



Instituto

Mora

**Documento de seguridad  
del Instituto de Investigaciones  
Dr. José María Luis Mora**





**Documento de seguridad  
del Instituto de Investigaciones  
Dr. José María Luis Mora**

**ÍNDICE**

	<b><i>Pág.</i></b>
<b>PARTE 1. CATÁLOGO DE SISTEMAS DE DATOS PERSONALES</b>	1
<b>A.</b> Dirección de Investigación	1
<b>B.</b> Dirección de Docencia	7
<b>C.</b> Dirección de Vinculación	22
<b>D.</b> Dirección de Administración y Finanzas	29
<b>PARTE 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES</b>	44
<b>A.</b> Dirección de Investigación	44
<b>B.</b> Dirección de Docencia	45
<b>C.</b> Dirección de Vinculación	47
<b>D.</b> Dirección de Administración y Finanzas	47
<b>PARTE 3. MEDIDAS DE SEGURIDAD</b>	49
<b>I.</b> Funciones y obligaciones del personal	49
<b>II.</b> Políticas de seguridad	49
<b>III.</b> Acceso a las instalaciones	52
<b>IV.</b> Accesos controlados y bitácoras	52
<b>V.</b> Gestión de soportes	52
<b>VI.</b> Perfiles de usuario y contraseñas	56
<b>VII.</b> Transmisión de datos personales	57
<b>VIII.</b> Plan de contingencia	58
<b>PARTE 4. PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS</b>	58
<b>PARTE 5. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE DATOS PERSONALES</b>	60
<b>PARTE 6. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD</b>	61
<b>PARTE 7. ANEXOS TÉCNICOS</b>	61

## PARTE 1. CATÁLOGO DE SISTEMAS DE DATOS PERSONALES

### A. Dirección de Investigación

#### A1. Sistema de Información Académica del Mora (SIAM)

**Nivel de seguridad:** Medio

**Responsable:**

Nombre: Dr. Francisco Javier Porras Sánchez.

- Cargo: Titular de la Dirección de Investigación.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Investigación tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Información Académica del Mora (SIAM).

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Información Académica del Mora (SIAM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Lorena Montoya Martínez.

- Cargo: Asistente de la Dirección de Investigación.

- Funciones:

-Mantener actualizados los datos personales de los profesores-investigadores, realizar cambios dentro del sistema desde el módulo Administración del Sistema.

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Integrar datos al catálogo de sistema.

• Obligaciones:

-Salvaguardar la información del sistema,

-Confidencialidad de los reportes generados del SIAM.

-Apoyar a los profesores-investigadores con las dudas suscitadas acerca de la integración de información al sistema.

### **Usuario:**

Nombre: Agustín Herrera Berthely.

• Cargo: Asistente de la Dirección de Investigación.

• Funciones:

-Realización de diversos informes, con la información contenida en el sistema.

• Obligaciones:

-Salvaguardar la información consultada.

-Confidencialidad de los reportes generados del SIAM.

Nota: Los profesores-investigadores adscritos al Instituto tienen acceso a su cuenta en el SIAM por medio de una clave para ingresar su productividad trimestralmente.

**Folio del registro en el Sistema Persona: 11280000100001**

### **Datos personales contenidos en el sistema:**

#### Datos de identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico
- Estado Civil
- Firma
- RFC
- CURP
- Lugar de nacimiento
- Fecha de nacimiento
- Nacionalidad

#### Datos académicos

- Trayectoria educativa
- Títulos
- Reconocimientos

#### Datos laborales

- Actividades extracurriculares
- Trabajo actual
- Documentos de nombramiento
- Documentos de capacitación
- Puesto
- Domicilio de trabajo
- Correo electrónico institucional

#### Tránsito y movimientos migratorios

- Información migratoria de las personas

## **A2. Sistema de Información Académica del Mora (SIAM), Módulo Dictámenes Categorías, Promoción y Estímulos Académicos**

**Nivel de seguridad:** Medio

#### **Responsable:**

Nombre: Dr. Francisco Javier Porras Sánchez.

- Cargo: Titular de la Dirección de Investigación.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Investigación tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Información Académica del Mora (SIAM) Módulo Dictámenes (Categorías, Promoción y Estímulos Académicos).

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Información Académica del Mora (SIAM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado,

salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;  
-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado y usuario:**

Nombre: Lorena Montoya Martínez.

- Cargo: Asistente de la Dirección de Investigación.
- Funciones:

-Mantener actualizados los datos personales de los profesores-investigadores, realizar cambios dentro del sistema desde el módulo Administración del Sistema.

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Integrar datos al catálogo de sistema.

- Obligaciones:

-Salvaguardar la información del sistema,

-Confidencialidad de los reportes generados del SIAM.

-Apoyar a los profesores-investigadores con las dudas suscitadas acerca de la integración de información al sistema.

**Folio del registro en el Sistema Persona: 11280000100004**

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico
- Estado Civil
- Firma
- RFC
- CURP
- Lugar de nacimiento
- Fecha de nacimiento
- Nacionalidad
- Edad

**A3. Sistema de Librería**

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Dr. Francisco Javier Porras Sánchez.

- Cargo: Titular de la Dirección de Investigación.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de

Investigación tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Librería.

- **Funciones:**

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Librería, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:**

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargados:**

Nombre: Raúl Zepeda Baltazar.

- **Cargo:** Responsable del Área de Distribución de Publicaciones.

- **Funciones:** Adoptar los procedimientos adecuados para atender las solicitudes de acceso y corrección de datos del Sistema de Librería, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:**

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Arturo Hazael López González.

- Cargo: Técnico auxiliar “C”.
- Funciones: Adoptar los procedimientos adecuados para atender las solicitudes de acceso y corrección de datos del Sistema de Librería, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Obligaciones:
  - Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
  - Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
  - No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

#### **Usuarios:**

Nombre: Antonio García García

- Cargo: Responsable del Almacén de Publicaciones.
- Funciones: De acuerdo a lo establecido en el Manual General de Organización del Instituto, son: la ejecución y control de almacenamiento y el registro de las entradas y salidas de las publicaciones del Instituto en el sistema de la Librería Virtual.
- Obligaciones:
  - Procurar que los datos personales sean exactos y actualizados;
  - Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
  - Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
  - No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Arturo Hazael López González.

- Cargo: Técnico auxiliar “C”.
- Funciones:
  - Adoptar los procedimientos adecuados para atender las solicitudes de acceso y corrección de datos del Sistema de Librería, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones: -Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona:** 11280000100002

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico
- RFC

**B. Dirección de Docencia**

**B1. Base de datos de usuarios de la Biblioteca Ernesto de la Torre Villar**

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Marisa Pérez Domínguez.

- Cargo: Titular de la Dirección de Docencia.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Subdirección de Biblioteca tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de datos personales de los usuarios de la Biblioteca Ernesto de la Torre Villar.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre políticas en relación con la protección de datos personales de los usuarios de la Biblioteca, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas por el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esa situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargados:**

Nombre: Carlos Gabino Arellano Osorio.

- Cargo: Subdirector de biblioteca.
- Funciones: Coordinar la operación y funcionamiento del Sistema de Automatización de Bibliotecas *Aleph 500* repositorio de la base de datos de usuarios de la biblioteca
- Obligaciones: Mantener y controlar la base de datos de usuarios de la Biblioteca.

Nombre: Germán Eloy Mejía Estrada.

- Cargo: Jefe del Departamento de Servicios al Público.
- Funciones: Controlar y supervisar el funcionamiento del Sistema de Automatización de Bibliotecas *Aleph 500*.
- Obligaciones: Mantener y controlar la base de datos de usuarios de la Biblioteca.

Nombre: José Martín Ascencio Camacho.

- Cargo: Coordinador de biblioteca.
- Funciones: Administrar el Sistema de Automatización de Bibliotecas *Aleph 500*
- Obligaciones: Mantener y controlar la base de datos de usuarios de la Biblioteca.

**Usuarios:**

Nombre: Miguel Ángel Jurado Ayala.

- Cargo: Coordinador de biblioteca.
- Funciones: Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas *Aleph 500* e identifica al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Irma Osorio Cisneros.

- Cargo: Secretaria ejecutiva bilingüe.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Pedro Esquivel Hernández.

- Cargo: Responsable de sistemas de cómputo.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Fernando Alvarado Montaña.

- Cargo: Técnico administrativo especializado.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Roberto Olivos Sánchez.

- Cargo: Coordinador de biblioteca.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Daniel Eduardo Fernández Reséndiz.

- Cargo: Técnico bibliotecario especializado.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Araceli Medina Chávez.

- Cargo: Responsable de sistemas de cómputo.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.

- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

Nombre: Sandra Magdalena Ramírez Vilchis.

- Cargo: Personal Eventual.
- Funciones Ingresar al Módulo de Circulación del Sistema Automatizado de Bibliotecas Aleph 500 e identificar al usuario a través del registro creado en el propio sistema.
- Obligaciones: Operar de manera eficiente el Módulo de Circulación para brindar los servicios que ofrece la biblioteca.

**Folio del registro en el Sistema Persona:** Pendiente de registro.

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico

**B2. Sistema de Seguimiento de Egresados del Mora (SISEM)**

**Nivel de seguridad:** Medio

**Responsable:**

Nombre: Marisa Pérez Domínguez.

- Cargo: Titular de la Dirección de Docencia.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Docencia tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM).

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Lorena Navarro Sandoval.

- Cargo: Titular del Departamento de Servicios Escolares.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Usuarios:**

Nombre: Lucy Araceli Tirso Álvarez.

- Cargo: Asistente del Departamento de Servicios Escolares.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de

Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Aurea Graciela Castellanos Becerra.

- Cargo: Asistente del departamento de Servicios Escolares.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado,

salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;  
-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Martha Beatriz Rodríguez Pacheco.

- Cargo: Secretaria del Departamento de Servicios Escolares.

- Funciones:

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Procurar que los datos personales sean exactos y actualizados;

- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona: 11280000300001**

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico
- Estado Civil
- RFC
- Lugar de nacimiento
- Fecha de nacimiento

- Nacionalidad

#### Datos Académicos

- Trayectoria educativa
- Reconocimientos

#### Datos Laborales

- Puesto
- Domicilio de trabajo
- Correo electrónico institucional
- Referencias laborales
- Trabajo actual
- Trabajos anteriores
- Teléfono institucional

### B3. Expedientes de alumnos

**Nivel de seguridad:** Alto

**Responsable:**

Nombre: Marisa Pérez Domínguez.

- Cargo: Titular de la Dirección de Docencia.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Docencia tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales de los Expedientes de alumnos.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado,

salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;  
-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Lorena Navarro Sandoval.

- Cargo: Titular del Departamento de Servicios Escolares.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;  
-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;  
-Procurar que los datos personales sean exactos y actualizados;  
-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;  
-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;  
-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Usuarios:**

Nombre: Lucy Araceli Tirso Álvarez.

- Cargo: Asistente del Departamento de Servicios Escolares.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Aurea Graciela Castellanos Becerra.

- Cargo: Asistente del departamento de Servicios Escolares.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Martha Beatriz Rodríguez Pacheco.

- Cargo: Secretaria del Departamento de Servicios Escolares.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona:** Pendiente de registro.

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Comprobante de Domicilio
- Teléfono particular
- Correo electrónico
- Sexo
- Estado Civil
- Correo electrónico
- RFC
- CURP
- Acta de nacimiento
- Credencial de elector
- Certificado médico

#### Datos Académicos

- Trayectoria educativa
- Título
- Certificado de estudios
- Carta promedio
- Reconocimientos (Cargos, premios y distinciones)
- Calificaciones parciales del Programa
- Cartas de presentación
- Solicitudes de beca
- Cartas de recomendación académicas
- Proyecto de investigación
- Currículum vitae
- Constancias de calificaciones
- Viáticos

#### **B4. Sistema de Evaluación del Desempeño Académico (SEDA)**

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Marisa Pérez Domínguez.

- Cargo: Titular de la Dirección de Docencia.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Docencia tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Evaluación del Desempeño Académico (SEDA).

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Lorena Navarro Sandoval.

- Cargo: Titular del Departamento de Servicios Escolares.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Usuarios:**

Nombre: Lucy Araceli Tirso Álvarez.

- Cargo: Asistente del Departamento de Servicios Escolares.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes

previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Aurea Graciela Castellanos Becerra.

- Cargo: Asistente del departamento de Servicios Escolares.

- Funciones:

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombre: Martha Beatriz Rodríguez Pacheco.

- Cargo: Secretaria del Departamento de Servicios Escolares.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

Nombres:

Dra. Ana María Serna Rodríguez,

Dra. Enriqueta María Quiroz Muñoz,

Mtra. María Eugenia Chapul Pereyra,

Dr. Alejandro Monsiváis Carrillo,

Dr. Aaron Joel Pollack,

- Cargo: Coordinadores Académicos de los programas de Docencia.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Seguimiento de Egresados del Mora (SISEM), de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:**

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona:** Pendiente de registro

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Estado Civil
- Grado Académico
- Sexo
- Fecha de nacimiento
- CURP
- RFC
- País de nacimiento
- País de naturalización
- Domicilio
- Correo electrónico
- Teléfono

**C. Dirección de Vinculación**

**C1. Directorio del Mora**

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Benjamín Antonio Juárez Echenique.

- Cargo: Titular de la Dirección de Vinculación.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de

Vinculación tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Directorio del Mora.

- **Funciones:**

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Directorio del Mora, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:**

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Procurar que los datos personales sean exactos y actualizados;

- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Mónica Rodríguez Sánchez.

- **Cargo:** Titular del Departamento de Difusión.

- Funciones: Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Directorio del Mora, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:** Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

**Usuario:**

Nombre: Raymundo Zendejas Rioja.

- Cargo: Asistente del departamento de difusión.  
Funciones: Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Directorio del Mora, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Obligaciones: Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
  - Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
  - Procurar que los datos personales sean exactos y actualizados;
  - Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
  - Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
  - No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona:** 11280040000001

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico

Datos Laborales

- Puesto
- Domicilio de trabajo
- Trabajo actual
- Teléfono institucional

## C2. Registro de Invitados

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Benjamín Antonio Juárez Echenique.

- Cargo: Titular de la Dirección de Vinculación.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Vinculación tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Registro de Invitados.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Registro de Invitados, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Mónica Rodríguez Sánchez.

- Cargo: Titular del Departamento de Difusión.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Registro de Invitados, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Usuario:**

Nombre: Raymundo Zendejas Rioja.

- Cargo: Asistente del Departamento de Difusión.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Registro de Invitados, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
  - Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona:** 11280040000003

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Domicilio
- Teléfono particular
- Correo electrónico

Datos Laborales

- Puesto
- Domicilio de trabajo
- Trabajo actual
- Teléfono institucional

**C3. Sistema de registro de correos electrónicos**

**Nivel de seguridad:** Básico

**Responsable:**

- Nombre: Benjamín Antonio Juárez Echenique.
- Cargo: Titular de la Dirección de Vinculación.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Vinculación tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de registro de correos electrónicos.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de registro de correos electrónicos, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

- Nombre: Mónica Rodríguez Sánchez.
- Cargo: Titular del Departamento de Difusión.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de registro de correos electrónicos, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Usuario:**

Nombre: Raymundo Zendejas Rioja.

- Cargo: Asistente del Departamento de Difusión.
- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de registro de correos electrónicos, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el

Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Folio del registro en el Sistema Persona:** 11280040000004

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Correo electrónico

**D. Dirección de Administración y Finanzas**

**D1. Kardex**

**Nivel de seguridad:** Medio

**Responsable:**

Nombre: Eunice Maldonado Sánchez.

- Cargo: Titular de la Dirección de Administración y Finanzas.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Kardex.

- Funciones:

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Kardex, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:**

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Juan Carlos Luna Mendoza.

- Cargo: Titular del Departamento de Recursos Humanos.

- **Funciones:**

- Validar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.
- Verificar que se lleve a cabo el registro de los servidores públicos, que previamente se les hace entrega de información física y electrónica (KARDEX) del Sistema de Datos Personales.
- Constatar que se actualice trimestralmente la relación de los servidores públicos a los que se les hace entrega de información física y (KARDEX) del Sistema de Datos Personales.
- Recibir y validar las entregas parciales o totales de información física y electrónica (KARDEX) del Sistema de Datos Personales.
- Recibir los informes de los incidentes que ocurran sobre datos personales y constatar que se lleve a cabo un registro de los mismos.

- **Obligaciones:**

- Validar los mecanismos que permitan asegurar que los datos personales en posición de la unidad administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.
- Verificar que se garantice la seguridad de los datos personales y evitar la alteración, pérdida transmisión y acceso no autorizado.

**Usuarios:**

Nombre: Alfredo Martínez Pérez

- Cargo: Ejecutivo de Proyectos Técnicos
- Funciones:

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.
- Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (KARDEX) del Sistema de Datos Personales.
- Actualizar trimestralmente la relación de los servidores públicos a los que se les hace entrega de información física y electrónica (KARDEX) del Sistema de Datos Personales.
- Informar al encargado sobre entregas parciales o totales de información física y electrónica (KARDEX) del Sistema de Datos Personales.
- Informar al encargado del Sistema de Datos Personales sobre los incidentes que ocurran y llevar un registro.
  - Obligaciones:
    - Proponer mecanismos para asegurar que los datos personales en posición de la unidad administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.
    - Garantizar la seguridad de los datos personales y evitar la alteración, pérdida transmisión y acceso no autorizado.

Nombre: Rodolfo Ramírez Martínez

- Cargo: Jefe de Servicios Especializados
- Funciones:
  - Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.
  - Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (KARDEX) del Sistema de Datos Personales.
  - Actualizar trimestralmente la relación de los servidores públicos a los que se les hace entrega de información física y electrónica (KARDEX) del Sistema de Datos Personales.
  - Informar al encargado sobre entregas parciales o totales de información física y electrónica (KARDEX) del Sistema de Datos Personales.
  - Informar al encargado del Sistema de Datos Personales sobre los incidentes que ocurran y llevar un registro.
    - Obligaciones:
      - Proponer mecanismos para asegurar que los datos personales en posición de la unidad administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.
      - Garantizar la seguridad de los datos personales y evitar la alteración, pérdida transmisión y acceso no autorizado.

**Folio del registro en el Sistema Persona: 11280050000002**

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre

- Domicilio
- Teléfono particular
- Firma
- RFC
- CURP
- Fecha de nacimiento
- Edad

Datos Laborales

- Puesto

Datos Patrimoniales

- Ingresos y egresos
- Otros

**D2. Sistema de Recursos Humanos (SIRH)**

**Nivel de seguridad:** Medio

**Responsable:**

Nombre: Eunice Maldonado Sánchez.

- Cargo: Titular de la Dirección de Administración y Finanzas.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Recursos Humanos (SIRH).

