Instituto Nacional para la Educación de los Adultos.

Documento de seguridad

Datos del documento

Nombre del documento:	Documento de seguridad
Código del documento	
Responsable de la elaboración	Subdirección Técnica
Dueño del documento	Director de Acreditación y Sistemas
Fecha de creación	Diciembre 2009
Creado por	Nombre del creador
Clasificación de seguridad	Confidencial
Software en que se editó	Microsoft Word ver. 2007
Versión actual	0.1

Historia de Revisiones

Fecha	Comentarios	Editó	Versión
Diciembre 2009	Versión inicial. Creación del documento.	Nombre del que editó.	0.1

CONTENIDO Pág

ANTECEDENTES

El Artículo 4 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental establece, entre sus objetivos, garantizar la protección de los datos personales que posean las Dependencias de la Administración Pública Federal.

El Artículo 20 de ésta Ley señala que los titulares de las Dependencias serán responsables de los datos personales que poseen y deberán adoptar las medidas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, transmisión y acceso no autorizado.

Los Lineamientos de protección de datos personales, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005, establecen las medidas que deberán adoptar las dependencias de la Administración Pública Federal para proveer seguridad a los sistemas de datos personales que manejan y custodian en el ejercicio de sus facultades.

El artículo Trigésimo tercero de los Lineamientos, establece que las dependencias, a través del Comité de Información y conjuntamente con el área de informática, expedirán un documento que contenga las medidas administrativas, físicas y técnicas de seguridad aplicables a los sistemas de datos personales, tomando en cuenta los lineamientos y las recomendaciones que en la materia emita el Instituto Federal de Acceso a la Información Pública (IFAI).

Mediante oficio número IFAI/SA-DGCV/642/09, el Instituto Federal de Acceso a la Información Pública informa que otorga como último plazo, hasta el 15 de diciembre de 2009 para que cada dependencia o entidad elabore y cuente o en su caso revise para completar el Documento de seguridad, de conformidad con el Trigésimo tercero de los Lineamientos de Protección de Datos Personales.

MARCO JURÍDICO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Orgánica de la Administración Pública Federal.
- Ley Federal de las Entidades Paraestatales.
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
- Reglamento de la Ley Federal de las Entidades Paraestatales.
- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Decreto por el que se crea el Instituto Nacional para la Educación de los Adultos.
- Decreto que establece las Medidas de Austeridad y Disciplina del Gasto de la Administración Pública Federal.
- Acuerdo por el que se designa a la Unidad de Enlace y se integra el Comité de Información del Instituto Nacional para la Educación de los Adultos. . Acuerdo por el que se modifica el cuadragésimo de los Lineamientos de Protección de Datos Personales.
- Acuerdo por el que se adiciona y modifican los Lineamientos Específicos para la Aplicación y Seguimiento de las Medidas de Austeridad y Disciplina del Gasto de la Administración Pública Federal.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.
- Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.
- Lineamientos Generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.
- Lineamientos de protección de Datos Personales.
- Lineamientos específicos para la aplicación y seguimiento de las medidas de austeridad y disciplina del gasto de la Administración Pública Federal.
- Estatuto Orgánico del Instituto Nacional para la Educación de los Adultos.
- Aviso por el que se dan a conocer los formatos de solicitudes de acceso a la información, de acceso y corrección a datos personales, y de recurso de revisión, cuya presentación no se realiza a través de medios electrónicos.

CAPÍTULO I DISPOSICIONES GENERALES

OBJETO Y ÁMBITO DE APLICACIÓN

1.- El presente documento indica las medidas de seguridad para el manejo y protección de los sistemas de datos personales tanto físicos como automáticos, para cumplir con las disposiciones aplicables por parte de los responsables, encargados y usuarios de los sistemas de datos personales con que cuenta el Instituto Nacional para la Educación de los Adultos, y son de observancia obligatoria para todas las áreas que manejen sistemas de datos personales.

