Documento de Seguridad para la Protección de Datos Personales en el Sistema de Administración Escolar (SAES)

Dirección de Administración Escolar

I.- Introducción

El presente documento tiene como finalidad describir y dar cuenta de las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Dirección de Administración Escolar del Instituto Politécnico Nacional, de conformidad con lo previsto en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, a efecto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales que obran en el Sistema de Administración Escolar (SAES).

La Dirección de administración Escolar (DAE), es la unidad administrativa del Instituto Politécnico Nacional (IPN) encargada de la gestión y seguimiento del estudiante, desde el proceso de admisión; durante toda su estancia en el IPN, realizando los diferentes trámites obligatorios y su acreditación oficial, hasta el trámite de titulación.

II.- Inventario de datos personales y de los sistemas de tratamiento.

El Sistema de Administración Escolar (SAES) es la herramienta informática diseñada para apoyar en la consulta y realización de trámites escolares de los alumnos del IPN.

En esta base de datos se encuentra la totalidad de la información de los alumnos pertenecientes a los niveles educativos de nivel Medio Superior y Superior del Instituto Politécnico Nacional, esta plataforma se encuentra administrada por la DAE; dicho sistema cuenta con dos interfaces, una interfaz de usuario basada en Web y es a través de este que la comunidad estudiantil tiene acceso a la revisión de su kardex, inscripciones, reinscripciones a semestres lectivos, con un cuenta y clave previamente autorizados. El SAES en su versión de escritorio, se encuentra instalado en el departamento de gestión escolar de todas y cada una de las Unidades académicas del IPN, al cual tienen acceso para consulta el director y subdirectores académicos y de servicios educativos, así como el personal adscrito al departamento, cuyo acceso y permiso solo los otorga la DAE, y como mecanismo de autorización y autenticación se cuenta con un usuario y contraseña.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece el concepto de datos personales, indicando que es cualquier información concerniente a una persona física identificada o identificable, considerándose que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información y, la definición específica de datos personales sensibles, que son aquellos que se refieran a las esfera más íntima, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En ese sentido, para el cumplimiento de las atribuciones y funciones del Instituto Politécnico Nacional, el SAES contiene los siguientes datos personales:

Datos personales de Alumnos	Nombre, edad, nacionalidad; fecha de nacimiento; clave del Registro Federal de Contribuyentes (RFC); Clave Única de Registro de Población (CURP), domicilio, correo personal; número de teléfono celular y casa; copias de identificación oficial, actas de nacimiento; firmas; comprobantes de domicilio. Número de Boleta, Nombre del padre o tutor.
Datos personales de padres	Nombre, Teléfono de oficina.
Datos personales de docentes	Nombre, CURP, Domicilio, Teléfono, Teléfono Celular, correo personal.

III.- Roles y responsabilidades de los involucrados en el tratamiento de datos personales.

Roles en el Sistema de Administración Escolar

Nombre	Descripción
Usuario sin login	Usuarios que utilizan huella digital para realizar acciones en SICOES
Registro	Departamento de registro (DAE)
Soporte	Soporte al Departamento de gestión escolar del plantel
Tutorias	Departamento de Tutorías, del plantel
Becas	Usuarios del plantel que consultan las trayectorias de los alumnos
Supervisión	Personal de Supervisión del departamento de registro (DAE)
Movilidad	Usuario complementario para el manejo de alumnos en Movilidad Académica
Jefe de control escolar	Representante del departamento de control escolar
Kardista	Secretarias del departamento de gestión escolar
Horarios	Usuarios de la subdirección académica del plantel
Caja	Usuarios del departamento de pagaduría del plantel
Archivo	Usuario del archivo del departamento de gestión escolar del plantel
Dictamenes	Asignación de dictámenes a un alumno
Enlace	Enlace gestión escolar - DAE

A) Servidor público administrador del sistema:

Nombre	Lic. Fabiola Guadalupe Rodríguez Jiménez
Cargo	Directora de la DAE
Funciones/perfil	Administrar la información del sistema para el cumplimiento de las atribuciones de la DAE
Obligaciones	Resguardar la información

Nombre	Titulares de las unidades académicas del IPN, Dirección de Educación Media Superior y Dirección de Educación Superior.
Cargo	Directores de las unidades académicas del IPN y de coordinación del IPN
Funciones/perfil	Administrar la información del sistema para el cumplimiento de las atribuciones de la unidad politécnica.
Obligaciones	Resguardar la información

B) Servidores públicos operadores del sistema: (ANEXO 1)

C) Servidores públicos usuarios del sistema: (ANEXO 2)

IV.- Análisis de riesgos.

