, editando o accediendo a la base de datos.	
Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Ingeniería social para con el personal de la CGC y la SP.	
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)	
Resultados ¿Qué efecto tendría la vulneración del activo de información?	(X) Relevancia (X) Modificación	( ) Destrucción ( ) Interrupción
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Acceder a los equipos dedicados y a su base de datos o a los archiveros.	
Probabilidad	(X) baja / ( ) Media / ( ) Alta	
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?	
	Área de impacto	Valor / Puntaje
Se revelan datos de personales de los proveedores y estos ya no querrán darse de alta ante la Universidad	[redacted]	

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL:** Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Puede existir denuncia por parte de los proveedores para resarcir el daño causado por la revelación de los datos personales	[redacted]
Puntaje del valor relativo	
Mitigación del riesgo Acción a tomar para mitigar el riesgo	
( ) aceptar	**( ) aplazar**	**(X) Mitigar**	**( ) Transferir**
Indicar las mediadas a realizar conforme al riesgo	
Base de datos y servidores	Mejorar la seguridad de los servidores.

DGENP/SP/Informe Anual de Actividades - formato 4

Plan de trabajo

Control	Actividad a realizar	Duración	Prioridad	Áreas responsables
[redacted]				

Eliminado: Análisis de Riesgo, Análisis de Brecha y Plan de Trabajo, contenido en el documento de seguridad, toda vez que de dar a conocer dicha información, potencializa el nivel de vulnerabilidad de las medidas de seguridad para la protección de datos personales de la Dirección General de la Escuela Nacional Preparatoria, de la Universidad Nacional Autónoma de México, lo que traería como consecuencia aumentar la probabilidad d que se cometa la comisión de un delito tipificado en el Código Penal Federal, como lo son, el acceso no autorizado a los sistemas, robo de información, suplantación de identidad, entre otros. **FUNDAMENTO LEGAL**: Artículo 113 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, artículo 110 fracción VII de la Ley Federal de transparencia y acceso a la Información Publica, en correlación con el artículo 41 del Reglamento de Trasparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en la Gaceta UNAM el 25 de agosto de 2016, así como los numerales Quincuagésimo sexto y Sexagésimo primero de los Lineamientos Generales en materia de Clasificación y Desclasificación, así como para la elaboración de Versiones Públicas.

Sistema Automatizado de Evaluación Psicométrica

DGENP/UIAP/Sistema Automatizado de Evaluación Psicométrica - formato 1

Identificador único	DGENP/UIAP/PSICO	
Nombre del sistema	Sistema Automatizado de Evaluación Psicométrica	
Datos personales (sensibles o no) contenidos en el sistema	Varios: RFC, CURP, domicilio, fecha de nacimiento, estado civil, celular, correo, nombre, evaluaciones psicométricas.	
Responsables		
Nombre		
Cargo	Coordinador de la UIAP	
Funciones	Monitorear las evaluaciones de aspirantes.	
Obligaciones	Resguardo adecuado de los datos consultados, así como de los datos utilizados para ingresar al sistema.	
Encargados		
Nombre del encargado 1	Laura Ramírez Juárez	
Cargo	Técnico Académico	
Funciones	Programación y aplicación de evaluaciones.	
Obligaciones	Por medio de una sesión validada a través de una contraseña personal. Registro de aspirantes en el sistema. Consulta de resultado de las pruebas.	
Nombre del encargado 2		
Cargo		
Funciones		
Obligaciones		
Nombre del encargado 3		
Funciones		
Obligaciones		
Usuarios		
Nombre del usuario 1	Aspirantes en proceso de selección.	
Cargo		
Funciones		
Obligaciones		
Nombre del usuario 2		
Cargo		
Funciones		
Obligaciones		
Nombre del usuario 3		
Cargo		
Funciones		
Obligaciones		
Nombre del usuario 4		
Cargo		
Funciones		
Obligaciones		
Estructura		
Tipo de soporte	Ambos	
Descripción	Base de datos y reportes generados.	
Características del lugar donde se resguardan los soportes	Equipos de cómputo dedicados, carpeta y archivero.	
Análisis de Riesgo		
Riesgo	Impacto	Mitigación