2.- Este documento presenta las medidas de seguridad administrativa, física y técnica que el Instituto aplica para la protección de datos personales para asegurar la integridad, confidencialidad y disponibilidad de los datos relacionados. A la vez presenta los sistemas de datos personales que posee el Instituto, el tipo de datos personales que contiene cada uno, los responsables, encargados y usuarios de cada sistema así como las medidas de seguridad concretas implementadas para la protección de la información; por lo anterior, este documento también permite identificar los roles, actividades y responsabilidades de los servidores públicos o terceros contratados que dan tratamiento a información personal.

3.- El presente documento se integra considerando lo establecido en los Lineamientos de protección de datos personales, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005

4.- Definiciones

I. Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales.

II. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.

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

IV. 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.

V. 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.

VI. MEVyT: Modelo de Educación para la Vida y el Trabajo.

VII. Sistema "Persona": Aplicación informática desarrollada por el Instituto para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

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. Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

XI. SASA: Sistema Automatizado de Seguimiento y Acreditación.

XII. Sistema de datos personales: Un Sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

a) Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

b) Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

XIII. SITE: Término utilizado para referirse a un Centro de Cómputo con algún nivel de seguridad física y lógica.

XIV. SITE externo: SITE ubicado fuera de las instalaciones del Instituto y que no es de su pertenecía.

XV. SITE interno: SITE ubicado dentro de las instalaciones del Instituto, perteneciente y dependiente a él.

XVI. Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

XVII. Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la Interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

XVIII. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión.

XIX. Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.

XX. Usuario: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

PARTE 1. CATÁLOGO DE SISTEMAS DE DATOS PERSONALES

A.1 ÁREA: Dirección de Acreditación y Sistemas

A.1.1 NOMBRE DEL SISTEMA: SASA en línea

Ubicación: SITE externo

Responsable

Nombre: Ma. Gertrudis Alcaraz Ortega
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales
Obligaciones: Asegurar la protección de datos personales

Encargados

Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos personales de la aplicación.

Nombre: Mireya Rodríguez Navarro
Cargo: Jefe de Departamento
Funciones: Manipulación y consulta de datos de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Marco Antonio Rosales
Cargo: Jefe de Departamento
Funciones: Manipulación y consulta de datos personales de la aplicación
Obligaciones: Mantener la integridad de los datos personales de la aplicación

Usuarios
Nombre: Usuarios en las Entidades Federativas
Cargo: Director o Delegad, Jefes de departamento, Coordinador de Zona, apoyos técnicos.
Funciones: Captura y consulta de datos personales de la aplicación
Obligaciones: Mantener la integridad de los datos personales de la aplicación de acuerdo al perfil de *usuario* establecido.

Datos personales contenidos en el sistema

- Nombre completo
- CURP
- Fecha de nacimiento
- Domicilio
- Teléfono
- Sexo
- Estado Civil
- Idioma
- Número de hijos

- Ocupación de la esposa
- Fotografía
- Correo electrónico

Datos laborales:

- Ocupación

Datos académicos:

- Datos escolares

A.1.2. Nombre del sistema: Exámenes en Línea

Ubicación: SITE externo

Responsable

Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales
Obligaciones: Asegurar la protección de datos personales

Encargados

Nombre: Laura Elena Marin Bastarrachea

Cargo: Subdirectora de Normatividad
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*.
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Usuarios

Empresa: Transaction Language, Co. S.A. de C.V.
Funciones: Manipulación, configuración y consulta de datos de la aplicación (bajo un contrato de servicios)
Obligaciones: Asegurar la integridad y confidencialidad de los datos personales a nivel aplicación

Nombre: Maricela Aguilera Gómez
Cargo: Técnico Superior
Funciones: Consulta de datos personales de la aplicación
Obligaciones: Asegurar la confidencialidad de los datos personales a nivel aplicación

Nombre: Maria de los Ángeles Bernal Santamaría
Cargo: Eventual
Funciones: Consulta de datos personales de la aplicación
Obligaciones: Asegurar la confidencialidad de los datos personales a nivel aplicación

Datos personales contenidos en el sistema

- Nombre Completo
- Sexo
- Edad
- RFE RFC CURP
- Nacionalidad

- Correo Electrónico

Datos Laborales

- Empresa Dirección Giro Puesto Fecha de ingreso.