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del SIRH, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado,

salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;  
-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Juan Carlos Luna Mendoza.

- Cargo: Titular del departamento de Recursos Humanos.

- Funciones:

-Validar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

-Verificar que se lleve a cabo el registro de los servidores públicos, que previamente se les hace entrega de información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

-Recibir y validar las entregas parciales o totales de información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

-Recibir los informes de los incidentes que ocurran sobre datos personales y constatar que se lleve a cabo un registro de los mismos.

- Obligaciones:

-Validar los mecanismos que permitan asegurar que los datos personales en posición de la unidad administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.

-Verificar que se garantice la seguridad de los datos personales y evitar la alteración, pérdida transmisión y acceso no autorizado.

**Usuarios:**

Nombre: Alfredo Martínez Pérez.

- Cargo: Ejecutivo de Proyectos Técnicos.

- Funciones:

-Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

-Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

-Informar al responsable sobre entregas parciales o totales de información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

-Informar al responsable del Sistema de Datos Personales sobre los incidentes que ocurran y llevar un registro.

- Obligaciones:

-Proponer mecanismos para asegurar que los datos personales en posición de la unidad administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.

-Garantizar la seguridad de los datos personales y evitar la alteración, pérdida transmisión y acceso no autorizado.

Nombre: Claudia Leticia Páez Ruiz.

- Cargo: Jefe de Servicios Especializados.

- **Funciones:**

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

- Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

- Informar al encargado sobre entregas parciales o totales de información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

- Informar al encargado del Sistema de Datos Personales sobre los incidentes que ocurran y llevar un registro.

- **Obligaciones:**

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

- Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

Nombre: Rodolfo Ramírez Martínez.

- Cargo: Jefe de Servicios Especializados.

- **Funciones:**

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

- Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

- Informar al encargado sobre entregas parciales o totales de información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

- Informar al encargado del Sistema de Datos Personales sobre los incidentes que ocurran y llevar un registro.

- **Obligaciones:**

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

- Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (dispersión) del Sistema de Datos Personales (SIRH).

**Folio del registro en el Sistema Persona: 11280050000003**

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Firma
- RFC
- CURP

Datos Laborales

- Puesto

Datos Patrimoniales

- Ingresos y egresos
- Servicios contratados
- Otros

**D3. Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora**

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Eunice Maldonado Sánchez.

- Cargo: Titular de la Dirección de Administración y Finanzas.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales de los expedientes de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales de los expedientes de los Servidores Públicos, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargados:**

Nombre: Juan Carlos Luna Mendoza.

- Cargo: Titular del departamento de Recursos Humanos.

- **Funciones:**

- Validar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

- Verificar que se lleve a cabo el registro de los servidores públicos, que previamente se les hace entrega de información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

- Constatar que se actualice trimestralmente la relación de los servidores públicos a los que se les hace entrega de información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

- Recibir y validar las entregas parciales o totales de información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

- Recibir los informes de los incidentes que ocurran sobre datos personales y constatar que se lleve a cabo un registro de los mismos.

- **Obligaciones:**

- Validar los mecanismos que permitan asegurar que los datos personales en posición de la unidad administrativa, en el ejercicio de sus facultades, no se difundan, distribuyan o comercialicen.

- Verificar que se garantice la seguridad de los datos personales y evitar la alteración, pérdida transmisión y acceso no autorizado.

**Usuarios:**

Nombre: Gabriela Trejo Solis.

- Cargo: Ejecutivo de Proyectos Técnicos.

- **Funciones:**

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

- Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

- Actualizar trimestralmente la relación de los servidores públicos a los que se les hace entrega de información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

- Informar al encargado sobre entregas parciales o totales de información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

- Informar al encargado del Sistema de Datos Personales sobre los incidentes que ocurran y llevar un registro.

- **Obligaciones:**

- Verificar que el Sistema de Datos Personales se encuentre completo y sin alteraciones.

-Llevar un registro de los servidores públicos, que previamente se les hace entrega la información física y electrónica (Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora) del Sistema de Datos Personales.

**Folio del registro en el Sistema Persona:** Pendiente de registro.

**Datos personales contenidos en el sistema:**

**Datos de identificación:**

- Nombre
- Domicilio
- Teléfono particular
- Teléfono celular
- Correo electrónico
- Estado civil
- Firma
- RFC
- CURP
- Cartilla militar
- Lugar de nacimiento
- Fecha de nacimiento
- Nacionalidad
- Edad
- Nombres de familiares
- Dependientes y beneficiarios
- Fotografía
- Costumbres
- Contratos
- Idioma o lengua
- otros

**Datos de Laborales:**

- Nombramiento
- Incidencias
- Constancias de capacitación
- Puesto
- Domicilio de trabajo
- Correo electrónico institucional
- Teléfono institucional
- Actividades extracurriculares
- Referencias laborales
- Referencias personales
- otros

#### **D4. Sistema de Captura de Solicitudes de Pago**

**Nivel de seguridad:** Básico

**Responsable:**

Nombre: Eunice Maldonado Sánchez.

- Cargo: Titular de la Dirección de Administración y Finanzas.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Captura de Solicitudes de Pago.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Captura de Solicitudes de Pago, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: I. Eddgar Prado Sánchez.

- Cargo: Titular del Departamento de Recursos Materiales y Servicios Generales.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales del Sistema de Captura de Solicitudes de Pago.

- **Funciones:**

- Adoptar los procedimientos adecuados para atender las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Sistema de Captura de Solicitudes de Pago, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

- **Obligaciones:**

- Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
- Procurar que los datos personales sean exactos y actualizados;
- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;
- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;
- No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Usuarios:**

Nombre: Ivonne Mercedes Mayo Núñez.

- Cargo: Técnico Especializado en Sistemas de Cómputo.
- Funciones: Elaboración de solicitudes de cheque, así como asignar número de contratos y generar la actualización del catálogo de proveedores,
- Obligaciones: Actualización de catálogo y tramitar pagos así como darle seguimiento a los mismos.

Nombre: Verónica Patricia Moreno Cárdenas.

- Cargo: Jefe de Servicios Especializados.
- Funciones: Generar el reporte Modelo Integral de Desempeño de Órganos de Vigilancia y Control (MIDO), que se envía al Órgano Interno de Control, que a su vez envía a la SFP.
- Obligaciones: Generar reporte (MIDO), para cumplir con el requerimiento de la SFP.

Nombre: Daniela Betzabé Juárez Osnaya.

- Cargo: Técnico Superior.
- Funciones: Captura de solicitudes de cheques, asignación de partida presupuestal, asignación de folio único, crear el reporte para conciliación de recursos fiscales, crear reporte del cálculo y determinación del porcentaje del 50% - 50% a que se refiere al artículo 42 de la ley de Adquisiciones, Arrendamientos y Servicios del sector público.
- Obligaciones: Actualizar los reportes de conciliación que se envía al Órgano Interno de Control, Actualización de reporte del cálculo del 50% - 50% para

cumplir con la normatividad de Adquisiciones, Obras públicas, Servicio y Patrimonio Federal, que es enviado al (CAAS) y a la Junta de Gobierno.

**Folio de registro en el Sistema Persona:** 11280050000004

#### **Datos de Identificación**

- Nombre
- RFC
- Domicilio
- Teléfono
- Fax
- Correo electrónico
- Página de Internet

#### **D5. Recibos de Nómina**

**Nivel de seguridad:** Medio.

#### **Responsable:**

Nombre: Lic. Eunice A. Maldonado Sánchez.

- Cargo: Titular de la Dirección de Administración y Finanzas.

Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales de los Recibos de Nómina.

- Funciones:

-Adoptar los procedimientos adecuados para recibir y atender responder las solicitudes de acceso a la información y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del Kardex, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias competentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

- Obligaciones:

-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

-Procurar que los datos personales sean exactos y actualizados;

-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;

-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;

-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargado:**

Nombre: Paola Ariadna Piña Figueroa.

- Cargo: Titular del Departamento de Contabilidad y Finanzas.
- Funciones:
  - Validar que el Sistema de Datos Personales se encuentre correcto, completo y sin alteraciones.
  - Recibir y validar las entregas parciales o totales de información física del Sistema de Datos Personales.
- Obligaciones:
  - Vigilar que los datos personales que se encuentran bajo resguardo en el área a su cargo, no se difundan.
  - Verificar el aseguramiento de los datos personales.

**Usuarios:**

Nombre: Eleuterio Torres Romero.

- Cargo: Técnico Administrativo Especializado.
- Funciones:
  - Encargado del Archivo Contable.
  - Recepción y revisión de las solicitudes de cheque.
  - Recepción de correspondencia interna y externa.
  - Envío de los recibos de nómina a la sedes de Plaza y Madrid, así como entregar en la sede Búfalo recibos atrasados previamente solicitados.
- Obligaciones:
  - Tener el archivo contable actualizado para disposición de las diferentes instancias que soliciten información.
  - Proponer medidas de seguridad para la conservación de los documentos bajo resguardo del Departamento.

Nombre: Araceli Beatriz Díaz Fortis.

- Cargo: Ejecutivo de Proyectos Técnicos.
- Funciones:
  - Codificar y capturar pólizas de ingresos, egresos y diario.
  - Depuración de cuentas contables.
  - Determinar pagos, realizar análisis y depurar cuentas contables.
  - Emitir pólizas de diario e ingreso mensuales.
- Obligaciones:
  - Tener la contabilidad a actualizada par la revisión de las auditorias.

**Folio del registro en el Sistema Persona:** Pendiente de registro.

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Firma

- RFC
- CURP
- Fecha de nacimiento
- Edad

Datos Laborales

- Puesto

Datos Patrimoniales

- Ingresos

**D6. Comprobantes de pago**

**Nivel de seguridad:** Medio.

**Responsable:**

Nombre: Eunice Maldonado Sánchez.

- Cargo: Titular de la Dirección de Administración y Finanzas.  
-Con base en los artículos 20 y 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Titular de la Dirección de Administración y Finanzas tendrá las siguientes funciones y obligaciones en cuanto al tratamiento de los datos personales de los Comprobantes de pago.
- Funciones:  
-Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos y dar a conocer información sobre sus políticas en relación con la protección de datos personales del SIRH, de conformidad con los lineamientos que al respecto establezca el IFAI o las instancias equivalentes previstas en el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- Obligaciones:  
-Tratar datos personales sólo cuando éstos sean adecuados, pertinentes, y no excesivos en relación con los propósitos para los cuales se hayan obtenido;  
-Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;  
-Procurar que los datos personales sean exactos y actualizados;  
-Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación;  
-Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado, salvo que haya mediado, el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información;  
-No podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.

**Encargados:**

Nombre: Paola Ariadna Piña Figueroa.

- Cargo: Titular del Departamento de Contabilidad y Finanzas.
- Funciones:
  - Validar que el Sistema de Datos Personales se encuentre correcto, completo y sin alteraciones.
  - Recibir y validar las entregas parciales o totales de información física del Sistema de Datos Personales.
- Obligaciones:
  - Vigilar que los datos personales que encuentren bajo resguardo en el área a su cargo, no se difundan.
  - Verificar el aseguramiento de los datos personales.

**Usuarios:**

Nombre: Eleuterio Torres Romero.

- Cargo: Técnico Administrativo Especializado.
- Funciones:
  - Encargado del Archivo Contable.
  - Recepción y revisión de las solicitudes de cheque.
  - Recepción de correspondencia interna y externa
  - Envío de los recibos de nómina a la sedes Plaza y Madrid, así como entregar en la sede Búfalo recibos atrasados previamente solicitados
- Obligaciones:
  - Tener el archivo contable actualizado para disposición de las diferentes instancias que soliciten información.
  - Proponer medidas de seguridad para la conservación de los documentos bajo resguardo del Departamento.
  - Verificar la veracidad de la información personal.

Nombre: Edith Cedillo Rosales.

- Cargo: Técnico Especializado.
- Funciones:
  - Elaboración de conciliaciones de ingresos y gastos
  - Control de proveedores y acreedores diversos
  - Control de honorarios
- Obligaciones:
  - Verificar que el Sistema de Datos Personales se encuentre correcto y completo.
  - Llevar un buen registro de los datos personales que se entregan físicamente para su captura.

Nombre: Jazmín Díaz Mercado.

- Cargo: Jefe de Técnicos.
- Funciones:
  - Envío de formatos del Sistema Integral de Información.
  - Registro de Nómina

- Obligaciones:
  - Verificar que el Sistema de Datos Personales se encuentre completo
  - Llevar un buen registro de los datos personales que se entregan físicamente para su captura

**Folio del registro en el Sistema Persona:** Pendiente de registro.

**Datos personales contenidos en el sistema:**

Datos de Identificación

- Nombre
- Firma
- RFC
- CURP
- Dirección
- Teléfono
- Correo Electrónico
- Ingresos

## **PARTE 2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES**

### **A. DIRECCIÓN DE INVESTIGACIÓN**

#### **A1. Sistema de Información Académica del Mora (SIAM)**

**Nivel de seguridad:** Medio

**1. Tipo de soporte:**

- a) Tipo de soporte: Electrónico.
- b) Descripción: El Sistema de Información Académica del Instituto Mora, es un sistema automatizado conectado a la red mundial con interconexión cliente-servidor, con acceso mediante un nombre de usuario y contraseña, que permite la captura de productos académicos de los profesores-investigadores en su módulo 1.

**2. Características del lugar donde se resguardan los soportes:**

Red electrónica con interconexión cliente-servidor.

El soporte electrónico se encuentra en las computadoras de los encargados y usuarios del sistema.

#### **A2. Sistema de Información Académica del Mora (SIAM), Módulo Dictámenes Categorías, Promoción y Estímulos Académicos**

**Nivel de seguridad:** Medio

**1. Tipo de soporte:**

- a) Tipo de soporte: Electrónico.
- b) Descripción: El Sistema de Información Académica del Instituto Mora, es un sistema automatizado conectado a la red mundial con interconexión cliente-servidor, con acceso mediante un nombre de usuario y

contraseña, que permite la captura y consulta de dictámenes de asignación de categorías, promoción y estímulos en su módulo 3.

## **2. Características del lugar donde se resguardan los soportes:**

Red electrónica con interconexión cliente-servidor.

El soporte electrónico se encuentra en las computadoras de los encargados y usuarios del sistema.

### **A3. Sistema de Librería.**

**Nivel de seguridad:** Básico

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Electrónico.
- b) Descripción: Sistema automatizado que permite la administración de inventarios de publicaciones, conectado a la red mundial con interconexión cliente-servidor, que permite realizar ventas en línea

## **2. Características del lugar donde se resguardan los soportes:**

Red electrónica con interconexión cliente-servidor.

El soporte electrónico se encuentra en las computadoras de los encargados y usuarios del sistema, y el físico en una gaveta en resguardo del Responsable del Área de Distribución de Publicaciones.

## **B. DIRECCIÓN DE DOCENCIA**

### **B1. Bases de datos personales de usuarios de la Biblioteca Ernesto de la Torre Villar**

**Nivel de seguridad:** Básico

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Electrónico
- b) Descripción: Base de datos relacional

## **2. Características del lugar donde se resguardan los soportes:**

Red electrónica con interconexión cliente-servidor.

### **B2. Sistema de Seguimiento de Egresados del Mora (SISEM)**

**Nivel de seguridad:** Medio

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico
- b) Descripción: Se tiene el soporte físicamente en carpetas que contienen los programas y las diferentes generaciones contando con una hoja general en la que se tiene la siguiente información: Nombre, generación, último grado obtenido, trabajo actual, dependencia y grado de SNI. De igual manera contiene los cuestionarios que se aplican a cada egresado con el fin de dar seguimiento a su trayectoria académica y laboral. También se tiene soporte electrónico llamado SISEM en el que se guarda la información de los egresados la cual ellos mismos actualizan, y se manejan por medio de claves para los egresados, servicios escolares y el administrador.

## **2. Características del lugar donde se resguardan los soportes:**

Se resguardan en los estantes de madera que se encuentran en la oficina del Departamento de Servicios Escolares.

Electrónicamente se cuenta con un centro de datos para resguardar la información.

### **B3. Expedientes de alumnos**

**Nivel de seguridad:** Alto

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: Se tiene el soporte físicamente de los expedientes de alumnos que cursan actualmente alguno de los programas de Docencia en los estantes metálicos del Departamento de Servicios Escolares y las generaciones anteriores se mantienen en el archivo de concentración. También se tiene soporte en carpetas electrónicas con la información y los documentos escaneados de los alumnos, esta información puede ser consultada solamente por los integrantes del Departamento de Servicios Escolares.

## **2. Características del lugar donde se resguardan los soportes:**

Se resguardan en los estantes metálicos de la oficina del Departamento de Servicios Escolares y en el Archivo de Concentración.

### **B4. Sistema de Evaluación del Desempeño Académico (SEDA)**

**Nivel de seguridad:** Básico

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: Se cuenta con un sistema llamado SEDA (Sistema de Evaluación del Desempeño Académico) de manera electrónica en el cual se integra y actualiza la información de los profesores que imparten alguna materia en el Instituto por medio de un administrador, de igual forma se integra la información de los alumnos y al momento de evaluar el desempeño académico de los profesores se les da una clave de acceso. También se tiene soporte físico por medio de carpetas en donde se resguardan los informes de dichas evaluaciones y también se tiene los expedientes tanto de los alumnos como de los profesores, esta información puede ser consultada por los integrantes del Departamento de Servicios Escolares y los coordinadores académicos de cada programa.

## **2. Características del lugar donde se resguardan los soportes:**

Se resguardan en los estantes de madera y metálicos de la oficina del Departamento de Servicios Escolares y las coordinaciones académicas de cada programa.

Electrónicamente se cuenta con un centro de datos para resguardar la información.

## C. DIRECCIÓN DE VINCULACIÓN

### C1. Directorio del Mora

**Nivel de seguridad:** Básico

#### 1. Tipo de soporte:

- a) Tipo de soporte: Electrónico.
- b) Descripción: El directorio se alberga en Excel y únicamente el encargado y el usuario pueden entrar al archivo.

#### 2. Características del lugar donde se resguardan los soportes:

El directorio se resguarda en una computadora bajo una clave de acceso.

### C2. Registro de Invitados

**Nivel de seguridad:** Básico

#### 1. Tipo de soporte:

- a) Tipo de soporte: Electrónico.
- b) Descripción: El directorio se alberga en Word y únicamente el encargado y el usuario pueden entrar al archivo.

#### 2. Características del lugar donde se resguardan los soportes:

El directorio se resguarda en una computadora bajo una clave de acceso.

## C3. Sistema de registro de correos electrónicos

**Nivel de seguridad:** Básico

#### 1. Tipo de soporte:

- a) Tipo de soporte: Electrónico
- b) Descripción: El registro de correos electrónicos se alberga en Outlook y únicamente el usuario de este sistema puede entrar al directorio

#### 2. Características del lugar donde se resguardan los soportes:

El sistema de registro de correos electrónicos se resguarda en una computadora bajo dos claves de acceso.

