Contenido

1. PRESENTACIÓN

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO o Ley General) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura la Universidad Autónoma Agraria Antonio Narro (UAAAN).

De ahí que el presente Documento de Seguridad en cumplimiento a lo previsto en los artículos 35 y 36 de la LGPDPPSO, establece el marco de referencia para tratamiento de los datos personales que se llevan a cabo al interior de la UAAAN.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de la UAAAN, pues tal y como lo dispone el artículo 34 de la LGPDPPSO, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

Así, la UAAAN comprometida con la tutela de los datos personales que trata y, acorde a la recomendación emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendientes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos.

Dicho lo anterior, el presente documento se integra a partir de la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para la UAAAN la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LGPDPPSO.

2. OBJETIVO

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que operan en la UAAAN para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diversos sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LGPDPPSO y a los Lineamientos Generales de Protección de Datos Personales.

3. ALCANCE

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte de las diferentes entidades que conforman la estructura universitaria en los que de acuerdo con su ámbito de funciones llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad, tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan dichos datos personales.

En este sentido, la Rectoría integra el presente documento de seguridad con base en la información generada por las diferentes entidades administrativas y académicas acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

4. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES EN POSESIÓN DE LA UAAAN

Para el tratamiento de los datos personales que lleva a cabo la UAAAN a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismo, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley General de Transparencia y Acceso a la Información Pública.

La UAAAN mediante la identificación de procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas entidades que conforman la institución, se involucra el tratamiento de datos personales, se lleva a cabo el levantamiento del **inventario de datos,** con el propósito de identificar, entre otros aspectos, la categoría y tipo datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos.

De igual forma, una vez integrados los inventarios de datos, se dispone~~uso~~ de la metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV de la Ley General de la materia, las áreas responsables de su tratamiento identifican~~ron~~ el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y, los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad ***administrativas,*** entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; ***físicas***, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, ***técnicas*** que se valen de la tecnología para proteger el entorno digital de la información.

Considerando que la identificación de vulnerabilidades **tiene** por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan como posibles vulnerabilidades, las siguientes:

1. Controles de acceso físico y electrónicos inadecuados a sistemas de archivos.
2. Deficiente conocimiento de procedimientos en materia de seguridad de datos.
3. Inadecuada administración de autorizaciones de accesos a los datos personales

4. Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.

5. Falta de seguimiento y monitoreo a políticas de seguridad.

6. Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

TIPOS DE AMENAZAS

 Robo, extravío o copia no autorizada.

 Uso, acceso o tratamiento no autorizado.

 Daño, alteración o modificación no autorizado.

 Pérdida o destrucción no autorizada.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional, se enmarcan las reglas generales siguientes:

a). Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General;

b). Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;

c). Informar a los titulares del tratamiento de los datos y sus finalidades;

d). Procurar que los datos personales tratados sean correctos y estén actualizados;

e). Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;

f). Tratar los datos personales estrictamente para propósitos legales o legítimos de la UAAAN;

g). Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;

h). No obtener datos personales a través de medios fraudulentos;

i). Respetar la expectativa razonable de privacidad del titular;

j). Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;

k). Velar por el cumplimiento de los principios;

l). Establecer y mantener medidas de seguridad;

m). Guardar la confidencialidad de los datos personales;

n). Identificar el flujo y ciclo de vida de los datos personales;

o). Mantener actualizado el inventario de datos personales o de las categorías que maneja la UAAAN;

p). Respetar los derechos de los titulares en relación con sus datos personales;

q). Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y;

r). Identificar a los servidores públicos de la UAAAN responsables del tratamiento de los datos personales.

Con base en lo anterior, la UAAAN determina las pautas de acción del personal encargado del tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPPSO y los Lineamientos de la materia, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

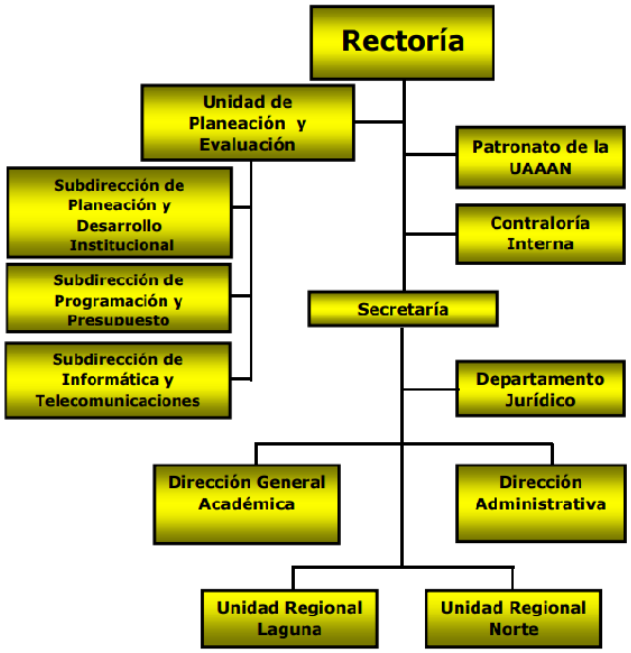
5. *INVENTARIO DE DATOS PERSONALES DE LA UAAAN*

Para cumplir con los objetivos y obligaciones que prevé la *LGPDPPSO*, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales de la UAAAN, se realizó una actualización dentro de las entidades que conforman su estructura orgánica, para identificar los procesos en los que actualmente se lleva a cabo el tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales de la UAAAN.