Sistema Automatizado de Evaluación Psicométrica

Acceso no autorizado a los reportes impresos.	Filtración de datos sensibles y evaluaciones de los aspirantes.	Guardar bajo llave en un archivero dichos reportes.
Falla de software o hardware en los equipos dedicados.	Perdida parcial o total de los datos.	Realizar un respaldo al terminar de evaluar a un aspirante.
Vulneración de los archivos .mdb de las bases de datos.	Filtración, duplicidad y/o alteración de datos sensibles de los aspirantes.	Cifrado de la base de datos y aumentar los protocolos de seguridad en los equipos de cómputo de la aplicación de escritorio.
Análisis de brecha		
Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación
Acceso al equipo de cómputo dedicado, con contraseña. Electrónicamente el encargado tiene acceso al sistema de escritorio por medio del usuario y contraseña y el aspirante a través de RFC.	Agregar una contraseña aleatoria para los aspirantes.	Agregar campos de contraseña cifrada en el inicio de sesión del sistema.
Plan de trabajo		
Actividad	Descripción	duración	Cobertura
[redacted]			

DGENP/UIAP/Sistema Automatizado de Evaluación Psicométrica - formato 2

De acuerdo con el catalogo de áreas y roles llenar las funciones asociadas al sistema, enunciar el procedimiento, párrafo corto.

Tratamiento de datos personales	**Área (siglas)**
Cargar los datos del banco web.	UIAP
Dar de alta y monitorear evaluaciones.	UIAP
Analizar e imprimir resultados.	UIAP

DGENP/UIAP/Sistema Automatizado de Evaluación Psicométrica - formato 3

Activos asociados al sistema

Perfil de activo de información

Sistema Automatizado de Evaluación Psicométrica

Activo de información critico	Motivo de la selección		Descripción
Datos de los candidatos a profesor de la ENP	Son datos sensibles.		Contienen datos personales que identifican a los aspirantes.
Propietario(s)			
UIAP			
Requerimientos de seguridad			
Confidencialidad	Solo el siguiente personal autorizado puede ver el activo		Sólo el personal del área del proceso de evaluación de aspirantes.
Integridad	Solo el siguiente personal autorizado puede modificar el activo		Sólo el encargado del proceso de la aplicación del examen y el jefe de la UIAP tiene permitido actualizar los datos.
Disponibilidad	El activo debe estar disponible para el personal		La base de datos y reportes deben estar disponibles para el personal del área.
	Los horarios en que debe estar disponible la información		En el horario laboral.
Otros	N/A		N/A
Requerimiento de seguridad de mayor importancia Indicar cual es requerimiento de seguridad con mayor relevancia en el activo			
Confidencialidad (Si / No)	Integridad (Si/No)	Disponibilidad (Si/No)	Otros (Si/No)
Entorno del riesgo del activo de la información (contenedor)			
Entorno Interno			
Categoría	Descripción del contenedor		Propietario(s)
Técnico	Base de datos de Access		Jefe de la UIAP
Física	Equipo de cómputo dedicado de la UIAP y archiveros con las impresiones de las evaluaciones.		Jefe de la UIAP
Administrativo			
Entorno Externo			
Categoría	Descripcion del contenedor		Propietario(s)
Técnico	N/A		N/A
	N/A		N/A
Física	N/A		N/A
Administrativo	N/A		N/A
Riesgo del Activo de información			
Área de preocupación	Divulgación de datos personales de los candidatos y evaluaciones.		
Actor	Personal no autorizado consultando o editando las impresiones, alterando el equipo de cómputo o accediendo a la base de datos.		
Medios ¿Qué y cómo el actor explotaría la vulnerabilidad?	Ingeniería social para con el personal de la UIAP.		
Motivo	Allegase de datos personales para obtener un beneficio (económico, fama, otros)		
Resultados ¿Qué efecto tendría la vulneración del activo de información?	(X) Relevancia		( ) Destrucción
	(X) Modificación		( ) Interrupción
Requerimientos de seguridad ¿Cómo podrían ser violados los requerimientos de seguridad?	Acceder a los equipos dedicados y a su base de datos o a los archiveros.		
Probabilidad	(X) baja	( ) Media	( ) Alta
Consecuencias ¿Cuáles son las consecuencias para la organización o el propietario de los activos de información como resultado del resultado y el incumplimiento de los requisitos de seguridad?	**Severidad** ¿Qué tan graves son estas consecuencias para la organización o el propietario de los activos por área de impacto?		
	Área de impacto	Valor	Puntaje
Se revelan datos de personales de los proveedores y estos ya no querrán darse de alta ante la Universidad	Pérdida de confianza en el área universitaria (Reputación) – 9	[redacted]	
	Financiera 3		