Datos académicos

- Escolaridad Cursos tomados Calificaciones

A.1.3. Nombre del sistema: Exámenes en Línea (Estados Unidos)

Ubicación: SITE externo

Responsable:

Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales
Obligaciones: Asegurar la protección de datos personales

Encargados

Nombre: Laura Elena Marin Bastarrachea
Cargo: Subdirectora de Normatividad
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*.
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Nombre: Jorge Alberto Díaz Stringel
Cargo: Coordinador Regional
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios

Nombre: Transaction Language, Co. S.A. de C.V.
Funciones: Manipulación, configuración y consulta de datos de la aplicación (bajo un contrato de servicios)
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Nombre: Jorge Alberto Díaz Stringel
Cargo: Coordinador Regional
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Datos personales contenidos en el sistema:

- Nombre Completo
- Sexo
- Edad
- RFE RFC
- CURP
- Nacionalidad
- Correo Electrónico

Datos Laborales

- Empresa Dirección Giro Puesto Fecha de ingreso.

Datos académicos

- Escolaridad Cursos tomados Calificaciones

A.1.4 Nombre del sistema: Módulo Indígena del MEVyT (Módulo Educativo Indígena)

Ubicación: SITE externo

Responsable:
Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Definir perfiles de usuarios.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Óscar Ulises Contreras Luna
Cargo: Jefe de Departamento
Funciones: Desarrollador de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Datos personales contenidos en el sistema:

- Datos de identificación
- Nombre Completo RFE CURP Fecha de Nacimiento Lugar de nacimiento Idioma Domicilio Teléfono Sexo Estado Civil Número de Hijos Correo Electrónico
- Datos Laborales
- Ocupación
- Datos Académicos
- Datos Escolares Antecedentes escolares

A.1.5 Nombre del sistema: Sistema de Plazas (SINAPLAC)

Ubicación: SITE externo

Responsable:
Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*..
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: David Martínez Velazquez
Cargo: Subdirector de Atención Educativa
Funciones: Manipulación y consulta de datos de la aplicación
Obligaciones: Asegurar la confidencialidad de datos personales

Nombre: Óscar Ulises Contreras Luna
Cargo: Jefe de Departamento
Funciones: Coordinar el desarrollado de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Efrén Flores Baca
Cargo: Programador Web
Funciones: Desarrollador de la aplicación
Obligaciones: Realizar las modificaciones necesarias al sistema sobre código fuente.
Folio de registro en el Sistema Persona:

Datos personales contenidos en el sistema:

- Datos de identificación
- Nombre Completo
- Datos Laborales
- Puesto
- Datos Académicos

A.1.6 Nombre del sistema: Registro Estatal de Formación

Ubicación: SITE externo

Responsable:
Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*..
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Óscar Ulises Contreras Luna
Cargo: Jefe de Departamento
Funciones: Coordinar el desarrollado de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Datos personales contenidos en el sistema:

- Nombre Completo RFC Correo electrónico.
- Datos Laborales

- Puesto
- Datos Académicos
- Datos Escolares Grado de estudios.

A.1.7 Nombre del sistema: Sistema de Acreditación y Seguimiento Automatizado para Comunidades en el Exterior (SASACE)

Ubicación: SITE externo

Responsable:
Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Óscar Ulises Contreras Luna
Cargo: Jefe de Departamento
Funciones: Coordinar el desarrollado de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Efrén Flores Baca
Cargo: Programador Web
Funciones: Desarrollador de la aplicación
Obligaciones: Realizar las modificaciones necesarias al sistema sobre código fuente.