En el análisis de riesgo se deben considerar las amenazas y vulneración a las que están expuestos los datos personales en posesión del responsable y los recursos involucrados en su tratamiento como pueden ser hardware, software y personal, principalmente.

Dirección General: Dirección de Administración Escolar

Nombre del Sistema: Sistema de Administración Escolar (SAES)

1.- Tipo de Soporte: Electrónico

Tipo de soporte: soporte electrónico.

a) Descripción: Base de datos que contiene la información correspondiente a la trayectoria escolar de los alumnos del IPN

2.- Características del Lugar donde se guardan los soportes:

Derivado de que el Sistema de Administración Escolar (SAES) es un sistema descentralizado, esto quiere decir, que la información se almacena en diferentes bases de datos las cuales se encuentran en un servidor independiente en cada Unidad Académica.

3.- Amenazas y vulnerabilidades:

Se encuentran en el entorno social, tecnológico, ambiental:

a) Amenazas sociales: técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de los usuarios del sistema para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta. Son todas las acciones, causadas por la intervención humana, que violan la ley y que están penadas por esta. Como puede ser Perdida de información por rotación, salida de personal, mal manejo de equipos y programas.

b) Amenazas tecnológicas: Todas aquellas amenazas que pueden ser generadas por medios electrónicos ya sea por Malware o código malicioso, botnets, y ataques en la red como una Denegación de servicio o de diccionario de datos.

c) Amenazas Institucionales: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionadas con el comportamiento humano.

d) Vulnerabilidades ambientales/físicas: Son todas aquellas que no se tiene control por parte del sistema, y exponen la información que se encuentra en los equipos servidores, siendo así, inundaciones, incendios, temblores, entre otras.

e) Vulnerabilidades económicas: Aquellas que no depende del sistema de manera lógica, pero afectan su funcionalidad poniendo en riesgo la información almacenada. Los equipos de cómputo que cuentan con información importante, deben encontrarse en ambientes físicos aptos, ventilación apropiada, aire acondicionado para evitar calentamiento en los procesadores de los equipos, instalaciones eléctricas adecuadas con equipos ups o supresores de pico que eviten el daño físico y lógico de los equipos en donde se resguarda la información, así como de contar con un acceso restringido a estas áreas.

V.- Análisis de brecha.

Se debe hacer un análisis de las medidas de seguridad existentes contra las faltantes, considerando las mejores prácticas.

Nombre del sistema: Sistema de Administración Escolar (SAES)

Medidas de seguridad existentes

Administrativas:

1. Hacer de conocimiento de los servidores públicos a los que se autoriza usuario y contraseña la responsabilidad del resguardo, uso y manejo de los datos personales.
2. Identificación del ciclo de vida de los datos personales.
3. Capacitación para el personal en materia de protección de datos personales, de acuerdo con sus roles y responsabilidades.
4. Notificaciones de requerimientos a los directores de las unidades académicas y áreas administrativas que tienen acceso al SAES, para reiterarles la importancia de notificar los cambios de personas analistas que tratan datos personales, a efecto de salvaguardar la confidencialidad, integridad y disponibilidad de los datos personales.
5. No se otorgan accesos al Sistema a quien no cuente con un nombramiento y las funciones del cargo correspondan a control y gestión escolar.
6.

Físicas:

1. Seguridad perimetral exterior, se tiene contratada a la Policía Auxiliar de la Ciudad de México, quien comisiona a dos oficiales para resguardar la entrada principal de las instalaciones de la DAE, donde informen el motivo de la visita.
2. Seguridad interior, una persona controla el acceso a las oficinas de la DAE, previo registro e identificación.
3. Bitácora donde se lleva el registro del personal que ingresa al área donde se encuentra el sistema de computo que contiene la base de datos con los datos personales de los alumnos.
4. Acceso solo de personal debidamente identificado y autorizado al área donde se localiza la base de datos.

Técnicas:

1. Bitácoras para acceso y operación cotidiana.
2. Control de acceso a la base de datos solo por personal debidamente identificado y autorizado con clave y contraseña.
3. Establecimiento de privilegios a los responsables y usuarios de acuerdo con las actividades a realizar y en términos de sus funciones.
4. Programa de mantenimiento preventivo de los equipos que contiene la base de datos personales.

5. Procedimiento de respaldo de la base que contiene los datos personales.
6. Monitoreo de las conexiones a la base de datos.
7. Administración y monitoreo de bitácoras de bases de datos.
8. Buenas prácticas en el desarrollo de procedimientos almacenados y patrones de desarrollo de software.

Medidas de seguridad faltantes

Administrativas:

1.- Intensificación de la campaña de capacitación para el personal de las unidades académicas, enfocada en la concientización de la responsabilidad del uso y manejo de la información almacenada en el sistema, así como del usuario y contraseña.