## D. DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

### D1. Kardex

**Nivel de seguridad:** Medio

#### 1. Tipo de soporte:

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: El sistema únicamente se encuentra instalado en tres equipos, se tienen claves de acceso por usuario y el sistema emite un reporte de acceso a los procesos realizados. Se tiene una bitácora para la entrega de la información en medio electrónico (dispersión) y físico, donde firma quien entrega, quien recibe y la misma es controlada con un número de folio.

Asimismo, la única persona que puede autorizar la entrega de la información es el titular del departamento de Recursos Humanos.

## **2. Características del lugar donde se resguardan los soportes:**

Los soportes se encuentran resguardados en el departamento de Recursos Humanos en una gaveta del archivo del departamento que se encuentra bajo llave y en el propio sistema.

### **D2. Sistema de Recursos Humanos (SIRH)**

**Nivel de seguridad:** Medio

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: Para ingresar al sistema solamente se tienen claves de acceso confidenciales para cada uno de los usuarios, las mismas se asignan de acuerdo a sus facultades operativas, lo que nos permite identificar el acceso a los procesos y poder emitir dictámenes de ingreso.  
Asimismo, se tiene una bitácora para la entrega de la información en medio electrónico (dispersión) y físico, donde firma quien entrega, quien recibe y la misma será controlada con un número de folio (como un soporte adicional para el caso de la información física, se anota el número de memorándum de entrega de información).

## **2. Características del lugar donde se resguardan los soportes:**

Los soportes se encuentran ubicados en el departamento de Recursos Humanos en los archiveros de madera y en el propio sistema.

### **D3. Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora**

**Nivel de seguridad:** Básico

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: La única persona que puede ingresar a los expedientes es la responsable del archivo del departamento.

## **2. Características del lugar donde se resguardan los soportes:**

Se cuenta con una bitácora para la entrega de la información física y electrónica, donde firma quien entrega, quien recibe y la misma será controlada con un número de folio (en el caso de la información solicitada vía correo electrónico, se anexara correo de solicitud y entrega impreso).

### **D4. Sistema de Captura de Solicitudes de Pago**

**Nivel de seguridad:** Básico

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: Elaborada en Microsoft Office Access, la información de los proveedores se obtiene de realizar una consulta en Access, dicha consulta se exporta a un archivo de Excel. Esta protegido. También contamos con expedientes.

## **2. Características del lugar donde se resguardan los soportes:**

El soporte electrónico se encuentra en las computadoras de las C. Ivonne M. Mayo Núñez, Daniela B. Juárez Osnaya y de la Lic. Verónica P. Moreno Cárdenas. Y el físico en una gaveta archivadora que se ubica en las oficinas del Departamento de Recursos Materiales y Servicios Generales en la Bodega ubicada en Búfalo No. 166, Col. Del Valle, CP 03100 México, DF.

### **D5. Recibos de Nómina**

**Nivel de seguridad:** Medio

#### **1. Tipo de soporte:**

- a) Tipo de soporte: Físico.
- b) Descripción: Los recibos se encuentran en expedientes y estos están en libreros debidamente identificados para un mejor control y manejo.

#### **2. Características del lugar donde se resguardan los soportes:**

Los recibos entregados y los no recogidos se encuentran en el departamento de Contabilidad y Finanzas en lugar bien ventilado para conservar en buen estado los documentos.

### **D6. Comprobantes de pago**

**Nivel de seguridad:** Medio

#### **1) Tipo de soporte:**

- a) Tipo de soporte: Físico y electrónico.
- b) Descripción: Los comprobantes se encuentran en expedientes y estos están en libreros debidamente identificados para un mejor control y manejo. En lo que se refiere al soporte electrónico la información se encuentran en los equipos de Edith Cedillo y Jazmín Díaz.

#### **2) Características del lugar donde se resguardan los soportes:**

Los soportes se encuentran en el departamento de Contabilidad y Finanzas en lugares bien ventilados para evitar que se deteriore la documentación.

## **PARTE 3. MEDIDAS DE SEGURIDAD**

### **I. FUNCIONES Y OBLIGACIONES DEL PERSONAL**

1. Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.
2. Constituye una obligación del personal notificar al encargado del sistema, en su caso, de las incidencias de seguridad de las que tenga conocimiento.
3. Todo el personal deberá guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

### **II. POLÍTICAS DE SEGURIDAD**

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación

con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

## **NIVELES**

### **Nivel básico**

A los sistemas que contienen alguno de los datos que se enlistan a continuación, les resultan aplicables únicamente, las medidas de seguridad de nivel básico.

- De identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
- 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.

### **Nivel medio**

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas con nivel medio.

- Datos Patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
- Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
- Datos Académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
- Tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

### **Nivel alto**

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con nivel alto.

- Datos Ideológicos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
- Datos de Salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas,

consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

- Características personales: Tipo de sangre, ADN, huella digital, u otros análogos.
- Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
- Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.
- Origen: Étnico y racial.

## POLÍTICAS

### Nivel básico

1. Llevar control y registros del Sistema de Datos Personales en la “Bitácora de operación de Datos Personales” **Anexo 1**, con la finalidad de asentar los usuarios, accesos, respaldos e incidentes, así como la transmisión de datos y sus destinatarios;
2. Garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del Sistema de Datos Personales según su perfil de usuario;
3. Elaborar respaldos de bases de datos, y realizar pruebas periódicas de restauración;
4. Llevar un control de los medios magnéticos u ópticos de respaldo de los datos personales, utilizando el “Control de Respaldos de Datos Personales” **Anexo 2**.
5. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;
6. Garantizar que durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accedidos, reproducidos, alterados o suprimidos sin autorización;
7. Llevar a cabo verificaciones por medio de la Subdirección de Informática, según corresponda y respecto a las medidas técnicas establecidas; en su caso, remitirlas al Órgano Interno de Control.

### Nivel medio

1. Llevar control y registros del Sistema de Datos Personales en la “Bitácora de operación de Datos Personales” **Anexo 1**, con la finalidad de asentar los usuarios, accesos, respaldos e incidentes, así como la transmisión de datos y sus destinatarios;
2. Garantizar que el personal encargado del tratamiento de datos personales, sólo tenga acceso a las funciones autorizadas del Sistema de Datos Personales según su perfil de usuario;
3. Aplicar el procedimiento de respaldo y recuperación de datos, y realizar pruebas periódicas de restauración;
4. Llevar control de inventarios y clasificación de los medios magnéticos u ópticos de respaldo de los datos personales, utilizando el “Control de de Respaldos de Datos Personales” **Anexo 2**.
5. Utilizar un espacio externo seguro para guardar de manera sistemática los respaldos de las bases de datos de los sistemas de datos personales;

6. Garantizar que durante la transmisión de datos personales y el transporte de los soportes de almacenamiento, los datos no sean accedidos, reproducidos, alterados o suprimidos sin autorización;
7. Llevar a cabo verificaciones a través de la Subdirección de Informática, según corresponda, respecto de medidas técnicas de seguridad establecidas y en su caso, remitirlos al Órgano Interno de Control.

#### **Nivel alto**

1. Sólo el Director General del Instituto, podrá facultar al responsable y designar a los encargados del manejo de documentos pertenecientes a un Sistema de Datos Personales catalogado con nivel de seguridad alto.
2. En los accesos a los datos de los documentos de nivel alto, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el documento accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.
3. Los datos del registro de accesos se conservaran por cinco años.

### **III. ACCESO A LAS INSTALACIONES**

#### **1. Seguridad perimetral exterior:**

El acceso de personas a las instalaciones del Instituto quedará asentado en un "Libro de registro de entrada y salida", el cual se utilizará en cualquiera de las tres sedes del Instituto, incluyendo los almacenes.

Para las personas que acceden a las instalaciones:

- a) La identificación se realizará bajo registro de entrada y salida.
- b) La autenticación se llevará a cabo cuando el vigilante en turno realice una llamada telefónica para preguntar si puede pasar esa persona (llamada según corresponda a la persona a quien vienen a buscar).
- c) La autorización se da cuando el vigilante en turno solicita la autorización del personal en turno para permitir el acceso de persona distinta a la plantilla de personal y estudiantes del Instituto Mora.

### **IV. ACCESOS CONTROLADOS Y BITÁCORAS**

1. Cada acceso a un Sistema de Datos Personales deberá registrarse en la "Bitácora de operación de Datos Personales" **Anexo 1**, asentando lo siguiente:
  - a) Datos completos del Responsable, Encargado o Usuario (quien autoriza el acceso);
  - b) Fecha y hora en que se realizó el acceso, o se intentó el mismo;
  - c) Sistema de Datos Personales accedido;
  - d) Motivo de las operaciones o acciones llevadas a cabo dentro del Sistema de Datos Personales; y
  - e) Fecha y hora en que se realizó la salida del Sistema de Datos Personales.

### **V. GESTIÓN DE SOPORTES**

1. Los soportes que contengan datos de carácter personal deberán ser etiquetados para permitir su identificación, inventariados y almacenados en

un lugar de acceso restringido al que sólo tendrán acceso las personas con autorización del Responsable.

2. Los soportes informáticos se almacenarán de acuerdo a los procedimientos que establezca la Subdirección de Informática, para tal efecto.
3. La salida de soportes informáticos que contengan datos de carácter personal, únicamente puede ser autorizada por el responsable del documento o aquel en que se hubiera delegado esta función.
4. Si los soportes con datos de los mencionados documentos van a salir fuera de las instalaciones del Instituto Mora, como consecuencia de operaciones de mantenimiento, se adoptarán las medidas que para tal efecto establezca el responsable del Sistema de Datos Personales, dejando evidencia por escrito de tal resolución.
5. Distribución cifrada de soportes.  
La distribución y salida de soportes que contengan datos de carácter personal clasificados con nivel alto, se realizará con mecanismos que garanticen que dicha información no sea inteligible ni manipulada durante su transporte. Dicho procedimiento será responsabilidad de la Subdirección de Informática, previa solicitud del Responsable del Sistema de Datos Personales.
6. Es obligatorio realizar copias de respaldo de los sistemas automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
7. Características de la gestión de soportes de los sistemas automatizados de datos personales.

**7.1** Sistemas automatizados cuyo soporte técnico depende de la Subdirección de Informática:

**A. DIRECCIÓN DE INVESTIGACIÓN**

**A1.** Sistema de Información Académica del Mora (SIAM)

**A2** Sistema de Información Académica del Mora (SIAM), Módulo Dictámenes Categorías, Promoción y Estímulos Académicos

**A3** Sistema de Librería

**B. DIRECCIÓN DE DOCENCIA**

**B2.** Sistema de Seguimiento de Egresados del Mora (SISEM)

**B4.** Sistema de Evaluación del Desempeño Académico (SEDA)

- Modelo de control de acceso:
  - El control de acceso a cada sistema está basado en roles (perfiles/administrador, usuarios).
- Perfiles de usuario y contraseñas:
  - Los sistemas de datos automatizados del Instituto Mora requieren de nombre de usuario y contraseña de acceso.
- En caso de que el sistema presente una falla, el plan de contingencia con el cual garantiza la continuidad de la operación del sistema:
  - a) Obedece un protocolo informático ya establecido.
  - b) Utiliza los últimos respaldos para rescatar los datos perdidos.

- Tipos de respaldos:
  - a) Completos,
  - b) Diferenciales, (Respaldo de los datos que se agregaron en un determinado periodo)
- Medios utilizados para almacenar las copias de seguridad.
  - a) Cintas magnéticas.
  - b) Discos duros.
  - c) CD.
  - d) Otros.
- Ubicación de los medios de respaldo:

Nombre del servidor	Nombre de la tarea	Rol del Servidor	Tipo de respaldo	Hora inicio	Día	Número de semana
IMDBPLAZA	Imdbplaza	SIAM, SISEM, Librería, SEDA, BD Oracle	Full	9:00 AM	Martes	Todas

- Responsable de realizar estas operaciones:  
Nombre: Laura Icela González Pérez.  
Cargo: Administrador de redes.

## 7.2 Sistemas automatizados de soporte técnico externo:

### D. DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

#### D2. Sistema de Recursos Humanos (SIRH)

- Modelo de control de acceso
  - Es obligatoria la acreditación para acceder al sistema.
- Los perfiles de usuario y contraseñas son manejados por el software aplicativo del Sistema de Recursos Humanos.
- En caso de que el sistema presente una falla, seleccione el plan de contingencia con el cual garantiza la continuidad de la operación del sistema.
  - a) Obedece un protocolo informático ya establecido.
  - b) Utiliza los últimos respaldos para rescatar los datos perdidos.
- Tipos de respaldos:
  - a) Completos,
  - b) Diferenciales, (Respaldo de los datos que se agregaron en un determinado periodo) o
  - c) Incrementales del sistema; (Respaldo de los datos que se agregaron en el último periodo)
- Medios utilizados para almacenar las copias de seguridad
  - a) Cintas magnéticas
  - b) Discos duros,
- Ubicación de los medios de respaldo.
  - Departamento de Recursos Humanos

- Responsable de realizar estas operaciones.  
-Soporte externo.
8. Características de la gestión de soportes de los sistemas no automatizados de datos personales:
- B. DIRECCIÓN DE DOCENCIA**
- B1.** Bases de datos de usuarios de la Biblioteca Ernesto de la Torre Villar
- B3.** Expedientes de alumnos
- C. DIRECCIÓN DE VINCULACIÓN**
- C1.** Directorio del Mora
- C2.** Registro de Invitados
- C3.** Sistema de registro de correos electrónicos
- D. DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS**
- D1.** Kardex
- D3.** Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora
- D4.** Sistema de Captura de Solicitudes de Pago
- D5.** Recibos de Nómina
- D6.** Comprobantes de pago
- Modelo de control de acceso:
    - a) El control de acceso al sistema está basado en reglas (políticas/manual de procedimientos).
    - b) Sólo los encargados y usuarios pueden acceder a las bases de datos y expedientes de cada sistema.
  - Tipos de respaldos:
    - f) Completos,
    - g) Diferenciales, (Respaldo de los datos que se agregaron en un determinado periodo)
    - h) Incrementales del sistema; (Respaldo de los datos que se agregaron en el último periodo)
  - Medios utilizados para almacenar las copias de seguridad.
    - a) Discos duros,
    - b) CD-ROM,
    - c) Otros.
  - Ubicación de los medios de respaldo de cada sistema, en las áreas responsables de cada uno de ellos.
  - Responsables de realizar estas operaciones en cada sistema:  
Nombre: Carlos Gabino Arellano Osorio  
Cargo: Titular de la Subdirección de Biblioteca.  
**-B1.** Bases de datos de usuarios de la Biblioteca Ernesto de la Torre Villar  
  
Nombre: Lorena Navarro Sandoval  
Cargo: Titular del Departamento de Servicios Escolares.  
**-B3.** Expedientes de alumnos

Nombre: Mónica Rodríguez Sánchez

Cargo: Titular del Departamento de Difusión

- C1. Directorio del Mora
- C2. Registro de Invitados
- C3. Sistema de registro de correos electrónicos

Nombre: Juan Carlos Luna Mendoza

Cargo: Titular del Departamento de Recursos Humanos

- D1. Kardex
- D3. Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora

Nombre: Eddgar Prado Sánchez

Cargo: Titular del Departamento de Recursos Materiales y Servicios Generales

- D4. Sistema de Captura de Solicitudes de Pago

Nombre: Lic. Paola Ariadna Piña Figueroa

Cargo: Titular del Departamento de Contabilidad y Finanzas

- D5. Recibos de Nómina
- D6. Comprobantes de pago

## VI. PERFILES DE USUARIO Y CONTRASEÑAS

1. Todas las claves de acceso, que actualmente se encuentran activas, fueron autorizadas por el administrador responsable de la aplicación con un perfil de acceso específico a las funciones a desempeñar en el sistema, donde este mismo perfil se encuentra enlazado con un "Rol" a nivel base de datos. Asimismo es importante señalar que todas las contraseñas de dichas claves de acceso para cada uno de los usuarios, se encuentran encriptadas por el mismo manejador de la base de datos, por lo que el personal de informática nunca sabrá la contraseña de un usuario, al menos que se regenere el password a petición del responsable.
2. Administración de perfiles de usuario y contraseñas:
  - Los nuevos usuarios y perfiles son dados de alta por el administrador de cada aplicación.
  - El responsable de cada Sistema de Datos Personales es la única persona facultada para autorizar la creación de nuevos perfiles.
  - Se evita el acceso remoto no autorizado a través de certificados de seguridad.
  - Se deberá mantener un registro de usuarios nuevos a nivel sistema y base de datos.
3. Características de la gestión de soportes de los sistemas automatizados de datos personales.
  - 3.1 Sistemas automatizados cuyo soporte técnico depende de la Subdirección de Informática:
    - Modelo de control de acceso:

El control de acceso a cada sistema está basado en roles (perfiles/administrador, usuarios).

- Perfiles de usuario y contraseñas:  
Los sistemas de datos automatizados del Instituto Mora requieren de nombre de usuario y contraseña de acceso.

### 3.2 Sistemas automatizados de soporte técnico externo:

- Modelo de control de acceso  
Es obligatoria la acreditación para acceder al sistema.
- Los perfiles de usuario y contraseñas son manejados por el software aplicativo del Sistema de Recursos Humanos.

### 4. Características de la gestión de soportes de los sistemas no automatizados de datos personales:

- Modelo de control de acceso:
  - a) El control de acceso al sistema está basado en reglas (políticas/manual de procedimientos).
  - b) Sólo los encargados y usuarios pueden acceder a las bases de datos y expedientes de cada sistema mediante nombre y clave que los identifica en la red institucional.