Sistema Automatizado de Evaluación Psicométrica

Puede existir denuncia por parte de los proveedores para resarcir el daño causado por la revelación de los datos personales	Productividad 2	[redacted]
	Seguridad 1	
	Amonestación pública y medidas de apremio (en multas) del INAI / Sanciones y procesos legales (Multas / penas legales) 4	
	Incumplimiento de obligaciones legales 8	
	Interrupción del servicio **5**	
	Orden público **7**	
	Persecución de delitos **6**	
Puntaje del valor relativo		

Mitigación del riesgo Acción a tomar para mitigar el riesgo			
( ) aceptar	**( ) aplazar**	**(X) Mitigar**	**( ) Transferir**
Indicar las medidas a realizar conforme al riesgo			
[redacted]			

DGENP/UIAP/Sistema Automatizado de Evaluación Psicométrica - formato 4

Plan de trabajo

Control	Actividad a realizar	Duración	Prioridad	Áreas responsables
[redacted]				

Anexos

Anexo 1 : Términos, definiciones y abreviaturas

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.

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.

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.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. La información acadé- mica que obre en los archivos universitarios constituye un dato personal.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, así como opiniones políticas y preferencia sexual.

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.

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.

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.

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 intencionalmente.

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.

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.

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

Titular: Persona física a quien corresponden los datos personales.

Tratamiento: Cualquier operación(es) efectuadas mediante procedimientos manualeso automatizados aplicados a los datos personales, relacionadas con obtención, uso, registro, organización, conservación, elaboración, utilización, cumunicación, difusicón, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición.

Usuario: El funcionario, personal académico o empleado universitario que tiene una sesión en un equipo de cómputo específico.

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.

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.

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;

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

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.

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.

Anexo 2 : Políticas de actualización.

Objetivo

Definir las políticas y procedimientos para la actualización de sistemas operativos, software y software antimalware de los principales sistemas y equipos de cómputo (servidores, equipos de red, PC's) de la Dirección General de la Escuela Nacional Preparatoria.

Alcance

Las presentes políticas definen la periodicidad para la actualización de sistemas operativos, software y software antimalware conforme a los niveles de criticidad de los equipos de cómputo de la Dirección General de la Escuela Nacional Preparatoria.

Responsabilidades

Es responsabilidad de la Coordinación General de Cómputo de configurar inicialmente los equipos de cómputo dedicado a los usuarios de la Dirección de la Escuela Nacional Preparatoria con las siguientes características:

- Establecer los periodos de actividad del equipo para la instalación de actualizaciones de software
- Instalar software antimalware
- Instalar software para el desempeño de las funciones diarias del usuario que utilizará el equipo.

La actualización de los servidores y equipos de red estará bajo la responsabilidad de la Coordinación de Cómputo.
La responsabilidad de los trabajadores que cuenten con un equipo proporcionado por la Dirección General de la Escuela Nacional Preparatoria, son:

- Contactar a la Coordinación de Cómputo cuando el equipo indique la necesidad de actualizar.
- Analizar los dispositivos extraíbles que conecten a sus máquinas.
- Solamente conectar dispositivos extraíbles de confianza.
- Informar a la Coordinación de Cómputo cuando se desee instalar algún software.

Actualizaciones

Todo sistema operativo y software es susceptible a tener fallos y mejoras. Por ello, es indispensable que se instalen de forma periódica las actualizaciones que proporciona el fabricante.
Se debe de tener en cuenta que entre más tiempo pase entre actualizaciones, se está expuesto a que algún tipo de virus o malware pueda explotar alguna vulnerabilidad.

Servidores

Las actualizaciones de los servidores de producción se darán conforme a los siguientes puntos:

- Se prohíbe el uso de actualizaciones en versiones beta o similares.
- Las actualizaciones se deberán de probar con antelación en un ambiente similar.
- En caso de requerir reiniciar el equipo, dicha actualización se deberá aplicar en un horario que no afecte con las actividades del personal.
- En caso de necesitar instalar una actualización urgente, se deberá realizar una copia de seguridad completa del equipo antes de realizar la instalación.