Por inventario de tratamiento de datos, se entiende el *control documentado* del conjunto de operaciones que realizan las áreas que integran la UAAAN con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de éstos derechos en el ámbito de sus atribuciones.

En tal virtud, en coordinación con las áreas y derivado del proceso de actualización de información, las Direcciones y Coordinaciones mismas que se encuentran integradas a su vez por jefaturas y áreas, llevan a cabo el tratamiento de datos personales.

ESTRUCTURA CENTRAL DE LA UAAAN



Como resultado de dicha actualización, se encontró que en las entidades administrativas o académicas en la que se tratan datos, a través de sus departamentos y/o áreas que las conforman, dicho tratamiento atiende a las operaciones o procesos que realizan con motivo del ejercicio de sus facultades.

En este sentido, fue posible identificar los procesos y tipos de dato que involucran, los cuales se describen a continuación:

DIRECCION	DEPARTAMENTO/AREA	FUNCION	TIPO DE DATO
DIRECCION ADMINISTRATIVA			
	Recursos Humanos		
		Registro y Actualización de Información de Empleados	1,3
		Proceso de Nomina	1,2
		Seguros de Gastos Médicos	1,2
		IMSS	1,2
		Prestaciones	
	Contabilidad		
		Anticipos/pagos	,1
		Comprobaciones	,1
	Servicios Asistenciales		
		Comedor	1,2,3
		Internado	1,2,3
DIRECCION DOCENCIA			
	Control Escolar		
		Registro y Actualización de Alumnos Licenciatura y Posgrado	1,2,3
		Registro y Actualización de Kardex Académico de Licenciatura y Posgrado	1,2,3
		Elaboración de Documentos de Egreso	,1
		Becas	1,2
		Deportes	,1
		Tutorías	,1
DIRECCION DE COMUNICACIÓN			
	Servicio Social		
		Actualización Elaboración , Registro de Documentos de Servicio Social Licenciatura	,1

	Difusión Cultura		
		Registro de Alumnos Grupos Artísticos	,1
DIRECCION DE INVESTIGACION			
	Subdirección de Proyectos		
		Registro de Proyectos de Investigación	,1
		Registro de Articulos	,1
		Sistema Nacional de Investigadores	,1

Donde Tipo de Dato= 1**.- Identificación**. Nombre, domicilio, C.U.R.P., fotografía, huella digital, firma, edad, clave de elector, estado civil, R.F.C., correo electrónico personal, teléfono, sexo, información académica, fecha y lugar de nacimiento, cédula profesional, nacionalidad, número de pasaporte, número de licencia de conducir, número de placa de vehículo, número de seguridad social; **2.- Patrimoniales.** - Cuentas bancarias, estados de cuentas bancarias, número de tarjeta bancaria, CLABE interbancaria, Institución bancaria, facturas, estados financieros, información fiscal, información fiduciaria, información financiera, saldos, propiedades, pensión alimenticia, descuentos por concepto de primas de seguro; **3.- Sensibles.** - Diagnóstico médico, antecedentes médicos, tipo de sangre, datos biométricos, antecedentes penales y resultados de evaluación psicométrica y de valores.

A partir de lo anterior, el Inventario de Datos Personales de la UAAAN se permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos, y con ello, enfocar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

6. ANALISIS DE RIESGO/BRECHA

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por la UAAAN al ejercer sus atribuciones.

La LGPDPPSO en sus artículos 32, fracción I, y 33, fracción IV, considera que el determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que se deben identificar las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Con base en la LGPDPPSO, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por la UAAAN, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

Aunado a lo anterior, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, emitidos por Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), indican en su artículo 60 que el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.
- El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
- Las consecuencias negativas para los titulares de los datos personales, que puedan derivar en una vulneración de seguridad.
- El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para los titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

Elementos para el análisis de riesgos

La seguridad de los datos personales que se tratan en la UAAAN demanda conocer y entender los riesgos a los que se encuentran expuestos en los distintos procesos que realizan las unidades administrativas y académicas, lo que permitiría afrontarlos de manera adecuada y oportuna.

Para analizar los riegos de los datos personales que son objeto de tratamiento por la UAAN, se debe elaborar un instrumento que clasifique los datos en tres tipos, tal y como ha sido referenciado con antelación.

1) De **identificación o contacto**, que se refieren a información por la que se identifica a una persona y/o permiten su contacto, como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.