## VII. TRANSMISIÓN DE DATOS PERSONALES

### 1. Los siguientes sistemas realizan transmisiones de datos mediante el traslado de datos sobre redes electrónicas:

#### A. DIRECCIÓN DE INVESTIGACIÓN

**A1.** Sistema de Información Académica del Mora (SIAM)

**A2** Sistema de Información Académica del Mora (SIAM), Módulo Dictámenes Categorías, Promoción y Estímulos Académicos.

**A3** Sistema de Librería

#### B. DIRECCIÓN DE DOCENCIA

**B2.** Sistema de Seguimiento de Egresados del Mora (SISEM)

**B4.** Sistema de Evaluación del Desempeño Académico (SEDA)

### 2. Los siguientes sistemas se sujetan a transmisiones físicas y/o la red local de cada área:

#### B. DIRECCIÓN DE DOCENCIA

**B1.** Bases de datos de usuarios de la Biblioteca Ernesto de la Torre Villar

**B3.** Expedientes de alumnos

#### C. DIRECCIÓN DE VINCULACIÓN

**C1.** Directorio del Mora

**C2.** Registro de Invitados

**C3.** Sistema de registro de correos electrónicos

#### D. DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

**D1.** Kardex

**D2.** Sistema de Recursos Humanos (SIRH)

**D3.** Expedientes personales de los Servidores Públicos del Instituto de Investigaciones Dr. José María Luis Mora

**D4.** Sistema de Captura de Solicitudes de Pago

- D5. Recibos de Nómina
- D6. Comprobantes de pago

3. El cifrado de datos de la red Institucional se lleva a cabo mediante el acceso a Internet:
  - Capacidad SSL-VPN
  - Cantidad Site to Site túneles
  - Encriptación/autenticación/DH Group: DES,3DES,AES(128,192, 256 bits), MD5, SHA-1/DH group 1,2,5,14
  - Key exchange: IKE, IKEv2, Manual key, PKI(X.509), L2TP over IPSec
  - Soporte de ruteo basado en VPN
  - Soporte de Dead Peer Detection
  - Soporte de IPSec Nat Transversal
  - Soporte Global VPN Cliente de plataformas soportadas: Microsoft Windows 2000, Windows XP, Microsoft Vista 32 bit/ 64 bit
  - Soporte de SSL VPN de plataformas soportadas: Microsoft Windows 2000/XP/Vista 32/65 bit, Mac 10.4+, linux FC3+/Ubuntu 7+/Open SUSE

#### VIII. PLAN DE CONTINGENCIA

El plan de contingencia con el cual se garantiza la continuidad de la operación de los sistemas no automatizados se encuentra en desarrollo. Actualmente los Sistemas de Datos Personales se soportan con los respaldos completos y diferenciales para atender las contingencias.  
Ver **Anexo 3**. Contingencias SIAM y SISEM

### PARTE 4. PROCEDIMIENTO DE RESPALDO Y RECUPERACIÓN DE DATOS

#### I. Normas:

1. El respaldo de información se efectuará en medio magnético (Disco duro o CD).
2. Invariablemente se harán respaldos de información por lo menos trimestralmente.
3. Se hará un respaldo anual de toda la información contenida en cada sistema de datos personales, y quedarán a resguardo de la Subdirección de Informática.
4. En el caso de que no se puedan hacer los respaldos (Virus o falla en unidad de almacenamiento) el responsable del Sistema de Datos Personales deberá elaborar un oficio dirigido al Director General, con copia al Subdirector de Informática y al Titular del Órgano Interno de Control, explicando los causales de la pérdida o retraso de respaldos de datos personales.
5. Se deberán reutilizar los medios de respaldo que contienen datos personales.
6. Las áreas responsables de cada sistema, deberán enviar un respaldo completo anual de datos personales.

7. Invariablemente la Subdirección de Informática deberá resguardar el respaldo anual de todos los Sistemas de Datos Personales.

## II. Descripción:

### 1. Responsable de cada Sistema de Datos Personales

- Revisa la información a respaldar y el proceso al que corresponde.
- Define la conveniencia del proceso a seguir, los archivos y el periodo que comprenderá el respaldo.
- Respalda la información, con base en el proceso determinado y genera la copia de los archivos en el medio magnético más conveniente.
- Anota en la Bitácora de operación de Datos Personales, **Anexo 1** la fecha, hora de inicio y fin del respaldo.
- Retira el medio magnético, adhiere etiqueta con el nombre del Sistema de Datos Personales, el proceso de respaldo y el periodo que comprende, con base en las políticas antes mencionadas. Guarda en la ubicación correspondiente.
- Si se trata de un respaldo anual.

### 2. Responsable de cada Sistema de Datos Personales

- Repite los pasos del 1 al 6 para generar un respaldo anual completo del Sistema de Datos Personales que corresponda.
- Elabora un oficio dirigido al Titular de la Subdirección de Informática Informa, con copia al Director General y al Titular del Órgano Interno de Control, donde especifica el nombre del Sistema de Datos Personales, el proceso de respaldo, y el año que comprende la información.
- Anexa al oficio el medio magnético que contiene el respaldo anual del Sistema de Datos Personales, y envía la información a la Subdirección de Informática para su resguardo.

### 3. Subdirección de Informática.

- Recibe el oficio y el medio magnético correspondiente, y los registra en el Control de Respaldos de Datos Personales, **Anexo 2**.
- Resguarda la información en un espacio físico al cuál sólo pueda acceder el Titular de la Subdirección de Informática, y personal autorizado.

Proceso de respaldo	Archivos en respaldo	Ventajas	Desventajas
<b>Completo</b>	Todos	Con este respaldo únicamente es posible recuperar toda la información	Tiempo de Ejecución
<b>De Incremento (Incremental)</b>	Aquellos que hayan cambiado desde el último Respaldo Completo	Velocidad	Requiere del último Respaldo Completo y de todos los Respaldos de Incremento que le siguieron para recuperar el Sistema

<b>Diferencial</b>	Aquellos que hayan cambiado desde el último Respaldo Completo	Sólo requiere del último Respaldo Completo y del último respaldo Diferencial	Ocupa mayor espacio en discos comparado con Respaldos de Incremento
--------------------	---	--	---

### III. Ver **Anexo 3.** Contingencias SIAM y SISEM

## **PARTE 5. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE DATOS PERSONALES**

### **I. Normas:**

1. Un Sistema de Datos Personales sólo podrá ser cancelado en los casos siguientes:
  - a) Derivado de la desaparición de la unidad administrativa a la cual estuviera a cargo, y en el caso de que las actividades y funciones desempeñadas por dicha unidad, no sean delegadas o comisionadas a otra instancia.
  - b) Por la creación de uno o más sistemas que resguarden los datos personales contenidos en el sistema anterior, y previa explicación y justificación por escrito de la Dirección de área encargada del sistema.
  - c) Por la publicación de normatividad externa o interna que instruya la destrucción parcial o total del sistema y/o de los datos personales contenidos en este.
2. La Dirección de área del Instituto deberá solicitar por escrito al Comité de Información, la cancelación de la plaza o plazas que estén en los supuestos anteriores.
3. El Comité de Información del Instituto de Investigaciones Dr. José María Luis Mora será la única instancia autorizada para autorizar la cancelación de los sistemas de datos personales, y la Unidad de Enlace para operar la cancelación del registro ante el IFAI

### **II. Descripción:**

1. Dirección de área. Elabora oficio en original y copia solicitando la cancelación del Sistema de Datos Personales, según sea el caso, y turna a la Unidad de Enlace del Instituto Mora.
2. Unidad de Enlace. Recibe oficio de solicitud en original y copia, firma de recibido en la copia y entrega a la Dirección de área; revisa y turna copia del oficio de la solicitud a los integrantes del Comité de Información, en la próxima sesión.
3. Comité de Información. Recibe oficio de solicitud, analiza y determina.
4. Unidad de Enlace. No procede, elabora oficio en original y dos copias, señalando la causa de la improcedencia y envía original a la Dirección de área, con copia a la Dirección General, a los integrantes del Comité de Información y archiva copia para su control.
5. Dirección de área. Recibe oficio en original, se entera y, en su caso, corrige. Se conecta con la operación No. 1.

6. Unidad de Enlace. Si procede, cancela el registro del Sistema de Datos Personales ante el IFAI. Elabora oficio en original y dos copias, señalando la fecha de cancelación del registro del Sistema de Datos Personales, envía original a la Dirección de área, con copia a la Dirección General, a los integrantes del Comité de Información y archiva copia para su control.
7. Dirección de área. Recibe oficio en original, se entera, aplica su procedimiento interno para cancelar el Sistema de Datos Personales atendiendo las medidas de seguridad correspondientes, y según sea el caso, solicita el apoyo de la Subdirección de Informática mediante oficio en original y dos copias, señalando la fecha de cancelación del Sistema de Datos Personales, con copia a la Unidad de Enlace.

## **PARTE 6. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD**

### **Responsable del desarrollo:**

Lic. Elizabeth García Duarte, Titular del Departamento de Organización e Información. 55 98 37 77 Ext. 1173

Lic. Enrique Ayala Covarrubias, Subdirector de Informática. 55 98 37 77 Ext. 1169

Lic. Héctor Valdez Luna, Asesor Técnico del Departamento de Organización e Información. 55 98 37 77 Ext. 1171

### **Revisó:**

Lic. Elizabeth García Duarte, Titular del Departamento de Organización e Información. 55 98 37 77 Ext. 1173

### **Autorizó:**

Dr. Oscar de los Reyes Heredia, Secretario General y Titular de la Unidad de Enlace. 55 98 37 77 Ext. 1144

Lic. Eunice Angélica Maldonado Sánchez, Directora de Administración y Finanzas e Integrante del Comité de Información. 55 24 36 54 Ext. 2224

Ing. Carlos Ladrón de Guevara Rivero, Titular del Órgano Interno de Control e Integrante del Comité de Información. 55 24 36 54 Ext. 2230

**Fecha:** Aprobado por el Comité de Información del Instituto de Investigaciones Dr. José María Luis Mora, el 7 de diciembre de 2009, en su Cuarta Reunión Ordinaria.

## **PARTE 7. ANEXOS TÉCNICOS**

**Anexo 1.** Bitácora de operación de Datos Personales.

**Anexo 2.** Control de Respaldos de Datos Personales.

**Anexo 3.** Contingencias SIAM y SISEM

**Anexo 4.** Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales.





**Tipo de Documento:** Contingencia  
**Objetivo:** Administrar el servidor de aplicaciones TOMCAT para el Sistema de Información Académica del Mora (SIAM) y Sistema de Información de Seguimiento de Egresados (SISEM)  
**Fecha de Elaboración:** Junio 2004  
**Última actualización:** Julio 2008  
**Elaboró:** Silvia Lazarini Gutiérrez  
**Revisó:** Enrique Ayala Covarrubias

Este procedimiento aplica en los siguientes casos:

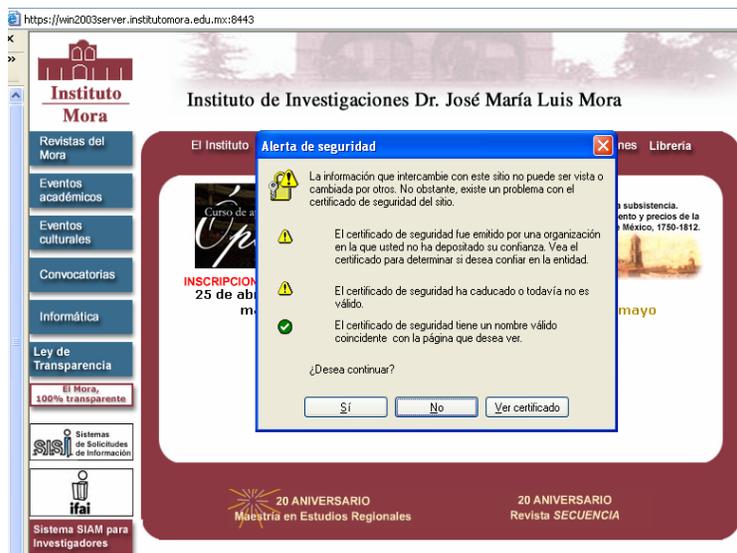
1. En caso de que se necesite reiniciar el servidor
2. En caso de actualizar la aplicación

Esta aplicación está corriendo en el servidor IMDBPLAZA

Para que el **Tomcat Manager y la aplicación** funcionen, en el servidor siempre debe estar abierta una ventana de Símbolo de sistema llamada **TOMCAT**

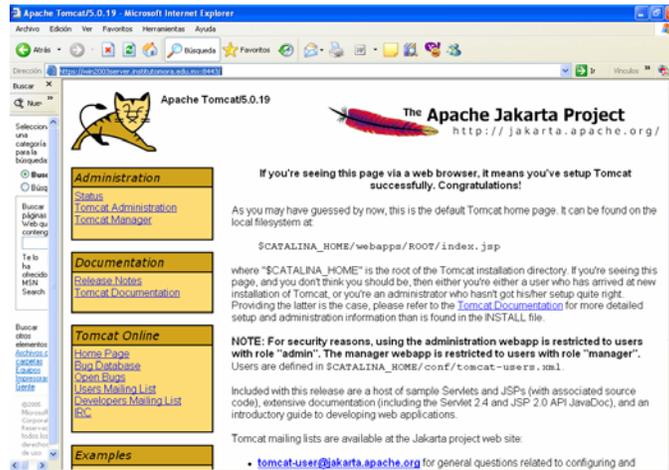
En caso de que el servidor se tuviera que reiniciar debemos:

- Verificar que no existan usuarios activos.
- Realizar una exportación de los datos se explica en procedimiento de respaldo de Base de Datos.
- Parar la aplicación desde el **tomcat manager**, como a continuación se describe. Posteriormente cerrar la ventana de símbolo de sistema llamada **tomcat**.
- Al reiniciar el servidor se sigue el procedimiento iniciando el icono que está en el escritorio llamado startup.bat. Ahí iniciará la ventana de símbolo de sistema. Posteriormente se sigue el procedimiento de tomcat manager y la aplicación estará publicada a todos los usuarios.

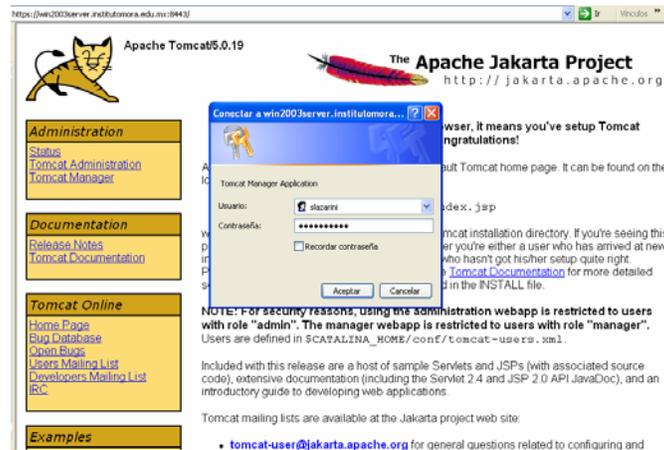


1. Se accede vía el Internet explorer a la dirección <https://imdbplaza.institutomora.edu.mx:8443/>
2. Se mostrará una pantalla de alerta de seguridad, y cuando pregunta si deseamos continuar le damos un clic en Sí

**Tipo de Documento:** Contingencia  
**Objetivo:** Administrar el servidor de aplicaciones TOMCAT para el Sistema de Información Académica del Mora (SIAM) y Sistema de Información de Seguimiento de Egresados (SISEM)  
**Fecha de Elaboración:** Junio 2004  
**Última actualización:** Julio 2008  
**Elaboró:** Silvia Lazarini Gutiérrez  
**Revisó:** Enrique Ayala Covarrubias

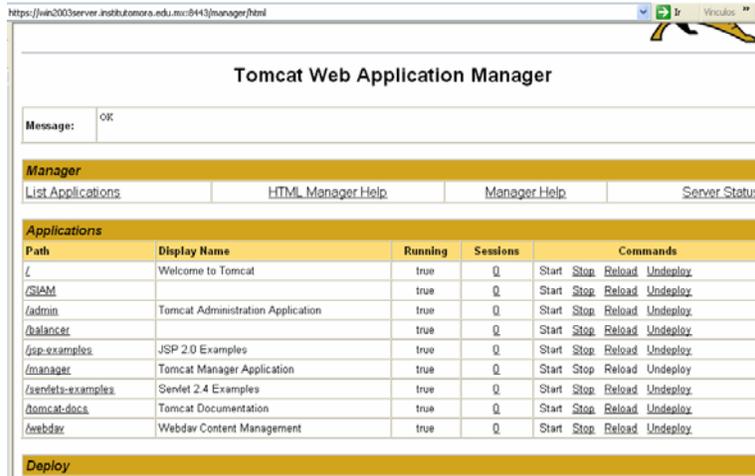


3. Automáticamente se muestra la página de Apache tomcat5.0.19
4. En ese momento hay que dar un clic al link TOMCAT MANAGER que se encuentra en la parte izquierda de la pantalla.

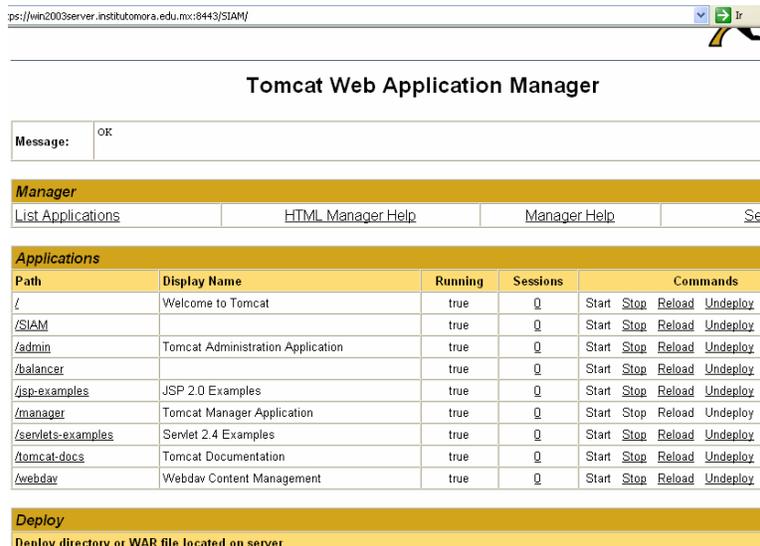


5. En ese momento se muestra una ventana para conectarse al servidor.
6. El login es slazarini, y el password lags730201.