Equipo administrativo

Los usuarios que cuenten con sistemas operativos Windows en sus equipos deberán de atender lo siguiente:

- Verificar que las actualizaciones automáticas se encuentren activadas. Esto se puede consultar de la siguiente forma:
  - Presionando el botón de inicio
  - Escribe “Windows Update” o “Buscar actualizaciones”
  - Hacer clic en el botón <<Buscar actualizaciones>> y en caso de tener una actualización

Usuarios que cuenten con sistemas operativos Mac, deberán de revisar las actualizaciones en:

- Para realizar una actualización en equipos Apple se debe de ingresar al apartado <<Actualización de Software>> o <<Software Update>>, el cual se encuentra en el Menú Apple de la barra principal.

Usuarios que cuenten con sistemas operativos Linux, deberán de realizar las siguientes acciones:

- Abrir una terminal y ejecutar las siguientes instrucciones:
  - Para derivaciones de Debian
    - apt update o apt-get update
    - apt upgrade o apt-get dist-upgrade
  - Para derivaciones de Red Hat
    - dnf update
    - yum update
  - Para derivaciones de Arch
    - pacman -Syy
    - aptitude update
    - pacman -Sulinux zypper
  - Para derivaciones de Suse
    - Zypper update

En caso de que se detecte que existen fallos en las actualizaciones para algún sistema operativo, se deberá avisar a cada uno de los responsables de las áreas de la Dirección General de la Escuela Nacional Preparatoria para que no se ejecuten actualizaciones, hasta nuevo aviso por parte de la Coordinación de Computo.

Periodicidad

La periodicidad nos indica la frecuencia con que las actualizaciones serán aplicadas. Para el equipo administrativo se deberán de realizar conforme a la siguiente periodicidad:

- Sistema operativo Windows
  - Verificar al menos una vez al mes si existe un nuevo parche de seguridad mediante la herramienta de Windows Update. En caso de existir un nuevo parche de seguridad, este se deberá dejar el equipo actualizando durante la noche.
  - Verificar al menos una vez cada semestre si existe una actualización de primer nivel. En caso de existir, se deberá de avisar a la Coordinación de Sistemas para que sea valorada la instalación de dicha actualización
- Sistema operativo MacOS, Linux, FreeBSD
  - Verificar mínimo una vez al mes.

Software

Para la instalación de nuevo software en el equipo de cómputo, el responsable del equipo deberá de contar con la licencia de activación en caso de requerirse y dar aviso a la Coordinación de Cómputo para que realice la instalación de dicho software.

Para las actualizaciones de software en equipo administrativo, la Coordinación de Cómputo dejara activa la actualización automática. En caso de que la actualización requiera reiniciar el equipo, el encargado del equipo decidirá el horario en el cual desea que se realice dicho reinicio.

En instalación y actualización de programas en servidores, la Coordinación de Cómputo primero instalará el nuevo software o actualización en un servidor de preproducción o QA, antes de pasar a producción, para evitar problemas de compatibilidad y disponibilidad de los servicios.

Control de cambios

Motivo del cambio	Autor del cambio	Descripción	Fecha	Versión
Creación		Creación de las políticas de actualización.		
Actualización		Se actualizan las responsabilidades.		
Actualización		Se actualiza documento.		
Actualización		Se actualiza el apartado de software.		
Revisión		Revisión de documento		

Anexo 3: Políticas de borrado seguro.

Objetivo

Definir las políticas y procedimientos para el borrado de archivos de los principales sistemas y equipos de cómputo (servidores, equipos de red, PC's) de la Unidad de Transparencia.

Alcance

Las presentes políticas definen el procedimiento para el borrado de archivos conforme a los niveles de criticidad de la información que se desee eliminar.

Responsabilidades

Es responsabilidad de cada uno de los jefes de las áreas funcionales de la Unidad de Transparencia dar aviso a la Coordinación de Sistemas sobre la transferencia de equipo entre personal, y es responsabilidad de la Unidad Administrativa de la Unidad de Transparencia avisar a la Coordinación de Sistemas con antelación sobre los equipos de cómputo que se darán de baja.

La Coordinación de Sistemas tiene como responsabilidad borrar la información de forma segura de los equipos que se van a dar de baja y de los equipos que van a ser traspasados; dicha información puede ser: fotos, documentos, música, videos o cualquier otro tipo de archivo de los equipos de cómputo de la Unidad de Transparencia.

Es responsabilidad del encargado del equipo de cómputo realizar el borrado seguro conforme a las presentes políticas de archivos con información sensible, reservada y/o que contenga datos personales.