2.- Seguimiento a las bajas y altas de usuarios que ya no se encuentran en los roles registrados en las bases de datos, con la finalidad de no hacer mal uso de la información almacenada en el sistema. En el momento en el que exista rotación de personal es necesario notificar de manera oficial dicho cambio.

3.- Apegarse a los procedimientos establecidos para las conexiones seguras en el área de trabajo.

4.- Capacitación constante en el manejo de equipos de cómputo.

5.- Capacitación constante en el uso del sistema.

Físicas:

1.- Contar con el espacio físico adecuado, para el resguardo del equipo servidor, instalación eléctrica, aire acondicionado, supresores de picos, limpieza del área.

Técnicas:

1.- Actualización de equipo de cómputo de cada usuario que cuente con una clave de acceso al sistema (sistema operativo, antivirus).

2.- Uso de software que cuente con licencia avalada por el Instituto.

3.- Evitar habilitar conexiones remotas a los equipos que tienen instalado el sistema.

4.- Descarga de archivos de dudosa procedencia.

La existencia de nuevas medidas de seguridad que pudieran reemplazar uno o más controles implementados actualmente o que se desee implementar para mayor protección de los activos involucrados en los datos personales.

Registro de Incidentes: Se llevará un control en la Dirección de Administración Escolar que consigne la información de incidentes tales como la pérdida o alteración no autorizada de expedientes electrónicos, así como para la recuperación de los datos.

Procedimiento de respaldo y recuperación de datos:

Se cuenta con un procedimiento a través del cual los respaldos que se realizan en las bases de datos del Sistema de Administración Escolar son de dos tipos:

Diferenciales: Estos respaldos se hacen cuando existen un cambio en la información que se tiene en la base de datos referente a la trayectoria escolar de los alumnos, no se realiza el respaldo de toda la información, sólo se hace una comparativa y cuando existe una diferencia, se realiza el respaldo, primero en el servidor de manera local y posteriormente es trasladado a otro servidor que actúa como concentrador de toda la información.

Totales: Estos respaldos se realizan con la finalidad de salvaguardar toda la información generada de la trayectoria escolar de los alumnos, previendo que si en algún punto se pierde la conexión en la transferencia de la información, ya sea por falta de red o fallas en la energía eléctrica, el respaldo de información sirva para restaurar el propio sistema evitando perdida de datos. Dichos respaldos se llevan a cabo de manera mensual y semestral, se guarda la información en el servidor local y posteriormente es trasladado a otro servidor que actúa como concentrador de toda la información.

Los respaldos después de haber sido transferidos al servidor denominado como concentrador, se almacenan en cintas magnéticas, con la finalidad de que si en algún momento el equipo concentrador cuenta con alguna falla, la información no se pierda y pueda ser recuperada y transferida en la base de datos que así se requiera.

El responsable de realizar estas actividades es el personal del Departamento de Registro y Supervisión Escolar, perteneciente a la Dirección de Administración Escolar (DAE).

VI.- Plan de trabajo.

La DAE definirá las acciones de conformidad con los recursos disponibles y con la participación de las unidades politécnicas competentes, para que, de acuerdo con el análisis de riesgo y análisis de brecha, se implementen las medidas de seguridad nuevas o faltantes más relevantes e inmediatas, indicando las fechas de su implementación. Esta evaluación se realizará de manera anual.

VII.- Mecanismo de monitoreo y revisión de las medidas de seguridad

La DAE evalúa y mide los resultados de sus políticas, planes, procesos y procedimientos implementados en materia de seguridad de datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua, en términos de lo dispuesto en el artículo 63 de los Lineamientos Generales de Protección de Datos personales para el Sector Público, considerando lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;
II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
VII. Los incidentes y vulneraciones de seguridad ocurridas.

VIII.- Programa General de Capacitación.

La Dirección de Administración Escolar realizará la capacitación que se proporcione en materia de protección de datos personales a través de la Unidad de Transparencia, respecto del personal de esa área, y apoyará a promoverlos con los responsables y analistas de las unidades académicas y dependencias administrativas que hagan uso del Sistema de Administración Escolar.

Aprobación del Documento de Seguridad

Revisó
Ing. Josué David Pazarán Balderas
Jefe del Departamento de Registro y Supervisión Escolar

SECRETARÍA DE EDUCACIÓN PÚBLICA
INSTITUTO POLITÉCNICO NACIONAL
DIRECCIÓN DE ADMINISTRACIÓN ESCOLAR

Autorizó
Lic. Fabiola Guadalupe Rodríguez Jiménez
Directora de Administración Escolar

Fecha
16 de junio de 2021