**Tipo de Documento:** Contingencia  
**Objetivo:** Administrar el servidor de aplicaciones TOMCAT para el Sistema de Información Académica del Mora (SIAM) y Sistema de Información de Seguimiento de Egresados (SISEM)  
**Fecha de Elaboración:** Junio 2004  
**Última actualización:** Julio 2008  
**Elaboró:** Silvia Lazarini Gutiérrez  
**Revisó:** Enrique Ayala Covarrubias



7. Posteriormente se muestra una ventana donde están las aplicaciones en forma de tabla.
8. El SIAM en específico al momento de tener en la columna de running TRUE quiere decir que está funcionando.
9. Para detener la aplicación, en la columna de Commands se debe dar un clic en STOP. (En ese momento la aplicación está fuera de servicio).
10. Para que la aplicación vuelva a estar en servicio, se debe orprimir Start, (en ese momento la aplicación regresa a estar en línea



**Tipo de Documento:** Contingencia  
**Objetivo:** Administrar el servidor de aplicaciones TOMCAT para el Sistema de Información Académica del Mora (SIAM) y Sistema de Información de Seguimiento de Egresados (SISEM)  
**Fecha de Elaboración:** Junio 2004  
**Última actualización:** Julio 2008  
**Elaboró:** Silvia Lazarini Gutiérrez  
**Revisó:** Enrique Ayala Covarrubias

11. Para verificar que la aplicación está en servicio, en la columna de PATH se debe dar un clic a SIAM.



12. En ese momento se puede acceder a SIAM, se puede probar accediendo a los módulos de administración del sistema, Dictámenes o Reportes. Los passwords se deben solicitar a las personas responsables de cada módulo:
- Captura de datos académicos: Silvia Juárez, Coordinación de Investigación, Plaza, ext. 1165
  - Administración del sistema: Silvia Juárez, Coordinación de Investigación, Plaza, ext. 1165
  - Reportes: Jazmín Zamora Asist. Dir. Investigación ext. 1162 Dictámenes: Jazmín Zamoral Asist. Dir. De Investigación ext. 1162

**Tipo de Documento:** Contingencia  
**Objetivo:** Actualización de versiones del Sistema de Información Académica del Mora (SIAM) y Sistema de Seguimiento de Egresados del Mora (SISEM)  
**Fecha de Elaboración:** Junio 2004  
**Última actualización:** Julio 2008  
**Elaboró:** Silvia Lazarini Gutiérrez  
**Revisó:** Enrique Ayala Covarrubias

La Base de datos del SIAM se encuentra en el servidor IMDBPLAZA.  
La Aplicación se encuentra en el TOMCAT del Servidor IMDBPLAZA.

1. Correr procedimiento para suspender la aplicación. Ver docto. "admin\_tomcat.doc"
2. Cerrar el cuadro de símbolo de sistema de TOMCAT.
3. Respalidar en un archivo Zip, la aplicación anterior ubicada en C:\TOMCAT\webapps\SIAM
4. Ya que está respaldado, hay que renombrar un archivo llamado "SIAMserver.ini" ubicado en C:\TOMCAT\webapps\SIAM (este archivo contiene la configuración para envío de correo electrónico).
5. Descargar la aplicación en C:\TOMCAT\webapps\SIAM en ese momento se descarga la nueva versión
6. Ya que está lista la versión, al archivo hay que sustituir el Archivo SIAMserver.ini nuevo, por el que habíamos renombrado anteriormente, ya que el que viene con la aplicación trae la configuración de LANIA, y el otro contiene la nuestra.
7. Concluidos estos pasos, se inicia el archivo startup.bat ubicado en el escritorio del equipo.
8. Posteriormente se hace el procedimiento para levantar la aplicación, descrito en el archivo "admin\_tomcat.doc"
  1. Si se necesitara correr algún script, que altere la Base de datos, hay que hacer un export de la base de datos, en símbolo de sistema ejecutar la siguiente sintaxis: exp username/password@"nombre de la instancia" <enter>
  2. Acceder a la base de datos vía la Consola de Oracle.
  3. Acceder en modo standalone, al servicio MORA\_IMDBPLAZA.institutomora.edu.mx con el usuario system password mora
  4. Ya estando conectados de lado izquierdo se muestra una barra de herramientas, elegir el tercer icono de abajo que dice database applications, es el que tiene un muñequito con una tabla de check list. Ahí se desplegará otro conjunto de íconos y hay que seleccionar el que trae una hoja de SQL con un lápiz.
  5. Se mostrará una ventana de símbolo de comando y atrás el SQL \*plus Worksheet. Hay que conectarnos con el usuario sys pass admin. y seleccionar el icono de rayo que viene de lado izquierdo el cual indica que se ejecuta el comando.
  6. Posteriormente se corre el script que indique LANIA especificando la ruta
  7. por ej. @ C:\TOMCAT\webapps\siam\scripts\scriptx.sql; y presionar el icono de lado derecho con el dibujo de rayo para que ejecute el comando.
  8. Al terminar de correr los scripts en menú, seleccionamos file exit, así salimos de sql \*plus worksheet. Y cerramos la ventana.

**Tipo de Documento:** Contingencia  
**Actualización de versiones del Sistema de Información Académica del Mora (SIAM) y Sistema de Seguimiento de Egresados del Mora (SISEM)**

**Objetivo:** Académica del Mora (SIAM) y Sistema de Seguimiento de Egresados del Mora (SISEM)

**Fecha de Elaboración:** Junio 2004

**Última actualización:** Julio 2008

**Elaboró:** Silvia Lazarini Gutiérrez

**Revisó:** Enrique Ayala Covarrubias

9. Después nos desconectamos de la instancia (MORA\_IMDBPLAZA.institutomora.edu.mx), seleccionando y dando clic con botón derecho y seleccionando la opción disconnect.
10. Y salimos de la consola de Oracle
11. Y se procede a utilizar el archivo "admin\_tomcat.doc" en donde se describe como levantar la aplicación en el TOMCAT manager, para que esté disponible para todo usuario.

## INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA

---

El Pleno del Instituto Federal de Acceso a la Información Pública, con fundamento en lo dispuesto por los artículos 37 fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2 fracción V de su Reglamento, y el Trigésimo Octavo y Quinto Transitorio de los Lineamientos de protección de datos personales, y:

### CONSIDERANDO:

Que es atribución del Instituto Federal de Acceso a la Información Pública establecer las recomendaciones sobre las políticas generales para el manejo, mantenimiento, seguridad y protección de datos personales, que estén en posesión de las dependencias y entidades de la Administración Pública Federal;

Que es necesario promover la adopción de las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, con base en estándares de seguridad internacionales;

Que para lograr lo anterior, es necesario tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya sea que provengan de la acción humana o de las condiciones físicas y ambientales, por lo que se han establecido distintos niveles de seguridad aplicables a cada categoría o tipo de datos, alojados en los sistemas de datos personales;

Que los alcances de estas recomendaciones son los de convertirse en propuestas y sugerencias específicas para lograr la mayor protección de los datos personales, por lo que las dependencias y entidades podrán utilizarlas como modelo a seguir, para lograr con ello un estándar de seguridad, sin perjuicio de que éstas establezcan medidas adicionales que coadyuven a la mejor protección mencionada, ha tenido a bien expedir las siguientes:

# RECOMENDACIONES SOBRE MEDIDAS DE SEGURIDAD APLICABLES A LOS SISTEMAS DE DATOS PERSONALES

---

## Contenido

Contenido .....	2
I. Instructivo .....	4
II. Niveles de Seguridad .....	4
III. Abreviaturas .....	6
IV. Definiciones .....	6
Recomendaciones .....	9
1. Medidas de seguridad para datos personales en soportes físicos .....	9
1.1. Área de recepción de datos personales .....	9
1.2. Área de resguardo de datos personales .....	9
1.3. Área de consulta de datos personales .....	10
1.4. Acceso y consulta de datos personales .....	11
1.5. Registro de actividades .....	12
1.6. Baja de datos personales .....	14
2. Medidas de Seguridad para datos personales en soportes electrónicos .....	16
2.1. Área de recepción de datos personales .....	16
2.2. Área de resguardo de datos personales .....	16
2.3. Área de consulta de datos personales .....	18
2.4. Acceso y consulta de datos personales .....	19
2.5. Registro de actividades .....	20
2.6. Baja de datos personales .....	21
3. Medidas de Seguridad para transmisión de datos personales .....	21
3.1. Transmisión de datos personales en soportes físicos .....	21
3.2. Transmisión de datos personales en soportes electrónicos .....	21
3.3. Registro de actividades .....	21
4. Medidas de Seguridad para equipo de cómputo en zonas de acceso restringido .....	21
4.1. Computadoras de escritorio .....	21
4.2. Servidores .....	21
4.3. Impresoras y otros equipos periféricos autorizados .....	21
4.4. Registro de actividades e inventario .....	21
4.5. Equipo no autorizado .....	21
5. Medidas de Seguridad para asegurar continuidad y enfrentar desastres .....	21
5.1. Respaldo y recuperación de sistemas de datos personales automatizados .....	21
5.2. Operación continua de sistemas de datos personales automatizados .....	21
5.3. Registro de actividades .....	21
6. Documentación de medidas de seguridad en procesos y políticas del sistema de protección de datos personales .....	21
6.1. Manual de operaciones .....	21
6.2. Sensibilización y capacitación .....	21
6.3. Cartas compromiso, cláusulas y contratos de confidencialidad .....	21

## I. Instructivo

El presente documento es un instrumento técnico de apoyo en materia de medidas de seguridad aplicables a los sistemas de datos personales tanto físicos como automatizados, en posesión de las dependencias y entidades de la Administración Pública Federal.

Las medidas de seguridad se redactan a manera de atributos, lo cual permite utilizar cada sección como una lista de verificación, a fin de facilitar la evaluación, implementación y supervisión de dichas medidas.

De esta forma, los responsables de uno o más sistemas de datos personales podrán determinar con facilidad si cuentan o no con la infraestructura, los procesos y los procedimientos para cumplir con las medidas de seguridad recomendadas por este documento.

Asimismo, el formato que sigue la presentación de las medidas de seguridad, permite que el responsable pueda utilizar solamente los apartados de Recomendaciones que resulten aplicables por el nivel de protección de los datos personales y el tipo de sistema. Es decir, quienes realicen el tratamiento de datos personales en soportes físicos podrán utilizar solamente el apartado que hace referencia a este tipo de soportes y dentro de ese apartado, únicamente las medidas correspondientes al nivel de protección que corresponda, por consiguiente, podrán omitir la revisión de otros apartados que no resulten aplicables.

## II. Niveles de Seguridad

Tomando en cuenta los criterios internacionales establecidos en los reglamentos sobre medidas de seguridad para el resguardo eficaz de los datos personales, al final de cada medida sugerida se establecen niveles de seguridad, las cuales deberán observarse atendiendo a la naturaleza de la información contenida en los sistemas de datos personales.

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales. Por lo tanto, las dependencias y entidades aplicarán el nivel básico, medio o alto de medidas de seguridad, de acuerdo con las categorías o tipos de datos personales que se detallan a continuación:

### A. Nivel básico

Las medidas de seguridad marcadas con el nivel básico serán aplicables a todos los sistemas de datos personales.

A los sistemas de datos personales que contienen alguno de los datos que se enlistan a continuación, les resultan aplicables únicamente, las medidas de seguridad de **nivel básico**:

- **De Identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de

nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.

- **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.

## **B. Nivel medio**

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas con nivel medio.

- **Datos Patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
- **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales:** Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
- **Datos Académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
- **Transito y movimientos migratorios:** Información relativa al transito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

## **C. Nivel alto**

Los sistemas de datos personales que contengan alguno de los datos que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las marcadas con nivel alto.

- **Datos Ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
- **Datos de Salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
- **Características personales:** Tipo de sangre, ADN, huella digital, u otros análogos.
- **Características físicas:** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.
- **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros.
- **Origen:** Étnico y racial.

### III. Abreviaturas

**MS.** Medidas de seguridad.

**SDP.** Sistema de datos personales.

**SDPs.** Sistemas de datos personales.

### IV. Definiciones

Para efectos de la aplicación de las presentes Recomendaciones, además de las definiciones contenidas en el Artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en el Diario Oficial de la Federación el 11 de junio de 2002, en el Artículo 2 de su Reglamento, publicado en el mismo Diario el 11 de junio de 2003, y en el Lineamiento Tercero de los Lineamientos de Protección de Datos Personales expedidos por el Instituto y publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005, se entenderá por:

**I. Área de consulta de datos personales:** El espacio destinado para que el personal autorizado examine aquellos datos personales que están autorizados a consultar, sin posibilidad de modificar su contenido.

**II. Área de recepción de datos personales:** El espacio donde se reciben datos personales en cualquier tipo de soporte (físico, electrónico, o ambos) en tanto se siguen las demás fases de su tratamiento para integrarlos a uno o más SDPs.

**III. Área de resguardo de datos personales:** El espacio para almacenar datos personales que han recibido el tratamiento correspondiente para que formen parte integral de uno o más SDPs, sin importar el soporte (físico, electrónico, o ambos) utilizado para su almacenamiento.

**IV. Divulgación de incidentes:** Las acciones que adoptan el Titular de la dependencia o entidad y el Responsable de los SDPs, a efecto de dar a conocer a las autoridades competentes, a los titulares de los datos y, en su caso, al público en general, los actos deliberados (*intrusión*, robo, etc.), los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), que hubieran ocasionado la pérdida total o parcial de los datos personales bajo su custodia.

**V. Intrusión:** Acción que una o más personas realizan para introducirse, sin derecho, en uno o más SDPs a fin de alterar, copiar o sustraer datos personales que forman parte de esos sistemas.

**VI. Malware:** Software malicioso o maligno utilizado por personas para causar daños en una o más computadoras o para sustraer archivos de los equipos; es decir, virus, gusanos cibernéticos, caballos de Troya, "spyware", "bots" y "rootkits", y los que se creen posteriormente con el mismo propósito.

**VII. Manual de operaciones:** Conjunto de documentos que enumeran, definen y detallan los procesos y procedimientos que los servidores públicos llevan a cabo dentro de una dependencia o entidad.

**VIII. Personal o Personal autorizado:** Los usuarios o encargados (servidores públicos) que han recibido autorización para interactuar con uno o más SDPs por parte del Responsable de dichos sistemas.

**IX. Personal de sistemas:** El personal que labora en el área de tecnologías de información, *sistemas*., telecomunicaciones u otras análogas.

**X. Soportes electrónicos:** Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs),

discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.

**XI. Soportes físicos:** Medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, formularios impresos llenados "a mano" o "a máquina", fotografías y placas radiológicas, entre otros.

**XII. Supervisión interna:** Proceso sistemático mediante el cual se realiza la recopilación, acumulación y evaluación de evidencia sobre la adopción y práctica de las MS recomendadas en este documento por una dependencia o entidad. Sus propósitos son precisar e informar el grado de cumplimiento entre la información recabada y los criterios establecidos.

**XIII. Zona de acceso restringido:** Todas aquellas áreas a las que sólo tienen acceso el personal autorizado y el personal de vigilancia; es decir, el área de recepción, el área de resguardo y el área de consulta de datos personales.

## Recomendaciones

### 1. MS para datos personales en soportes físicos

#### 1.1. Área de recepción de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales recibidos en el área de recepción, en tanto siguen las demás fases de su tratamiento. [Nivel básico]
2. El personal autorizado que labora en el área de recepción ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
3. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de recepción gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
4. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de recepción conforme se van presentando cambios de personal. [Nivel medio]
5. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “4.5. Equipo no autorizado” dentro del área de recepción. [Nivel medio]
6. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de recepción. [Nivel básico]

#### 1.2. Área de resguardo de datos personales

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales en soportes físicos dentro del área de resguardo. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de resguardo, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. Al interior del área de resguardo, existen las condiciones ambientales idóneas para preservar en buen estado los datos personales en soportes físicos durante el tiempo de conservación. [Nivel básico]
4. La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel básico]
5. El mobiliario utilizado dentro del área de resguardo protege los datos personales en soportes físicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas, entre otras. [Nivel básico]
6. El mobiliario utilizado para almacenar los datos personales en soportes físicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles. [Nivel medio]

7. El personal autorizado que labora en el área de resguardo ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
8. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de resguardo gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
9. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de resguardo conforme se presentan cambios de personal. [Nivel medio]
10. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “4.5. Equipo no autorizado” dentro del área de resguardo. [Nivel medio]
11. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo. [Nivel básico]

### **1.3. Área de consulta de datos personales**

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible supervisar y vigilar los datos personales en soportes físicos que consultan los Usuarios de los datos dentro del área de consulta. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de consulta, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. La puerta de acceso del área de consulta cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel medio]
4. El personal autorizado que labora en el área de consulta ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
5. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de consulta gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
6. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de consulta conforme se presentan cambios de personal. [Nivel medio]
7. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “4.5. Equipo no autorizado” dentro del área de consulta. [Nivel medio]
8. Existe señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de consulta. [Nivel básico]

### **1.4. Acceso y consulta de datos personales**

#### **1.4.1. Acceso**

1. Existen puntos de revisión en la dependencia o entidad en donde el personal de vigilancia controla el acceso y verifica la identidad de quienes tienen el propósito de ingresar a una zona de acceso restringido. [Nivel básico]
2. El personal que tienen intención de ingresar a una zona de acceso restringido se registra y entrega una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión. [Nivel medio]

3. El Encargado de los SDPs es el único que autoriza la entrada al área de recepción y al área de resguardo al personal debidamente registrado, anotando el hecho como se explica en la sección “1.5. Registro de actividades”. [Nivel básico]
4. En todo caso, la dependencia o entidad adopta las medidas de seguridad necesarias para el ingreso a una zona de acceso restringido.