Nombre: Jorge Alberto Díaz Stringel
Cargo: Coordinador Regional
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Datos personales contenidos en el sistema:
Datos de identificación
- Nombre Completo
- Sexo
- Estado civil
- Idiomas
- Correo Electrónico
- Teléfono
- RFE RFC
- Nacionalidad
- Fecha de nacimiento
- Lugar de nacimiento

Datos Laborales
- Ocupación Organismo Puesto

Datos Académicos
- Escolaridad

A.1.8 Nombre del sistema: Sistema de Autoevaluación, Evaluación y Seguimiento de la Educación Secundaria (SAESES)

Ubicación: SITE externo

Responsable:
Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Laura Elena Marin Bastarrachea
Cargo: Subdirectora de Normatividad
Funciones: Administrar la aplicación
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Usuarios
Nombre: César León Ledesma Ayala
Cargo: Enlace PC3 (Jefatura de Proyecto)
Funciones: Manipulación y consulta de datos de la aplicación, coordinador del desarrollo del sistema.
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Datos personales contenidos en el sistema:
Datos de identificación:
- Nombre Completo
- Dirección
- Sexo
- Edad
- Correo electrónico

A.1.9 Nombre del sistema: Sistema de Bitácora Electrónica de Plazas Comunitarias (SIBIPLAC)

Ubicación: SITE externo

Responsable:
Nombre: Mario Alberto Ríos Salas
Cargo: Directora de Acreditación y Sistemas
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información

Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Óscar Ulises Contreras Luna
Cargo: Jefe de Departamento
Funciones: Coordinar el desarrollado de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Alfredo Jiménez Dionisio
Cargo: Programador Web
Funciones: Desarrollador de la aplicación
Obligaciones: Realizar las modificaciones necesarias al sistema sobre código fuente.

Nombre: David Martínez Velazquez
Cargo: Subdirector de Atención Educativa
Funciones: Manipulación y consulta de datos de la aplicación
Obligaciones: Asegurar la confidencialidad de datos personales

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre Completo
- Fecha de Nacimiento
- RFC
- Sexo

Datos Laborales

- Puesto

Datos Académicos

- Escolaridad

A.2.1 Área: Dirección Académica

Nombre del sistema: Módulo Indígena del MEVyT (Módulo Educativo Indígena)

Ubicación: SITE externo

Responsable

Nombre: Luz Maria Castro Mussot
Cargo: Directora Académica
Funciones: Definir perfiles de usuario
Obligaciones: Asegurar la protección de datos personales

Encargados

Nombre: Maria de Lourdes Aravedo Resendiz
Cargo: Subdirectora de contenidos básicos
Funciones: Definir perfiles de usuario
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios

Nombre: Maria de Lourdes Aravedo Resendiz
Cargo: Subdirectora de contenidos básicos
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Datos personales contenidos en el sistema

- Nombre Completo
- RFE
- CURP
- Fecha de Nacimiento
- Domicilio
- Teléfono
- Sexo
- Estado Civil
- Número de Hijos
- Correo Electrónico

Datos laborales:

- Ocupación

Datos académicos:

- Datos escolares

A.2.2 Nombre del sistema: MEVyT en línea (Moodle)

Ubicación: SITE externo

Responsable:

Nombre: Luz Maria Castro Mussot
Cargo: Directora Académica
Funciones: Definir perfiles de usuario.
Obligaciones: Asegurar la protección de datos personales

Encargados

Nombre: Maria de Lourdes Aravedo Resendiz
Cargo: Subdirectora de contenidos básicos
Funciones: Definir perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios

Nombre: Luz Ma. Matamoros Vieyra
Jefa del Depto. de Proyectos Educativos con Aprovechamiento de las TIC
Funciones: Coordinar el desarrollo de la aplicación, atención a usuarios y operación del sistema.
Obligaciones: Mantener la integridad de los datos de la aplicación