Borrado seguro

El borrado seguro consiste en eliminar la información de cierta forma para que esta no pueda ser recuperada. Existen tres tipos de borrado seguro:

- Física: consiste en la destrucción total del dispositivo para que no sea recuperado por ningún medio la información que contuviese este. Este método es válido para cualquier tipo de dispositivo como: USB, SSD, HDD, CD, DVD, Blue-ray Disc, etc.
- Desmagnetización: consiste en exponer el dispositivo a un campo magnético. Este método de borrado seguro solo se puede utilizar en HDD, disquetes, cintas magnéticas, etc.
- Sobreescritura: consiste en la utilización de un software, el cual va a realizar una escritura de datos con ciertos patrones sobre el documento que se desea borrar. Este procedimiento no es aplicable para dispositivos que no son regrabables como CD, DVD, Blue-ray Disc, etc.

Aplicabilidad

Los tres métodos de borrado seguro no son aplicables a los diferentes dispositivos con los que se cuentan hoy en día. A continuación, se presenta la tabla de métodos de borrado seguro que se pueden aplicar a los diferentes dispositivos.

Dispositivo	Tipo de dispositivo	Destrucción física	Desmagnetización	Sobreescritura
Discos duros o HDD	Magnético	Aplica	Aplica	Aplica
Discos flexibles (floppies o disquetes)	Magnético	Aplica	Aplica	Aplica

Cintas	Magnético	Aplica	Aplica	Aplica
CD, DVD, Blue-ray disc	Óptico	Aplica	No aplica	No aplica
Pen driver o USB	Electrónico	Aplica	No aplica	Aplica**
Discos de estado sólido o SSD	Electrónico	Aplica	No aplica	Aplica**

**Para los dispositivos electrónicos se deben de utilizar herramientas que cuenten con estándares que aseguren el borrado seguro de la información.

Motivos

El borrado seguro se aplicará en los siguientes casos:

- Baja de equipo
- Archivos que sean trasladados al Sistema de Archivos.
- Equipo transferido a personal interno de la Unidad de Transparencia.
- Equipo transferido a una Área Universitaria diferente la Unidad de Transparencia.
- Solicitante exigiendo la cancelación de sus datos personales.

Herramientas

Las herramientas para el borrado seguro de archivos deben de contar como mínimo el método DoD5220.22-M para dispositivos magnéticos y el método NIST 800-88 para dispositivos como USB, SSD, etc.
Algunas de las herramientas que se pueden utilizar para realizar el borrado seguro, son:

- Windows
  - SDelete Wipe My Disks de HDDGURU
  - Eraser
- MacOS
  - Permanent eraser
  - Disk Utility
- Linux
  - srm
  - wipe
- Multiplataforma
  - dban
  - Blancco Driver Eraser

Bases de datos

El borrado seguro de la información contenida en cualquier tipo de motor de base de datos (MySQL, SQL, Oracle, etc) se deberá realizar mediante un método de sobreescritura de la información contenida en el registro o registros, posteriormente se procederá a realizar el borrado del registro: en caso de que el registro afecte la integridad de la información contenida en la base de datos solamente se realizará la anonimización o seudonimización de los datos.

Control de cambios

Motivo del cambio	Autor del cambio	Descripción	Fecha	Versión
Creación		Creación de las políticas de respaldo		
Actualización		Revisión del documento		
Actualización		Cambio en la redacción de una nota y se ajusta el texto		
Revisión		Revisión de documento		

Anexo 4: Políticas de contraseñas.

Objetivo

Definir las políticas y procedimientos para la creación, gestión y uso de contraseñas para sistemas y equipos de la Dirección General de la Escuela Nacional Preparatoria.

Alcance

Las presentes políticas la forma correcta para la creación de contraseñas robustas, buenas prácticas y la sugerencia para el almacenaje de estas.

Creación

Las contraseñas son las llaves con las cuales se puede acceder a los diferentes sistemas que contienen información personal o asuntos laborales, también nos permite acceder a herramientas de trabajo taeles como, correo electrónico, sitios institucionales, etc. Por ello es importante que una contraseña sea robusta y contenga como mínimo los siguientes puntos:

- Incluir letras mayúsculas y minúsculas (a-z A-Z),
- Incluir números (0-9)
- Incluir caracteres especiales, tales como: °!”#$%&/()=?¡|0¿
- Debe de tener una longitud mínima de 10 caracteres, Además, puede tomar en cuenta alguno de los siguientes puntos:
    - Elegir una frase que le resulte fácil de recordar o
    - Combinar dos o más palabras
    - Incluir mayúsculas y minúsculas en un orden específico para usted,
    - Escoge frases o palabras sin vocales
    - Cambia las vocales de las palabras por su representación numérica
    - Escoge algún número que te sea fácil de recordar y entre cada dígito una sucesión de letras
    - Usar una combinación de mayúsculas y minúsculas en las palabras