#### **1.4.2. Consulta**

1. El usuario consulta los datos personales en soportes físicos dentro del área de consulta. [Nivel alto]
2. El Encargado de los SDPs al autorizar la salida de datos personales en soportes electrónicos o en soportes físicos, anota el hecho como se explica en la sección “1.5. Registro de actividades”. [Nivel básico]

#### **1.4.3. Personas autorizadas y no autorizadas**

1. El ingreso a las zonas de acceso restringido donde existen datos personales en soportes físicos es sólo con la autorización del Encargado de los SDPs. [Nivel básico]
2. Cada acceso y consulta realizada por personas no autorizadas es considerada como un incidente de intrusión que se denuncia ante las autoridades competentes para su investigación. [Nivel medio]

#### **1.4.4. Medidas para la prevención de intrusiones**

1. El personal autorizado que labora en las zonas de acceso restringido de los SDPs verifica durante el desempeño de sus funciones que en dichas áreas no hay personas no autorizadas. [Nivel básico]
2. Además, el personal de vigilancia realiza funciones de forma permanente en las zonas de acceso restringido de los SDPs. [Nivel medio]
3. Las zonas de acceso restringido cuentan con un sistema de vídeo-vigilancia remota que permite vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opere las 24 horas, los 7 días de la semana (24x7) y un archivo que acumula grabaciones de los dos meses anteriores. [Nivel alto]
4. En caso de ocurrir un incidente de intrusión, el personal de vigilancia acude de inmediato a la zona de acceso restringido presuntamente violada para corroborar el hecho. De comprobarse este, la grabación realizada por el sistema de vídeo-vigilancia remota se transfiere a un soporte físico para que pueda ser utilizado como prueba por las autoridades que investiguen el caso. [Nivel alto]

### **1.5. Registro de actividades**

#### **1.5.1. Operación cotidiana**

1. El Responsable de los SDPs mantiene estricto control y registro de:
  - a) Las autorizaciones emitidas para facultar a un servidor público como usuario para interactuar con uno o más SDPs, ya sea que dicho servidor público lo haga acudiendo al área de consulta o desde otro lugar distinto, fuera de dicha área. [Nivel básico]

- b) La asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios para que éstos puedan abrir los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido. [Nivel básico]
  - c) Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que solicitan acceso a las áreas de recepción o resguardo. Para ello, el Encargado anota
    - Quién solicita el acceso
    - Cuándo lo solicita
    - Cuándo se lleva a cabo
    - La razón que lo motiva [Nivel básico]
  - d) Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes físicos del área de consulta. Para ello, el Encargado anota
    - Quién hace la solicitud
    - Qué documentos se lleva
    - Cuándo se los lleva
    - Cuándo promete devolverlos (si aplica)
    - Cuándo efectivamente los devuelve (si aplica)
    - Por qué necesita llevárselos [Nivel medio]
  - e) Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos tales como los mencionados en la sección “4.5. Equipo no autorizado”. Para ello, el Encargado anota
    - Quién hace la solicitud
    - Qué equipo introducirá
    - Cuándo y por cuánto tiempo
    - Por qué necesita introducirlo [Nivel medio]
2. El sistema de vídeo-vigilancia remoto registra las actividades diarias así como los incidentes en las zonas de acceso restringido. [Nivel alto]

### **1.5.2. Divulgación de incidentes**

1. En caso de presentarse un incidente, se sigue el procedimiento que la dependencia o entidad tenga definido. [Nivel básico]

En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:

2. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
3. En caso de robo o extravío de datos personales en soportes físicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querrelas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]

4. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
5. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

### **1.5.3. Supervisión**

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDPs. [Nivel básico]

## **1.6. Baja de datos personales**

Para proceder a la baja documental de soportes físicos que contienen datos personales, deberán observarse las disposiciones establecidas por el Capítulo III De la Conservación de Archivos, de los Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal (DOF 20/02/04), y además:

1. El Encargado de los SDPs:
  - a) Sigue procedimientos y utiliza mecanismos para asegurar la valoración y en su caso, destrucción de soportes físicos que contienen datos personales. [Nivel medio]
  - b) Destruye por completo dichos soportes físicos antes de desecharlos [Nivel básico]
  - c) Lleva una bitácora de las veces que se efectúa la acción de baja de datos personales. [Nivel básico]
2. Los métodos de destrucción de datos personales en soportes físicos están definidos en el Manual de operaciones de la dependencia o entidad; o, si no lo están, son aprobados por el Responsable de los SDPs antes de ejecutarlos. [Nivel básico]
3. Si en esa dependencia o entidad realizan la separación de materiales para su reciclaje (como podría suceder con el papel, el cartón, el metal y el plástico), los datos personales contenidos en materiales reciclables son triturados y la viruta resultante se entrega directamente a una empresa que los recibe para procesarlos de inmediato, garantizando por escrito que no serán examinados para su eventual reconstrucción. [Nivel medio]

## **2. MS para datos personales en soportes electrónicos**

### **2.1. Área de recepción de datos personales**

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales recibidos en el área de recepción, en tanto siguen la demás fases de su tratamiento. [Nivel básico]
2. El equipo de cómputo instalado en el área de recepción cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido”. [Nivel básico]
3. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de recepción. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda a la recepción de datos personales. [Nivel medio]
4. El personal autorizado que labora en el área de recepción ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
5. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de recepción gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
6. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de recepción conforme se van presentando cambios de personal. [Nivel medio]
7. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “4.5. Equipo no autorizado” dentro del área de recepción. [Nivel medio]
8. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de recepción. [Nivel básico]

### **2.2. Área de resguardo de datos personales**

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible mantener en forma organizada y segura los datos personales en soportes electrónicos dentro del área de resguardo. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de resguardo, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. Al interior del área de resguardo, existen las condiciones ambientales idóneas para preservar en buen estado los datos personales en soportes electrónicos durante el tiempo de conservación. [Nivel básico]
4. La puerta de acceso del área de resguardo cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel básico]
5. El equipo de cómputo instalado en el área de resguardo cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido”. [Nivel básico]

6. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de resguardo. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales. [Nivel medio]
7. El mobiliario utilizado dentro del área de resguardo protege los datos personales en soportes electrónicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas, entre otras. [Nivel básico]
8. El mobiliario utilizado para almacenar los datos personales en soportes electrónicos cuenta con cerraduras, dispositivos electrónicos o cualquier otra tecnología que impida la libre apertura de sus puertas, cajones o compartimientos. Tales mecanismos quedan cerrados en horas no hábiles. [Nivel básico]
9. El personal autorizado que labora en el área de resguardo ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
10. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de resguardo gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]
11. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de resguardo conforme se presentan cambios de personal. [Nivel medio]
12. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “4.5. Equipo no autorizado” dentro del área de resguardo. [Nivel básico]
13. Existe señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo. [Nivel básico]

### **2.3. Área de consulta de datos personales**

1. Existe la infraestructura apropiada —y se siguen los procesos y procedimientos necesarios y suficientes— de tal manera que es posible supervisar y vigilar los datos personales en soportes electrónicos que consultan los Usuarios de los datos dentro del área de consulta. [Nivel básico]
2. De existir ventanas o muros divisorios transparentes en el área de consulta, la visión está obstruida mediante una película translúcida (papel albanene, por ejemplo). [Nivel medio]
3. La puerta de acceso del área de consulta cuenta con cerradura, dispositivo electrónico o cualquier otra tecnología que impida su libre apertura. Este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área. [Nivel medio]
4. El equipo de cómputo instalado en el área de consulta cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido”. [Nivel básico]
5. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en el área de consulta. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda al resguardo de datos personales. [Nivel medio]
6. El usuario que labora en el área de consulta ostenta una identificación con fotografía (credencial o gafete) emitida por la dependencia o entidad. [Nivel básico]
7. Cualquier persona puede identificar con facilidad al personal autorizado que labora en el área de consulta gracias a que los nombres completos y fotografías de dicho personal se exhiben en un lugar visible dentro y fuera de dicha área. [Nivel medio]

8. El Encargado de los SDPs actualiza los nombres completos y fotografías que se exhiben en el área de consulta conforme se presentan cambios de personal. [Nivel medio]
9. No está permitido el libre acceso y el uso de aquellos aparatos referidos en la sección “4.5. Equipo no autorizado” dentro del área de consulta. [Nivel medio]
10. Existe señalización visible sobre: horarios de atención, restricciones de acceso, prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de consulta. [Nivel básico]

## **2.4. Acceso y consulta de datos personales**

### **2.4.1. Acceso**

1. Existen puntos de revisión en la dependencia o entidad en donde el personal de vigilancia controla el acceso y verifica la identidad de quienes tienen el propósito de ingresar a una zona de acceso restringido. [Nivel básico]
2. El personal que tienen intención de ingresar a una zona de acceso restringido se registra y entrega una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) al personal de vigilancia que atiende dicho punto de revisión. [Nivel medio]
3. El Encargado de los SDPs es el único que autoriza la entrada al área de recepción y al área de resguardo al personal debidamente registrado, anotando el hecho como se explica en la sección “2.5. Registro de actividades”. [Nivel básico]
4. En todo caso, la dependencia o entidad adopta las medidas de seguridad necesarias para el ingreso a una zona de acceso restringido.

### **2.4.2. Consulta**

1. El usuario consulta los datos personales en soportes electrónicos dentro del área de consulta. [Nivel medio]
2. El Encargado de los SDPs al autorizar la salida de datos personales en soportes electrónicos o en soportes físicos, anota el hecho como se explica en la sección “2.5. Registro de actividades”. [Nivel básico]

### **2.4.3. Personas autorizadas y no autorizadas**

1. El ingreso a las zonas de acceso restringido donde existen datos personales en soportes electrónicos es sólo con la autorización del Responsable de los SDPs. [Nivel básico]
2. Cada acceso y consulta realizada por personas no autorizadas es considerada como un incidente de intrusión que se denuncia ante las autoridades competentes para su investigación. [Nivel básico]

### **2.4.4. Medidas para la prevención de intrusiones**

1. El personal autorizado que labora en las zonas de acceso restringido de los SDPs verifica durante el desempeño de sus funciones que en dichas áreas no hay personas no autorizadas. [Nivel básico]
2. Además, el personal de vigilancia realiza funciones de forma permanente en las zonas de acceso restringido de los SDPs. [Nivel medio]

3. El equipo de cómputo instalado en las zonas de acceso restringido cumple con las Recomendaciones presentadas en la sección “4. MS para equipo de cómputo en zonas de acceso restringido”. [Nivel básico]
4. Dicho equipo de cómputo está provisto de la tecnología necesaria y suficiente para verificar la identidad del usuario que labora en estas zonas y que utiliza tal equipo. Ello implica que, mediante la verificación de claves de acceso, dicho usuario accede al equipo para interactuar con el o los SDPs que tiene autorizados. [Nivel medio]
5. Las zonas de acceso restringido cuentan con un sistema de vídeo-vigilancia remota que permite vigilar la puerta de acceso y el interior de dichas áreas. Dicho sistema cuenta con cámaras para visión nocturna, un sistema de grabación que opere las 24 horas, los 7 días de la semana (24x7) y un archivo que acumula grabaciones de los dos meses anteriores. [Nivel alto]
6. En caso de ocurrir un incidente de intrusión, el personal de vigilancia acude de inmediato a la zona de acceso restringido presuntamente violada para corroborar el hecho. De comprobarse este, la grabación realizada por el sistema de vídeo-vigilancia remota se transfiere a un soporte físico para que pueda ser utilizado como prueba por las autoridades que investiguen el caso. [Nivel alto]

## **2.5. Registro de actividades**

### **2.5.1. Operación cotidiana**

1. El Responsable de los SDPs mantiene estricto control y registro de:
  - a) Las autorizaciones emitidas para facultar a un servidor público como usuario para interactuar con uno o más SDPs, ya sea que dicho servidor público lo haga acudiendo al área de consulta o desde otro lugar distinto, fuera de dicha área. [Nivel básico]
  - b) La asignación, actualización y reemplazo de llaves, tarjetas, contraseñas de acceso y demás elementos que entregue a los usuarios para que éstos pueda abrir los mecanismos de apertura de puertas y mobiliario en las zonas de acceso restringido. [Nivel básico]
  - c) Las autorizaciones emitidas a los usuarios y demás personal debidamente registrado que solicitan acceso a las áreas de recepción o resguardo. Para ello, el Encargado anota
    - Quién solicita el acceso
    - Cuándo lo solicita
    - Cuándo se lleva a cabo
    - La razón que lo motiva [Nivel básico]
  - d) Las autorizaciones emitidas a los usuarios que solicitan permiso para extraer datos personales en soportes electrónicos del área de consulta. Para ello, el Encargado anota
    - Quién hace la solicitud
    - Qué documentos se lleva y en qué tipo de soporte (físico o electrónico)
    - Cuándo se los lleva
    - Cuándo promete devolverlos (si aplica)
    - Cuándo efectivamente los devuelve (si aplica)
    - Por qué necesita llevárselos [Nivel medio]
- b) Las autorizaciones emitidas a los usuarios que solicitan permiso para introducir a las zonas de acceso restringido aparatos tales como los mencionados en la sección “4.5. Equipo no autorizado”. Para ello, el Encargado anota

- Quién hace la solicitud
  - Qué equipo introducirá
  - Cuándo y por cuánto tiempo
  - Por qué necesita introducirlo [Nivel medio]
7. El sistema de vídeo-vigilancia remota registra las actividades diarias así como los incidentes en las zonas de acceso restringido. [Nivel alto]

### **2.5.2. Divulgación de incidentes**

5. En caso de presentarse un incidente, se sigue el procedimiento que la dependencia o entidad tenga definido. [Nivel básico]

En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:

6. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
7. En caso de robo o extravío de datos personales en soportes electrónicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querrelas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
8. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
9. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

### **2.5.3. Supervisión**

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDPs así como para los terceros contratados que interactúan con dichos SDPs. [Nivel básico]

## **2.6. Baja de datos personales**

Para proceder a la baja documental de soportes electrónicos que contienen datos personales, deberán observarse las disposiciones establecidas por el Capítulo III De la Conservación de Archivos, de los Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal (DOF 20/02/04), y además:

1. Todo soporte electrónico que será dado de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final antes de ser desechado. Dicho proceso incluye: la transferencia del contenido que sea preciso conservar hacia otro soporte electrónico y la destrucción, inhabilitación o daño que deje inservible dicho soporte. [Nivel básico]
2. Las únicas personas autorizadas para realizar proceso de preparación final son el área de sistemas y el personal de vigilancia. [Nivel básico]
3. Los métodos de destrucción de datos personales en soportes electrónicos están definidos en el Manual de operaciones de los SDPs; o, si no lo están, son aprobados por el Responsable de los SDPs antes de ejecutarlos. [Nivel básico]
4. El Encargado de los SDPs:
  - a) Vigila que se sigan los procedimientos y se utilicen los mecanismos para asegurar la destrucción de soportes electrónicos que contienen datos personales. [Nivel básico]
  - b) Lleva una bitácora donde registra la baja de soportes electrónicos que contienen datos personales anotando
    - Nombre y firma de la persona que realiza esta acción
    - Fecha y hora en la que se realiza
    - El destino que se le dará al soporte electrónico desechado
    - Nombre y firma (visto bueno) del Responsable de los SDPs [Nivel básico]

## **3. MS para transmisión de datos personales**

### **3.1. Transmisión de datos personales en soportes físicos**

#### **3.1.1. Transmisión mediante traslado físico**

1. La transmisión de datos personales en soportes físicos al interior de la dependencia o entidad se realiza mediante la vía elegida, de común acuerdo, entre las partes: mensajero interno, asistente secretarial, visita personal, etc. [Nivel básico]
2. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero. [Nivel medio]
3. El paquete con datos personales en soportes físicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo. [Nivel básico]
4. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. [Nivel medio]
5. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, es imperativo que el mensajero regrese dicho paquete al transmisor. [Nivel medio]
6. El Responsable de los SDPs verifica que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente. [Nivel medio]

### **3.2. Transmisión de datos personales en soportes electrónicos**

#### **3.2.1. Preparación previa a la transmisión**

1. Los datos personales que son enviados a un destinatario autorizado para manipularlos o procesarlos son sometidos a un proceso de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso:
  - Genera archivos electrónicos que contengan los datos personales solicitados en un formato que permita al destinatario efectuar las operaciones que requiera [Nivel básico]
  - Somete dichos archivos a un proceso de encriptación que los proteja durante su trayecto aplicando un nivel de encriptación ALTO, no menor a 1024 bits [Nivel medio]
2. Los datos personales que son enviados a un destinatario con autorización para manipularlos o procesarlos no son reintegrados al SDP de donde fueron extraídos, a menos que el destinatario haya efectuado una corrección solicitada por el titular de los datos. [Nivel básico]
3. Los datos personales que son enviados a un destinatario No autorizado para manipularlos o procesarlos son sometidos a un proceso distinto de preparación previa a la transmisión. En este caso, el encargado que realiza dicho proceso:
  - Genera archivos electrónicos que contengan los datos personales solicitados en un formato protegido, de manera que el destinatario pueda examinar su contenido pero no pueda editarlo, copiarlo ni imprimirlo [Nivel medio]

- Somete los archivos resultantes a un proceso de encriptación que proteja los archivos durante su trayecto aplicando un nivel de encriptación MEDIO, no menor a 512 bits [Nivel medio]

### **3.2.2. Transmisión mediante traslado físico**

1. La transmisión de datos personales en soportes electrónicos al interior de la dependencia o entidad se realiza mediante la vía elegida, de común acuerdo, entre las partes: mensajero interno, asistente secretarial, visita personal, etc. [Nivel básico]
2. La transmisión al exterior se realiza mediante un servicio de mensajería externo. En este caso, se define un destinatario primario y otro secundario por si el mensajero no encuentra al primero. [Nivel medio]
3. El paquete con datos personales en soportes electrónicos viaja debidamente sellado, de forma tal que sea perceptible cualquier violación o apertura no autorizada del mismo. Dichos soportes electrónicos contienen los archivos electrónicos resultantes del proceso de preparación previa a la transmisión. [Nivel básico]
4. La entrega del paquete se realiza sólo si el destinatario acredita su identidad. Para ello, el destinatario presenta una identificación oficial con fotografía (credencial de elector, pasaporte, etc.) y el mensajero recaba nombre, firma y un número de referencia que aparezca en tal identificación además de la fecha de entrega. [Nivel medio]
5. El mensajero no entrega el paquete si el destinatario no puede acreditar su identidad. En este caso, es imperativo que el mensajero regrese dicho paquete al transmisor. [Nivel medio]
6. El Encargado de los SDPs verifica que el mensajero entregó el paquete al destinatario. Si el transmisor detecta que dicho paquete fue entregado a otra persona, da inicio al proceso de atención de un incidente. [Nivel medio]

### **3.2.3. Transmisión mediante redes de comunicación electrónica**

1. La transmisión de datos personales en archivos electrónicos, previamente preparados para su transmisión, se realiza mediante redes de comunicación electrónica. [Nivel básico]
2. El transmisor recaba por escrito acuse de recibo del destinatario, ya sea por correo electrónico o mediante oficio enviado por fax. [Nivel medio]

### **3.2.4. Medidas para la prevención de intrusiones desde el exterior**

1. Existen dispositivos de alta seguridad instalados en caso de que la red de comunicación electrónica (que conecta los servidores que contienen los datos personales con las computadoras que se utilizan para acceder a ellos) esté conectada a Internet.