Datos personales contenidos en el sistema:

Datos de identificación

- Nombre Completo
- CURP
- Fecha de Nacimiento
- Lugar de nacimiento
- Domicilio
- Teléfono
- Sexo
- Estado Civil

Datos Laborales

- Profesión Ocupación

Datos Académicos

- Datos Escolares

A.2.3 Nombre del sistema: Enciclopedia temática

Ubicación: SITE externo

Responsable:

Nombre: Luz Maria Castro Mussot
Cargo: Directora Académica
Funciones: Definir perfiles de usuario.
Obligaciones: Asegurar la protección de datos personales

Encargados

Nombre: Maria de Lourdes Aravedo Resendiz
Cargo: Subdirectora de contenidos básicos
Funciones: Definir perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios

Nombre: Luz Ma. Matamoros Vieyra
Jefa del Depto. de Proyectos Educativos con Aprovechamiento de las TIC
Funciones: Coordinar el desarrollo de la aplicación, atención a usuarios y operación del sistema.
Obligaciones: Mantener la integridad de los datos de la aplicación

Datos personales contenidos en el sistema:

- Datos de identificación
- Nombre Completo

Datos Laborales

- Puesto Teléfono

Datos Académicos

- Datos Escolares

A.3. 1 Área: Dirección de Asuntos Internacionales

Nombre del sistema: Formación (Moodle Asuntos Internacionales)

Ubicación: SITE externo

Responsable:
Nombre: Jorge Alberto Díaz Stringel
Cargo: Director de Asuntos Internacionales.
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Jorge Alberto Díaz Stringel
Cargo: Coordinador Regional
Funciones: Administrar la aplicación, otorgar y autorizar perfiles de *usuario*..
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Jorge Alberto Díaz Stringel
Cargo: Coordinador Regional
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Datos personales contenidos en el sistema:

- Nombre Completo
- CURP
- Fecha de Nacimiento
- Lugar de nacimiento
- Domicilio Teléfono
- Sexo
- Estado Civil

Datos Laborales

- Profesión Ocupación

Datos Académicos

- Datos Escolares

A.4. 1 Área: Dirección de Planeación, Administración, Evaluación y Difusión

Nombre del sistema: Análisis estadístico (Cubos)

Ubicación: Centro de datos Oficinas Centrales

Responsable:
Nombre: Rebeca Josefina Molina Freaner
Cargo: Directora de Planeación, Administración, Evaluación y Difusión
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Betzabe Prieto Escutia
Cargo: Subdirectora de Información y Calidad
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Eduardo Hernández Falcón
Cargo: Jefe del Departamento de Estadísticas
Funciones: Obtención de estadísticas a partir de bases de datos del SASAOL
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre completo
- CURP
- Fecha de nacimiento
- Domicilio
- Teléfono
- Sexo
- Estado Civil
- Idioma
- Número de hijos

Datos Laborales

- Ocupación

Datos Académicos

- Datos escolares

A.4.2 Nombre del sistema: Sistema de Servicios Administrativos (SSA)

Ubicación: SITE interno Oficinas Centrales

Responsable:
Nombre: Rebeca Josefina Molina Freaner
Cargo: Directora de Planeación, Administración, Evaluación y Difusión
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Víctor Beltran Sánchez de Aparicio
Cargo: Subdirector de Recursos Humanos
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación y el desarrollo
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Nombre: Adriana Laura Abundez Arreola
Cargo: Jefa del Departamento de Admisión y Movimientos
Funciones: Coordinar la implementación y verificar el correcto funcionamiento de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Andrés Franco Ortiz
Cargo: Jefa del Departamento de Remuneraciones
Funciones: Coordinar la implementación y verificar el correcto funcionamiento de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Luis Ricardo Miranda Gallegos
Cargo: Jefe del Departamento de Administración de Sistemas
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Administrar la aplicación a nivel técnico.