2) **Patrimoniales**, que comprenden la información que se encuentran vinculados al patrimonio de una persona, como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

3) **Sensibles**, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste, como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Para la determinación del riesgo sobre esa tipología de datos personales se debe valorar la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con una diversidad de activos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza). Para facilitar el análisis, se identifican cuatro tipos de amenazas:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

7. MEDIDAS DE SEGURIDAD GENERALES

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta la UAAAN para mantener la confidencialidad e integralidad de la información, son las siguientes:

a) Medidas administrativas.

1. Implementación de un esquema de capacitación permanente en materia de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados (LGPDPPSO).
2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes personales y/o académicos.
4. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
5. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

b) Medidas físicas.

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.
6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.
7. Resguardo de llaves en oficinas de acceso restringido.

c) Medidas técnicas.

1. Utilizar claves de usuario y contraseñas por nivel de jerarquía funcional (Superusuario, Administrador, controlistas, Personal Administrativo, Personal Académico) de manera personal, y evitar compartirlas, prestarlas o registrarlas~~das~~ a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata a la Subdirección de Informática los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.

4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

Adicionalmente, como parte de la política de seguridad técnica, la Subdirección de Informática y Telecomunicaciones implementa los siguientes controles:

1. Definición de políticas de contraseñas.

2. Asignación de privilegios de acuerdo a roles y funciones.

3. Tareas de respaldo por servidor y por agente.

4. Operación *Hardening* en los servidores de Información en alta disponibilidad con contraseña de directorio de datos y acceso restringido.

5. Tareas de respaldo por servidor y de las instancias de base de datos del servicio.
6. Acceso a los sistemas conforme a procedimiento de administración de usuarios y contraseñas con cuenta local con permiso del administrador.
7. Borrado seguro de la información que reside en los equipos de cómputo.
8. Des habilitación de cuentas de personal que causa baja.
9. Acceso controlado de administración y accesos privilegiados.
10. Definición de procedimientos y controles de seguridad de la información.

8. PROPUESTA PARA CAPACITACON EN MATERIA DE DATOS PERSONALES

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad y a Ley, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el aprovechamiento de los recursos y herramientas que el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha dispuesto para su uso y obtención de beneficios, se propone que a través de la Unidad de Transparencia Institucional se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.

Así, entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

I) Introducción al derecho a la protección de datos personales.

- Principios.
- Deberes.
- Sistemas de datos personales.
- Medidas de seguridad.
- Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición).
- Medios de defensa.

II) La LGPDPPSO y sus Lineamientos.

- Antecedentes.
- ¿A quién aplica?
- ¿Qué objeto tiene?

III) Fundamentos conceptuales de la LGPDPSO.

- Inventario y Base de Datos.
- Medidas de seguridad.
- Análisis de brecha y de riesgo.
- Funciones y obligaciones.

IV) Relevancia de los Avisos de Privacidad.

- Consentimiento.
- Deber de información.
- Finalidades del tratamiento de los datos

9. FUNCIONES Y RESPONSABILIDADES DEL TRATAMIENTO DE DATOS PERSONALES

A raíz de los procesos determinados en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas que realizan tratamiento de éstos dentro de la UAAAN, resultó necesario asociar dichas actividades con las facultades que el Manual General de organización (MGO) otorga a los servidores públicos responsables de dicho tratamiento, a efecto de generar certeza y dar cumplimiento al principio de legalidad que debe atender cada entidad.

En tal virtud, a continuación, se precisan las funciones otorgadas por el MGO a las entidades administrativas y académicas que conforman la estructura orgánica de este ente de Fiscalización Superior:

DIRECCION	DEPARTAMENTO/AREA	Funciones relacionadas con el tratamiento de datos	OBLIGACIONES
DIRECCION ADMINISTRATIVA			
	Recursos Humanos		
		Registro y Actualización de Información de Empleados	
		Proceso de Nomina	
		Seguros de Gastos Médicos	
		IMSS	
		Prestaciones	
	Contabilidad		
		Anticipos/pagos	
		Comprobaciones	
	Servicios Asistenciales		
		Comedor	
		Internado	
DIRECCION DOCENCIA			
	Control Escolar		
		Registro y Actualización de Alumnos Licenciatura y Posgrado	
		Registro y Actualización de Kardex Académicos Licenciatura y Posgrado	
		Elaboración de Documentos de Egreso	
		Becas	
		Deportes	
		Tutorías	

DIRECCION DE COMUNICACIÓN			
	Servicio Social		
		Actualización Elaboración ,Registro de Documentos de Servicio Social Licenciatura	
	Difusión Cultural		
		Registro de Alumnos Grupos Artísticos	
DIRECCION DE INVESTIGACION			
	Subdirección de Proyectos		
		Registro de Proyectos de Investigación	
		Registro de Articulos	
		Sistema Nacional de Investigadores	