Los dispositivos instalados incluyen sistemas de protección perimetral (cortafuegos), de detección de intrusos, filtros de contenido, de prevención de intrusiones y de análisis de protocolos. [Nivel alto]

2. Se aplican las medidas necesarias y suficientes para que los puntos de acceso inalámbrico a la red de comunicación electrónica de la dependencia o entidad sean seguros y no existan huecos que puedan ser aprovechados por intrusos. [Nivel medio]
3. Las recomendaciones presentadas en la sección "4. MS para equipo de cómputo en zonas de acceso restringido" aplican en esta sección. [Nivel medio]

4. El personal de sistemas mantiene actualizada la memoria técnica de la red de comunicación electrónica con el fin de identificar los equipos inicialmente configurados y puestos a disposición del personal autorizado para interactuar los SDPs. [Nivel medio]
5. Si un equipo de cómputo queda en manos de una persona no autorizada o si es dado de baja, se utiliza la memoria técnica mencionada para cancelar la configuración del equipo en cuestión. [Nivel medio]
6. El personal de vigilancia o el Encargado de los SDPs, en coordinación con el área de sistemas, realiza de manera periódica y en forma programada análisis de vulnerabilidades y pruebas de intrusión controladas en la infraestructura de cómputo, almacenamiento y comunicaciones. El propósito de esta actividad es aplicar las medidas correctivas necesarias a fin de cerrar las vulnerabilidades encontradas y así evitar posibles incidentes de intrusión. [Nivel medio]

### **3.3. Registro de actividades**

#### **3.3.1. Operación cotidiana**

1. El Encargado de los SDPs mantiene estricto control y registro de:
  - a) Las autorizaciones emitidas a destinatarios que han solicitado que los datos personales en soportes electrónicos les sean transmitidos en un formato que permita manipularlos o procesarlos. [Nivel básico]
  - b) Todas las transmisiones efectuadas, para ello, anota los datos necesarios para emitir informes sobre la transmisión según el lineamiento vigésimo sexto de los Lineamientos de Protección de Datos Personales publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005. [Nivel básico]

#### **3.3.2. Divulgación de incidentes**

1. En caso de presentarse un incidente, se sigue el procedimiento que esa dependencia o entidad tenga definido. [Nivel básico]

En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:

2. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
3. En caso de robo o extravío de datos personales en soportes físicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querrelas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
4. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
5. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el

Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

### **3.3.3. Supervisión**

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión a las unidades administrativas que mantienen y operan SDPs así como a los terceros contratados. [Nivel básico]

## **4. MS para equipo de cómputo en zonas de acceso restringido**

### **4.1. Computadoras de escritorio**

#### **4.1.1. Recepción**

1. Una computadora de escritorio asignada para uso en zonas de acceso restringido, sea nueva o usada, pasa por un *proceso de preparación inicial* a fin de instalarle solamente software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante. [Nivel básico]
2. El proceso de preparación inicial de la computadora de escritorio incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% del medio principal de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel medio]
3. La lista de software autorizado para computadoras de escritorio en sitios de acceso restringido es un documento que prepara y actualiza el área de sistemas de la dependencia o entidad. Este documento se prepara en coordinación con el Responsable de los SDPs, según las necesidades y las funciones que desempeña el personal autorizado a su cargo. [Nivel medio]
4. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de las áreas de sistemas o de vigilancia. [Nivel medio]
5. El Encargado de los SDPs supervisa y verifica que la computadora de escritorio cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas. [Nivel básico]
6. El proceso de preparación inicial de una computadora de escritorio que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia. [Nivel básico]

#### **4.1.2. Resguardo**

1. La computadora de escritorio está asegurada físicamente para evitar el robo del gabinete o la sustracción de piezas o partes. Para tal propósito, está resguardada con cajones de protección, candados o cualquier otro dispositivo que impida la manipulación del gabinete y el acceso físico al interior del equipo. [Nivel básico]

#### **4.1.3. Operación**

1. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal autorizado del área de sistemas. [Nivel medio]
2. Están deshabilitados (en el interior del equipo) o cancelados (en el exterior) los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.). Las cancelaciones pueden ser abiertas por personal de sistemas. [Nivel medio]
3. No existen dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc.) en las computadoras de escritorio asignadas dentro de las zonas de acceso restringido de los SDPs. [Nivel medio]
4. El acceso a una computadora de escritorio dentro de una zona de acceso restringido, con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico,

es exclusivo para el personal de sistemas o, para un proveedor externo subcontratado. En cualquier caso, el Responsable de los SDPs es quien autoriza, supervisa y registra el acceso archivando la autorización que emite. [Nivel básico]

#### **4.1.4. Atención de fallas**

1. Cuando se presenta una falla en una computadora de escritorio, el usuario del equipo —o, en su caso, el Responsable de los SDPs— reporta de inmediato el evento al área de sistemas y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba del personal de sistemas. [Nivel básico]
2. En caso de que la falla requiera que la computadora de escritorio sea retirada de las zonas de acceso restringido de los SDPs para su reparación, los medios de almacenamiento no volátil son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de los datos personales que contiene. Dicha operación la realiza el personal autorizado del área de sistemas. [Nivel básico]

#### **4.1.5. Baja**

1. Toda computadora de escritorio que es dada de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final. [Nivel básico]
2. El proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel básico]
3. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de sistemas y de vigilancia. [Nivel básico]
4. El proceso de preparación final de una computadora de escritorio que se da de baja queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia con el formulario que en su momento registró el proceso de preparación inicial del equipo. [Nivel básico]

## **4.2. Servidores**

### **4.2.1. Recepción**

19. Un servidor asignado para uso en zonas de acceso restringido, sea nuevo o usado, pasa por un proceso de preparación inicial a fin de instalarle solamente software autorizado, configurado para brindar mayor seguridad que la predeterminada por el fabricante. [Nivel básico]
20. El proceso de preparación inicial del servidor incluye, antes de instalar el software, sobrescribir con un solo valor (unos o ceros) el 100% de los medios principales de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel básico]
21. La lista de software autorizado para servidores en sitios de acceso restringido es un documento que prepara y actualiza el área de sistemas de la dependencia o entidad. Este documento se prepara en coordinación con el Responsable de los SDPs, según las necesidades y las funciones que desempeña el personal autorizado a su cargo. [Nivel básico]
22. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de las áreas de sistemas o de vigilancia. [Nivel básico]
23. El Encargado de los SDPs supervisa y verifica que el servidor cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas. [Nivel básico]

24. El proceso de preparación inicial de un servidor que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia. [Nivel básico]

#### **4.2.2. Resguardo**

1. Todo servidor que está bajo la custodia del área de sistemas está instalado en un lugar que facilita adoptar:
  - Medidas de seguridad: Acceso restringido, sistema de vídeo-vigilancia remota.
  - Medidas para su buen funcionamiento: Temperatura de operación adecuada, mantenimiento preventivo y correctivo, atención inmediata en caso de fallas
  - Medidas que aseguran su operación continua: Elaboración y restauración de respaldos, sustitución rápida de partes dañadas [Nivel básico]
2. Aquel servidor que No está bajo la custodia del área de sistemas está asegurado físicamente para evitar el robo del gabinete o la sustracción de piezas o partes. Para tal propósito, está resguardado mediante cajones de protección, candados o cualquier otro dispositivo que impida la manipulación del gabinete y el acceso físico al interior del equipo. [Nivel básico]

#### **4.2.3. Operación**

1. Aquel servidor que No está bajo la custodia del área de sistemas tiene deshabilitados (en el interior del equipo) o cancelados (en el exterior) los puertos de comunicación (USB, paralelo, serial, etc.) que no se utilizan. Los cables o dispositivos conectados a los puertos que sí se utilizan están asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por personal de sistemas. [Nivel básico]
2. Aquel servidor que No está bajo la custodia del área de sistemas tiene deshabilitados (en el interior del equipo) o cancelados (en el exterior) los dispositivos de almacenamiento removible (unidades de disco flexible, quemadores de CD/DVD, etc.). Las cancelaciones pueden ser abiertas por personal de sistemas. [Nivel básico]
3. No existen dispositivos de conexión inalámbrica (Wi-Fi, Bluetooth, infrarrojo, etc.) en los servidores asignados dentro de las zonas de acceso restringido de los SDPs ni en aquellos que están bajo la custodia del área de sistemas. [Nivel básico]
4. El acceso a un servidor que No está bajo la custodia del área de sistemas, con el propósito de realizar labores de mantenimiento preventivo y correctivo o para soporte técnico, es exclusivo para el personal de sistemas o para un proveedor externo subcontratado. En cualquier caso, el Encargado de los SDPs es quien autoriza, supervisa y registra el acceso, archivando la autorización que emite. [Nivel básico]

#### **4.2.4. Atención de fallas**

1. Cuando se presenta una falla en un servidor que No está bajo la custodia del área de sistemas, el Responsable de los SDPs reporta de inmediato el evento al área de sistemas y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba del personal de sistemas. [Nivel básico]
2. Para los servidores críticos que están bajo la custodia del área de sistemas, dicha área tiene contratada una póliza de reparación, mantenimiento preventivo y correctivo cuyo tiempo de

- respuesta es suficiente para atender la criticidad de la información contenida en el equipo. [Nivel básico]
3. En caso de que la falla requiera que el servidor sea retirado de las zonas de acceso restringido de los SDPs para su reparación, los medios de almacenamiento no volátil son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de los datos personales que contiene. Dicha operación la realiza el personal autorizado del área de sistemas. [Nivel básico]

#### **4.2.5. Baja**

1. Todo servidor que es dado de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasa por un proceso de preparación final. [Nivel básico]
2. El proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel básico]
3. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de las áreas de sistemas y de vigilancia. [Nivel básico]
4. El proceso de preparación final de un servidor que se da de baja queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia con el formulario que en su momento registró el proceso de preparación inicial del equipo. [Nivel básico]

### **4.3. Impresoras y otros equipos periféricos autorizados**

#### **4.3.1. Recepción**

1. Las impresoras y los equipos periféricos autorizados (monitores, pantallas planas, etc.) usados en las zonas de acceso restringido de un SDP, sean nuevos o usados, pasan por un proceso de preparación inicial. Con ello se busca la presencia de puertos de comunicación (USB, paralelo, red local, por ejemplo) adicionales al principal que pudieran utilizarse para conectar dispositivos como los descritos en la sección "4.5. Equipo no autorizado". [Nivel medio]
2. Los puertos adicionales antes mencionados quedan inhabilitados (en el interior del equipo) o cancelados (en el exterior), mientras que los cables conectados a los puertos principales quedan asegurados para evitar su desconexión. Las cancelaciones pueden ser abiertas por el personal autorizado del área de sistemas. [Nivel medio]
3. Las únicas personas autorizadas para realizar el proceso de preparación inicial son miembros del personal de sistemas y de vigilancia. [Nivel medio]
4. El Encargado de los SDPs supervisa y verifica que el equipo de cómputo cumpla con los requerimientos de instalación establecidos y las configuraciones de seguridad definidas. [Nivel medio]
5. El proceso de preparación inicial de una impresora o de un equipo periférico autorizado que se asigna en zonas de acceso restringido queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia. [Nivel medio]

#### **4.3.2. Resguardo**

1. El equipo de impresión está asegurado físicamente para evitar el robo o la sustracción de cartuchos de tinta, piezas o partes. Para tal propósito, está resguardado mediante cajones de

- protección, candados o cualquier otro dispositivo que impida la manipulación del equipo y el acceso físico al interior del equipo. [Nivel medio]
2. El equipo de almacenamiento removible externo se mantiene bajo custodia del área de sistemas o del personal de vigilancia. [Nivel medio]

#### **4.3.3. Operación**

1. El uso de impresoras y equipo periférico autorizado que se conecta directamente a computadoras de escritorio y servidores dentro de zonas de acceso restringido es vigilado, supervisado o, en su caso, autorizado por el Responsable de los SDPs. [Nivel medio]
2. Las únicas personas autorizadas para utilizar el equipo de almacenamiento removible externo son miembros del personal de sistemas y de vigilancia. [Nivel medio]

#### **4.3.4. Atención de fallas**

1. Cuando se presenta una falla en una impresora o en un equipo periférico autorizado, el usuario del equipo —o, en su caso, el Responsable de los SDPs— reporta de inmediato el evento al área de sistemas y, de ser posible, toma las primeras acciones para evitar un mayor deterioro del equipo siguiendo las indicaciones que reciba del personal de sistemas. [Nivel básico]
2. En caso de que la falla requiera que la impresora o el equipo periférico autorizado sea retirado de las zonas de acceso restringido de los SDPs para su reparación, de existir medios de almacenamiento no volátil, estos son extraídos y puestos a resguardo para evitar la pérdida, robo o daño de datos personales. Dicha operación la realiza el personal autorizado del área de sistemas. [Nivel básico]

#### **4.3.5. Baja**

1. Toda impresora y todo equipo periférico autorizado que son dados de baja (ya sea por obsolescencia, sustitución o alguna otra causa) pasan por un proceso de preparación final. [Nivel básico]
2. Las impresoras y los equipos periféricos autorizados que en su interior contienen uno o más medios de almacenamiento no volátil, fijos o removibles, reciben atención especial. En este caso, el proceso de preparación final incluye transferir a otro equipo los archivos que contengan información que sea preciso conservar y sobrescribir con un solo valor (unos o ceros) el 100% de los medios de almacenamiento no volátil con alguna herramienta especializada para ello. [Nivel medio]
3. Las únicas personas autorizadas para realizar el proceso de preparación final son miembros del personal de sistemas y de vigilancia. [Nivel medio]
4. El proceso de preparación final de una impresora o de un equipo periférico autorizado que se da de baja queda registrado en un formulario. Este documento es archivado por el área de sistemas o por el personal de vigilancia y se archiva con el formulario que en su momento registró el proceso de preparación inicial del equipo. [Nivel básico]

## 4.4. Registro de actividades e inventario

### 4.4.1. Control de activos (inventarios)

1. El área de sistemas lleva un inventario actualizado (independiente de aquél que lleva el área administrativa correspondiente) para todos los activos de cómputo, separados por tipo; es decir, computadoras personales, servidores, impresoras y equipos periféricos autorizados. [Nivel básico]

### 4.4.2. Operación cotidiana

1. El Responsable de los SDPs mantiene estricto control y registro de:
  - a) Las autorizaciones emitidas al personal de sistemas o a proveedores externos subcontratados que proporcionan servicios de mantenimiento preventivo y correctivo así como soporte técnico para computadoras personales, servidores, impresoras y equipos periféricos autorizados asignados en áreas de acceso restringido. Dicho registro se lleva a cabo por el Encargado e incluye, por lo menos, los siguientes datos:
    - Causa que motiva el servicio
    - Número o identificación de activo del equipo de cómputo
    - Fecha y hora, tanto de inicio como de terminación del servicio
    - Nombre completo y firma de la o las personas que proporcionan el servicio
    - Tipo de identificación oficial que utiliza(n) dicha(s) persona(s) para acreditar su identidad (credencial de elector, pasaporte, etc.) y un número de referencia que aparezca en dicha identificación
    - Nombre y firma (visto bueno) del Responsable de los SDPs que autoriza el acceso
    - En forma opcional, se toma la fotografía de la(s) persona(s) que obtiene(n) acceso [Nivel básico]
  - b) Las autorizaciones para la operación de equipo de almacenamiento removible externo por parte del personal de sistemas o de vigilancia cuando es necesario llevar a cabo respaldos de información contenida en computadoras de escritorio o servidores que No están bajo la custodia del área de sistemas. [Nivel básico]
  - c) Las autorizaciones para el uso temporal de dispositivos como los que se listan en la sección "4.5. Equipo no autorizado" que se otorgan al personal autorizado que así lo solicite. Dicho registro incluye, por lo menos, los siguientes datos y documentos:
    - Causa que motiva la solicitud
    - Nombre completo de la persona que solicita autorización
    - Fecha en la que obtuvo autorización para interactuar con uno o más SDPs, nombre del Responsable de los SDPs que otorgó dicha autorización y fotocopia del documento que le otorgó la categoría de personal autorizado.
    - Tipo de identificación oficial con la que dicha persona acredita su identidad (credencial de elector, pasaporte, etc.) y un número de referencia que aparezca en tal identificación
    - Nombre y firma (visto bueno) del Responsable de los SDPs que autoriza el acceso
    - En forma opcional, se toma fotografía de la persona que obtiene acceso y del equipo no autorizado que utilizará en zonas de acceso restringido
    - Carta responsiva emitida por el usuario, encargado o demás personal que incluye su firma autógrafa y un manifiesto en el que asume la responsabilidad por el daño, pérdida o robo de los datos personales que almacene en el equipo no autorizado que utilice

temporalmente en cualesquiera de las zonas de acceso restringido de los SDPs [Nivel básico]

2. El área de sistemas o el personal de vigilancia mantiene estricto control y registro de:
  - a) El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada computadora de escritorio y cada servidor asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:
    - Nombre y firma de la o las personas que realizan el proceso de preparación inicial
    - Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
    - Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su recepción
    - Nombre y firma (visto bueno) dado por el Responsable de los SDPs
    - Número o identificación de activo del equipo que se asigna al equipo
    - Fecha en que el equipo queda instalado y se pone en operación
    - Área donde queda instalado el equipo [Nivel básico]
  - b) El formulario donde se asientan los detalles del proceso de preparación inicial que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:
    - Nombre y firma de la o las personas que realizan el proceso de preparación inicial
    - Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
    - Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; y demás componentes relevantes) en el momento de su recepción
    - Nombre y firma (visto bueno) dado por el Responsable de los SDPs
    - Número o identificación de activo del equipo que se asigna al equipo
    - Fecha en que el equipo queda instalado y se pone en operación
    - Área donde queda instalado el equipo [Nivel medio]
  - c) El inventario actualizado de activos de cómputo, mismo que incluye, por lo menos, los siguientes datos:
    - Descripción
    - Área donde se instaló el equipo
    - Número o identificación de activo que el equipo de cómputo tenía asignado
    - Características del equipo (marca, modelo y número de serie)
    - Características de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su recepción
    - Características de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca,

modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su baja

- Memoria técnica de las configuraciones de red del equipo, si aplica
- Folio del formulario que registra los detalles del proceso de preparación inicial y fecha de alta en el inventario
- Folio del formulario que registra los detalles del proceso de preparación final y fecha de baja del inventario [Nivel básico]

d) El formulario donde se asientan los detalles del proceso de preparación final que se lleva a cabo para cada computadora de escritorio y cada servidor asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:

- Área donde estaba instalado el equipo
- Número o identificación de activo que el equipo de cómputo tenía asignado
- Nombre y firma de la persona que realiza el proceso de preparación final
- Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
- Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y modelo de la unidad de procesamiento central; marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; marca y versión del sistema operativo instalado; y demás componentes relevantes) en el momento de su baja
- El destino que se le dará al equipo dado de baja
- Fecha en la que el equipo es efectivamente dado de baja
- Nombre y firma (visto bueno) del Responsable de los SDPs [Nivel básico]

e) El formulario donde se asientan los resultados del proceso de preparación final que se lleva a cabo para cada impresora y cada equipo periférico autorizado asignado en áreas de acceso restringido. Dicho registro incluye, por lo menos, los siguientes datos:

- Área donde estaba instalado el equipo
- Número o identificación de activo que el equipo de cómputo tenía asignado
- Nombre y firma de la persona que realiza el proceso de preparación final
- Fecha y hora en la que se realiza dicho proceso, tanto la de inicio como la de finalización
- Características del equipo (marca, modelo y número de serie) así como de los componentes de hardware al interior del equipo (marca y cantidad de la memoria volátil; marca, modelo y capacidad de los medios de almacenamiento no volátil; y demás componentes relevantes) en el momento de su recepción
- El destino que se le dará al equipo dado de baja
- Fecha en la que el equipo es efectivamente dado de baja
- Nombre y firma (visto bueno) del Responsable de los SDPs [Nivel medio]

f) El formulario en el que se registran los incidentes contiene la siguiente información:

- Registro del incidente donde se especifica: su tipo, gravedad, impacto, persona que lo detectó y personal que fue notificado.
- Los procedimientos implementados para la recuperación de los datos o aquellos procesos que permiten la pronta restauración de la operación del sistema.