Usuarios
Anexo IV

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre Completo
- RFC
- CURP
- Fecha de nacimiento
- Estado civil
- Idiomas
- Lugar de nacimiento
- Nombres de familiares y parentesco
- Domicilio

Datos Laborales

- Puesto
- Plaza
- Área de adscripción
- Fecha de primer contacto
- Trabajos anteriores
- Prestaciones
- Cuenta bancaria para deposito de nómina

Datos Académicos

- Estudios Cursos Capacitación

A.4.3 Nombre del sistema: Sistema Artus

Ubicación: SITE interno Oficinas Centrales

Responsable:
Nombre: Rebeca Josefina Molina Freaner
Cargo: Directora de Planeación, Administración, Evaluación y Difusión
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargado
Nombre: Betzabe Prieto Escutia
Cargo: Subdirectora de Información y Calidad
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: Eduardo Hernández Falcón
Cargo: Jefe del Departamento de Estadísticas
Funciones: Obtención de estadísticas a partir de bases de datos del SASAOL
Obligaciones: Asegurar la integridad de los datos personales a nivel aplicación

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre completo
- CURP
- Fecha de nacimiento
- Domicilio Teléfono
- Sexo
- Estado Civil I
- Idioma
- Número de hijos
- Ocupación de la esposa

Datos Laborales

- Ocupación

Datos Académicos

- Datos escolares

A.4.4 Nombre del sistema: Sistema NomiPlus TA.NET

Ubicación: SITE interno Oficinas Centrales

Responsable:
Nombre: Rebeca Josefina Molina Freaner
Cargo: Directora de Planeación, Administración, Evaluación y Difusión
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Víctor Beltran Sánchez de Aparicio
Cargo: Subdirector de Recursos Humanos
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Usuarios
Nombre: María Eugenia Parrilla Luna
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Captura de datos y generación de reportes

Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Mónica Reyes Zamora
Cargo: Técnico Superior
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Nombre: Mariana Zamora Ocampo
Cargo: Analista Administrativo
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Nombre: Nidia Sánchez Orozco
Cargo: Secretaria C
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre Completo
- Fecha de nacimiento
- Nacionalidad
- Estado Civil
- RFC
- Domicilio
- Sexo
- Huella digital

Datos Laborales

- Fecha de contratación
- Entradas/Salidas

A.4.5 Nombre del sistema: Sistema de Control de Accesos AxTrax

Ubicación: SITE interno Oficinas Centrales

Responsable:
Nombre: Rebeca Josefina Molina Freaner
Cargo: Directora de Planeación, Administración, Evaluación y Difusión
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargado
Nombre: Víctor Beltran Sánchez de Aparicio
Cargo: Subdirector de Recursos Humanos
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Nombre: Adriana Laura Abundez Arreola
Cargo: Jefa del Departamento de Admisión y Movimientos

Funciones: Coordinar la implementación y verificar el correcto funcionamiento de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Usuarios

Nombre: Maria Eugenia Parrilla Luna
Cargo: Analista
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Nombre: Mónica Reyes Zamora
Cargo: Técnico Superior
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Nombre: Mariana Zamora Ocampo
Cargo: Analista Administrativo
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Nombre: Nidia Sánchez Orozco
Cargo: Secretaria C
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Captura de datos y generación de reportes

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre Completo
- Teléfono

Datos Laborales

- Departamento
- Entradas/Salidas

A.4.5 Nombre del sistema: Sistema Integral de Recursos Humanos (SIRH)

Ubicación: SITE interno Oficinas Centrales

Responsable:
Nombre: Rebeca Josefina Molina Freaner
Cargo: Directora de Planeación, Administración, Evaluación y Difusión
Funciones: Avalar el procedimiento para la protección de datos personales.
Obligaciones: Asegurar la protección de datos personales