Para saber si la contraseña creada es segura, puede utilizar alguna de estas herramientas.

https://lowe.github.io/tryzxcvbn/

https://www.uic.edu/apps/strong-password/

https://password.kaspersky.com/es/

https://www.security.org/how-secure-is-my-password/

Gestión

De ser posible, utilice alguna herramienta de almacenamiento y gestión de contraseñas:

KeePass (Gratuito - https://keepass.info)

LastPass (Gratuito / Paga https://www.lastpass.com/es)

Enpass (Gratuito / Paga https://www.enpass.io/)

Keeper (Paga https://www.keepersecurity.com/es_ES/)

1Password (Paga https://1password.com/es/)

RoboForm (Gratuito / Paga https://www.roboform.com/es)

Las herramientas antes mencionadas cuentan con diferentes funcionalidades extras, la elección de dicha herramienta dependerá de las necesidades de cada uno.

Buenas prácticas

Evite usar alguna de las siguientes malas prácticas en el manejo de contraseñas:

- Apuntar las contraseñas en lugares no apropiados, tales como: libretas, post-its, pizarrones, papelitos o lugares poco seguros.
- Enviar contraseñas a través de un medio inseguro
- Usar una contraseña para todos los sistemas (correo, finanzas computadora, teléfono, etc)
- Utilizar datos personales en la creación de contraseñas (nombre, fecha de nacimiento, nombre de mascotas, etc)
- Utilizar contraseñas por defecto.
- Difundir la contraseña con personal no autorizado.
- Usar patrones predecibles o usar contraseñas poco seguras, tales como:
    - Qwerty
    - 1234567890
    - 123456
    - Password
    - password1
    - iloveyou

Ya que se sabe que practicas se deben de evitar, ahora veremos las practicas que se deben de realizar para mantener las diferentes cuentas seguras.

- Cambiar las contraseñas de forma periódica (cada 6 o 12 meses en sistemas no críticos y cada 2 o 3 meses en sistemas críticos)
- Uso de contraseñas únicas para cada sistema al que se tenga acceso
- Uso de gestores de contraseñas
- Uso de autenticación de doble factor (A2F) en los sistemas que lo permitan, como el correo institucional y para manejo de licencias de adobe.
- Acceder a los sitios mediante equipos seguros o confiables.

Control de cambios

Motivo del cambio	Autor del cambio	Descripción	Fecha
Creación		Creación de las políticas de contraseñas	

Actualización		Se modifican los temas	

Anexo 5: Bitácoras

	UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Formato de Bitácora de vulneraciones a los Sistemas de Información	
Nombre Sistema de Tratamiento	
Fecha del incidente	
Nombre de quien reporta el incidente	
Cargo	
Área universitaria	
Responsable del área	
Causa de la vulneración	
Componente(s) del sistema vulnerado(s)	
Cantidad de titulares de datos personales afectados	
Soporte de la información vulnerada	☐ Físico ☐ Electrónico ☐ Mixto
Seleccione el tipo de vulneración	☐ Pérdida o extravío ☐ Destrucción no autorizada
	☐ Robo ☐ Copia no autorizada
	☐ Uso, acceso o tratamiento no autorizado
	Daño, alteración o modificación no autorizada
Tipo de titular afectado	☐ Extranjeros ☐ Trabajadores ☐ Menores de edad ☐ Alumnos ☐ Estudiantes de movilidad nacional ☐ Profesores de asignatura ☐ Profesores de tiempo completo ☐ Investigadores ☐ Técnicos Académicos ☐ Proveedores o contratistas ☐ Terceros (visitantes, etc.)
Tipo de datos personales Comprometidos	☐ Identificativos Laborales
	☐ Datos Académicos
	☐ Procedimientos administrativos / Judiciales / Procedimientos seguidos en forma de juicio
	☐ Patrimonial ☐ Salud ☐ Afiliaciones políticas o ideológicas
	☐ Origen étnico ☐ Características Personales
	☐ Vida Sexual ☐ Discapacidades

Las acciones correctivas implementadas de forma inmediata y definitiva.		
Nombre y firma de quién reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del área