- Seguimiento donde se indique el personal que interviene en la atención del incidente, la metodología aplicada, los datos recuperados, y en su caso, aquellos datos que ha sido necesario grabar manualmente en el proceso de recuperación. [Nivel básico]

#### **4.4.3. Divulgación de incidentes**

1. En caso de presentarse un incidente, se sigue el procedimiento que esa dependencia o entidad tenga definido. [Nivel básico]

En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:

2. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
3. En caso de robo o extravío de datos personales en soportes físicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
4. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un desplegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
5. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su identidad. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

#### **4.4.4. Supervisión**

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna para las unidades administrativas que mantienen y operan SDPs así como a los terceros contratados. [Nivel básico]

### **4.5. Equipo no autorizado**

#### **4.5.1. Computadoras portátiles**

1. No está permitido el libre acceso de computadoras portátiles a las zonas de acceso restringido de los SDPs. [Nivel básico]
2. Es posible autorizar el acceso temporal de computadoras portátiles siguiendo las recomendaciones descritas en el inciso "c", numeral "1", apartado "4.4.2. Operación cotidiana" de la sección "4.4. Registro de actividades e inventario". [Nivel básico]
3. En caso de que se autorice el acceso temporal de una computadora portátil, el área de sistemas o el personal de vigilancia lleva a cabo una revisión inicial del equipo. Dicha revisión incluye:

- La revisión y el registro de la estructura de los medios de almacenamiento no volátil, específicamente el número de particiones y el espacio libre
  - La detección de cualquier software que suponga un riesgo, ya sea por la pérdida de datos personales o por la sustracción, como malware y herramientas de intrusión
  - La inhabilitación de dispositivos de conexión inalámbrica que pudieran suponer un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido [Nivel medio]
4. En caso de ser necesario el traslado de datos personales al equipo no autorizado, éste sería con las siguientes restricciones: sólo lectura, no para modificación, no para sustracción, no para impresión, no para quemado. [Nivel medio]
  5. Al finalizar la visita, se llevará a cabo una revisión final de la computadora portátil por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye:
    - La revisión y el registro de la estructura de los medios de almacenamiento no volátil a fin de comprobar que el número de particiones y el espacio libre sigue siendo el mismo que en la revisión inicial, lo que permite detectar si hay archivos almacenados en el equipo portátil que no estaban al inicio
    - Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescriben con un solo valor (unos o ceros) utilizando una herramienta especializada para ello [Nivel básico]
  6. Por el riesgo que implica, está prohibido el uso de computadoras portátiles para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección “3. MS para transmisión de datos personales”. [Nivel medio]

#### **4.5.2. Dispositivos de almacenamiento externo**

1. Sin excepción alguna, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo ajeno a la institución o sin autorización. [Nivel básico]
2. Es posible autorizar el acceso temporal de dispositivos de almacenamiento externo siguiendo las recomendaciones descritas en el inciso “c”, numeral “1”, apartado “4.4.2. Operación cotidiana” de la sección “4.4. Registro de actividades e inventario”. [Nivel básico]
3. En caso de que se autorice el acceso temporal de dispositivos de almacenamiento externo, el área de sistemas o el personal de vigilancia lleva a cabo una revisión inicial del equipo. Dicha revisión incluye:
  - La revisión y el registro de la estructura de los medios de almacenamiento no volátil, específicamente el número de particiones y el espacio libre
  - La detección de cualquier software que suponga un riesgo, ya sea por la pérdida de datos personales o por la sustracción, como malware y herramientas de intrusión
  - La inhabilitación de dispositivos de conexión inalámbrica que pudieran suponer un riesgo de extracción de datos personales por una persona que se encuentre fuera de las zonas de acceso restringido [Nivel medio]
4. En caso de ser necesario el traslado de datos personales al equipo no autorizado, éste sería con las siguientes restricciones: sólo lectura, no para modificación, no para sustracción, no para impresión, no para quemado. [Nivel medio]

5. Al finalizar la visita, se llevará a cabo una revisión final de los dispositivos de almacenamiento externo por parte del área de sistemas o del personal de vigilancia. Dicha revisión incluye:
  - La revisión y el registro de la estructura de los medios de almacenamiento no volátil a fin de comprobar que el número de particiones y el espacio libre sigue siendo el mismo que en la revisión inicial, lo que permitiría detectar si hay archivos almacenados en el equipo portátil que no estaba al inicio
  - Las áreas no utilizadas (vacías) en los medios de almacenamiento no volátil se sobrescriben con un solo valor (unos o ceros) utilizando una herramienta especializada para ello [Nivel medio]
6. Por el riesgo que implica, está terminantemente prohibido el uso de dispositivos de almacenamiento externo para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección “3. MS para transmisión de datos personales”. [Nivel medio]

#### **4.5.3. Otros dispositivos no autorizados**

1. Sin excepción alguna, no se permite el acceso de ningún tipo de dispositivo de almacenamiento externo portátil (memoria USB portátil, reproductor MP3, teléfono celular) ajeno a la institución. [Nivel básico]
2. Es posible autorizar el acceso temporal de estos dispositivos siguiendo las recomendaciones descritas en el inciso “c”, numeral “1”, apartado “4.4.2. Operación cotidiana” de la sección “4.4. Registro de actividades e inventario”. [Nivel básico]
3. Por el riesgo que implica, está prohibido el uso de dispositivos no autorizados para la transmisión de datos personales en soportes electrónicos, mediante traslado físico, sin antes haber sometido dichos datos personales a un proceso de preparación previa tal como se describe en la sección “3. MS para transmisión de datos personales”. [Nivel básico]
4. Está prohibido introducir objetos que pudiesen dañar o alterar los soportes físicos y electrónicos que contengan datos personales tales como: tijeras, navajas, marcadores, alimentos o líquidos, entre otros. [Nivel básico]

## 5. MS para asegurar continuidad y enfrentar desastres

### 5.1. Respaldo y recuperación de sistemas de datos personales automatizados

#### 5.1.1. Medios de almacenamiento autorizados y no autorizados

1. Los medios de almacenamiento no volátil autorizados para la generación y almacenamiento de copias de seguridad (o respaldos) se dividen en dos grupos: fijos y removibles. Los medios fijos son los discos duros internos. Los medios removibles, pueden ser (i) magnéticos (cintas, discos duros externos), (ii) ópticos (CDs, DVDs) o (iii) magneto-ópticos (discos magneto-ópticos). [Nivel básico]
2. Los medios de almacenamiento no volátil autorizados se utilizan solos o en combinación, según las necesidades de respaldo y de restauración para garantizar la operación continua del SDP. [Nivel básico]
3. El uso de las unidades para lectura y escritura de dichos medios autorizados es exclusivo para el personal de sistemas, quien se encarga de generar las copias de seguridad. Ello implica que, si se trata de unidades internas (dentro del gabinete de la computadora), existe cuando menos una forma de restringir su uso. Por otro lado, si se trata de unidades externas que se conectan a un puerto de comunicaciones, entonces existe cuando menos una forma de restringir el uso de dicho puerto. [Nivel básico]
4. Todos aquellos medios de almacenamiento —así como sus respectivas unidades para lectura y escritura— que no entren dentro de las descripciones anteriores son considerados *no autorizados*. Esto incluye los dispositivos portátiles que cuenten con memoria no volátil integrada y algún dispositivo de comunicación (por cable o inalámbrica) que permita el intercambio de datos con una computadora. Algunos ejemplos son los llamados “memory-sticks”, las agendas digitales, los teléfonos celulares inteligentes, las cámaras digitales de instantáneas fijas o vídeo y los dispositivos portátiles para reproducción de música/vídeo como el Apple iPod y similares. [Nivel básico]
5. El Encargado de los SDPs, en colaboración con el personal de seguridad, ha implementado medidas para restringir el acceso y el uso de los dispositivos no autorizados. Los puntos de revisión y los sistemas de vídeo-vigilancia remota coadyuvan a este propósito. [Nivel básico]

#### 5.1.2. Inventario y clasificación de medios

1. Existe un inventario de los equipos autorizados para almacenar información crítica así como de aquellos que se utilizan para generar copias de seguridad (respaldos) de la información. [Nivel básico]
2. Los medios de almacenamiento no volátil que contienen las copias de seguridad mencionadas son clasificados y protegidos por el área de sistemas o el personal de vigilancia a fin de evitar su extravío, robo o daño accidental. [Nivel básico]
3. Se siguen los procedimientos archivísticos necesarios y suficientes para clasificar los medios de almacenamiento no volátil, ya sean magnéticos, ópticos o magneto-ópticos, dependiendo de las tecnologías utilizadas; en caso de que existan dos o más tecnologías, se lleva un control por cada una. El propósito es reducir el tiempo de espera para localizar los archivos que sea necesario restaurar. [Nivel básico]

### 5.1.3. Almacenamiento de respaldos

1. El almacenamiento de los respaldos (es decir, de los medios de almacenamiento removibles que los contienen) se realiza en lugares seguros, preferentemente en bóvedas de seguridad. [Nivel medio]
2. El reemplazo de dichos medios de almacenamiento se lleva a cabo mediante un esquema calendarizado. Por ejemplo, un esquema de reemplazo mínimo incluye realizar un respaldo general cada 7 días, mismo que se almacena durante un mes, antes de reemplazarlo. En la bóveda, quedan siempre cuatro semanas de respaldo. [Nivel medio]
3. Los respaldos se llevan a cabo a diario, en modo incremental y en línea, en caso de que el sistema lo permita. El séptimo día se realiza un respaldo general, fuera de línea, el cual es llevado, como lo menciona el punto anterior, a un lugar seguro para su resguardo. [Nivel básico]
4. Se lleva registro de las veces que un respaldo se introduce en, o se extrae de, las bóvedas. Son sólo dos (y cuando mucho tres) personas las que estén autorizadas para realizar dichos tramites. [Nivel medio]

## 5.2. Operación continua de sistemas de datos personales automatizados

### 5.2.1. Sitios alternos

1. Existe un sitio alternativo para restablecer la operación de un SDP automatizado, en el menor tiempo posible, en caso de un desastre. Para ello, se tiene establecido SOLAMENTE UNO de los siguientes tres tipos de sitios:
  - a) **Sitio alternativo frío.** En este tipo de sitios alternos no se incluye ningún equipo de cómputo ni otros recursos, de no ser por un ambiente mínimo de operación que incluya aire acondicionado, corriente eléctrica, enlaces de comunicaciones, piso falso, etc. Este tipo de sitios alternos es el menos costoso y a la vez el que más demora supone para restaurar las operaciones de un SDP automatizado.
  - b) **Sitio alternativo tibio.** En este tipo de sitios alternos el equipo está disponible unas cuantas horas después de ocurrido el desastre pero el equipo no contiene datos personales ni software. Este tipo de sitios alternos es el punto medio en costo y en tiempo para restaurar las operaciones de un SDP automatizado.
  - c) **Sitio alternativo caliente.** En este tipo de sitios alternos se mantienen disponibles tanto el equipo como el software y los datos personales, en cualquier momento, y solo es necesario “dar la orden” para activarlo y hacer posible su operación en un tiempo mucho más corto que en los sitios alternos anteriores. Este tipo de sitios alternos es el más costoso pero el que menor demora supone para restaurar las operaciones de un SDP automatizado. [Nivel básico]
2. Dependiendo de la criticidad de un SDP automatizado, el Manual de operaciones tiene definido el tiempo requerido para su restauración como sigue: (i) no esencial, se restaura en 30 días naturales, (ii) normal, en 7 días naturales, (iii) importante, en 72 hrs., (iv) urgente, en 24 hrs., (v) crítica o esencial, de 1 a 4 horas. Estos tiempos dan pauta para elegir el sitio alternativo a utilizar. [Nivel básico]

### 5.2.2. Tecnologías de información y telecomunicaciones

1. Existe un Plan de contingencia que documenta los procedimientos para restablecer la operación de los sistemas de redes en un sitio alternativo que está separado del centro principal, fuera de las

- instalaciones de la dependencia o entidad, en otra ciudad, a kilómetros de distancia. [Nivel básico]
2. A fin de tener identificados los mínimos requeridos para continuar con la operación, dicho Plan de contingencia está basado en: (i) un análisis realizado para determinar los requerimientos de soporte de una red, como serían los requerimientos de equipo, periféricos, cableado, etc.; y (ii) un análisis para identificar el tipo de comunicaciones, como serían los enlaces requeridos, líneas telefónicas y servicios de redes de comunicación electrónica, tanto de área local como de área ampliada. [Nivel básico]

### **5.2.3. Personal para emergencias**

1. Existe un Plan de contingencia que identifica al personal que lleva la operación de un SDP automatizado y que cuenta con la capacitación requerida para seguir los procedimientos de restauración en caso de desastre. [Nivel básico]
2. Dichas personas estuvieron involucradas en la creación de la documentación necesaria para el mencionado plan. [Nivel básico]
3. Dicho Plan de contingencia designa el personal de cada área necesario para efectuar la operación y administración de los SDPs automatizados que se restauran en el sitio alterno. [Nivel básico]

## **5.3. Registro de actividades**

### **5.3.1. Pruebas y simulacros**

1. El Responsable de los SDPs, en coordinación con el área de sistemas y el personal de vigilancia, lleva a cabo pruebas y simulacros para minimizar riesgos en caso de presentarse alguna eventualidad adversa y para comprobar que los sistemas de seguridad y prevención funcionan correctamente y en el tiempo estimado como óptimo. Estas tareas se llevan a cabo periódicamente, según el nivel de criticidad de la información. [Nivel básico]
2. Existe un registro de pruebas y simulacros que contiene, cuando menos, los siguientes datos:
  - Fecha y hora, tanto de inicio como de finalización
  - Encargado de realizarlas
  - Encargado de evaluarlas
  - Tiempo de restauración
  - Firma (visto bueno) de los Responsables
  - Observaciones
  - Sugerencias de mejora

El propósito de este registro es permitir su análisis y evaluación a fin de realizar las adecuaciones necesarias antes de que se presente una contingencia. [Nivel básico]

### **5.3.2. Divulgación de incidentes**

1. En caso de que el incidente se refiera a la pérdida de información debida a fallas en el equipo o en sus dispositivos de almacenamiento, ya sea por fallas en instalaciones, acontecimientos de casos fortuitos o de fuerza mayor (desastres naturales, incendios, huelgas, etc.), entonces procede la declaración de este. En ese momento, se pone en marcha el Plan de Continuidad del Negocio, para asegurar la continuidad de la operación o el Plan de Recuperación en caso de

- desastres para enfrentar el incidente. Cuando menos existe uno de estos planes en la dependencia o entidad. [Nivel básico]
2. En caso de que el incidente se refiera a actos deliberados (alteración, pérdida o robo de datos personales), se sigue el procedimiento que esa dependencia o entidad tenga definido. [Nivel básico]

En caso de que dicho procedimiento no lo incluya, además, se llevan a cabo las siguientes actividades, sin necesidad de que se realicen en el orden que aparecen:

3. El responsable del personal de vigilancia emite un informe al Responsable de los SDPs a no más de 3 días naturales de haber ocurrido el incidente. [Nivel básico]
4. En caso de robo o extravío de datos personales en soportes electrónicos, el titular de la dependencia o entidad o el Responsable de los SDPs, al tener conocimiento del incidente, da vista al Órgano Interno de Control, al área jurídica y/o al servidor público que tenga facultades para presentar denuncias o querellas de cada dependencia o entidad, en términos de sus Reglamentos Interiores o Estatutos Orgánicas, según corresponda, para que cada uno, en el ámbito de sus atribuciones, determine lo conducente. [Nivel básico]
5. A no más de 3 días naturales de haber ocurrido el incidente, el Responsable de los SDPs da aviso al público mediante un despliegado de prensa que difunde el hecho por diversos medios, según la gravedad del caso, a escala local, regional o nacional. [Nivel medio]
6. En caso de robo o extravío de datos personales, se alerta a los titulares de los datos afectados para que tomen sus precauciones ante el posible uso ilegal de su información. Para tal efecto, el Responsable de los SDPs da aviso por escrito a dichos titulares, a más tardar cinco días naturales de haber ocurrido el incidente, recabando el acuse de recibo de esta notificación. Con anticipación a dicho escrito, si se cuentan con los datos actualizados, se da aviso por correo electrónico o por teléfono. [Nivel básico]

### **5.3.3. Supervisión**

1. El Comité de información de la dependencia o entidad propone la realización de una supervisión interna a las unidades administrativas que mantienen y operan SDPs así como a los terceros contratados. [Nivel básico]

## **6. Documentación de MS en procesos y políticas del SDP**

### **6.1. Manual de operaciones**

1. Existe un Manual de operaciones donde están documentados los procesos y procedimientos que los servidores públicos llevan a cabo dentro de la dependencia o entidad. Aquellos procesos y procedimientos en los que se describe la forma en que los titulares de los datos y los servidores públicos (usuarios, personal autorizado, encargados, responsables) interactúan con los SDPs, incorporan la adopción de estos MS recomendados para la protección de datos personales. [Nivel básico]

### **6.2. Sensibilización y capacitación**

1. Se ha desarrollado un curso de sensibilización sobre protección de datos personales en soportes físicos y soportes electrónicos. El personal a quien va dirigido este curso son servidores públicos que tienen funciones asignadas para interactuar con SDP's al interior de la dependencia o entidad. [Nivel básico]
2. Este curso se imparte al menos una vez cada año al personal, llevando un registro de asistencia. [Nivel básico]
3. Al finalizar el curso, el participante manifiesta conocer la relevancia de la seguridad de datos personales y sus responsabilidades mediante firma autógrafa que se recaba en una lista que archiva el Responsable de los SDPs en la dependencia o entidad. [Nivel básico]
4. Existen un curso de sensibilización y un documento de firmas, similares a los anteriores, que persiguen el mismo fin pero que están orientados a proveedores externos que interactúan con uno o más SDPs y a quienes también se exige aseguren la protección de datos personales. [Nivel básico]

### **6.3. Cartas compromiso, cláusulas y contratos de confidencialidad**

1. Al menos cada dos años, el Responsable de los SDPs recibe (y archiva) una carta compromiso de parte de cada uno de los miembros del personal autorizado que interactúa con uno o más SDPs. [Nivel medio]
2. En dicha carta, el servidor público manifiesta, con su firma autógrafa, su compromiso para realizar su trabajo apegándose a los MS que apliquen a los SDPs en esa dependencia o entidad. Además, el servidor público manifiesta conocer los Lineamientos, el Reglamento y la Ley que integran el marco jurídico de las presentes Recomendaciones a fin de garantizar al ciudadano la custodia de sus datos personales. [Nivel medio]
3. La dependencia o entidad cuenta con un contrato de confidencialidad que ha firmado con cada proveedor o prestador de servicios que llama para la realización de servicios que impliquen interactuar con los SDPs. [Nivel básico]