Encargados
Nombre: Víctor Beltran Sánchez de Aparicio
Cargo: Subdirector de Recursos Humanos
Funciones: Administrar la aplicación, otorgar perfiles de usuario.
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Nombre: Juan Froylán López
Cargo: Subdirector de Tecnologías de la Información
Funciones: Administrar la aplicación y el desarrollo
Obligaciones: Asegurar la operación de la aplicación y la protección de datos en la aplicación

Nombre: Adriana Laura Abundez Arreola
Cargo: Jefa del Departamento de Admisión y Movimientos
Funciones: Coordinar la implementación y verificar el correcto funcionamiento de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Andrés Franco Ortiz
Cargo: Jefa del Departamento de Remuneraciones
Funciones: Coordinar la implementación y verificar el correcto funcionamiento de la aplicación
Obligaciones: Mantener la integridad de los datos de la aplicación

Nombre: Luis Ricardo Miranda Gallegos
Cargo: Jefe del Departamento de Administración de Sistemas
Funciones: Mantener la integridad de los datos de la aplicación
Obligaciones: Administrar la aplicación a nivel técnico.

Usuarios

Anexo IV.

Datos personales contenidos en el sistema:
Datos de identificación

- Nombre Completo
- Fecha de nacimiento
- CURP
- Estado Civil
- RFC
- Domicilio

Datos Laborales

- Puesto
- Fecha de ingreso
- Código de puesto
- Antigüedad
- Cuenta bancaria para deposito de nómina

Datos Académicos

- Estudios Cursos de capacitación

B.1. ENCARGADOS DE LA INFRAESTRUCTURA Y SISTEMAS OPERATIVOS DE TODOS LOS SISTEMAS DEL INSTITUTO, TANTO LOS UBICADOS EN EL SITE EXTERNO, COMO EN EL SITE INTERNO EN OFICINAS CENTRALES.

Nombre: Juan Gabriel Mercado Escobar
Cargo: Subdirector Técnico
Funciones: Administrar la infraestructura y Sistemas Operativos de los servidores que alojan la aplicación
Obligaciones: Asegurar la disponibilidad de la infraestructura y seguridad de datos en cuanto al acceso a los servidores.

Nombre: Carlos A. Gutiérrez Gutiérrez
Cargo: Jefe de Departamento
Funciones: Administrador de infraestructura de los bienes TIC's en los SITE's externo e interno
Obligaciones: Administrar sistemas operativos y servidor Web de la Infraestructura de los SITE's externo e interno.

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

2.1 Nombre del sistema: Sistemas alojados en los SITE's interno y externos

Tipo de soporte electrónico

- La información se encuentra localizada en los siguientes soportes electrónicos:
- Bases de datos relacionales de SQL Server 2000.
- Archivos de respaldo de SQL Server 2000.
- MySQL
- Archivos compactados conteniendo archivos de respaldo de SQL Server 2000.

Los soportes anteriores se encuentran los siguientes medios:

- Discos duros de servidores de bases de datos.
- Discos duros de servidores de respaldo.
- Cintas magnéticas

2.2. Lugar donde se resguardan los soportes:

La información almacenada de forma electrónica, es almacenada en los siguientes lugares: - SITE externo y SITE interno en Oficinas Centrales.

El SITE externo tiene las siguientes características principales:

- Calidad mundial - Disponibilidad 99.999 %
- Sistema contrafuegos
- Ubicado en una zona de baja sismicidad
- Control de acceso por zonas, de acuerdo al perfil e identificación presentada
- Sistema de energía redundante
- Sistema automatizado de precisión de aire acondicionado

Este lugar se describe con mayor amplitud en el Anexo I.

El SITE interno Oficinas Centrales tiene las siguientes características principales:

- Acceso controlado por mecanismos biométricos.
- Vigilancia las 24 horas mediante cámaras de seguridad y personal de seguridad.
- Control de temperatura mediante aire acondicionado.
- Protegido por sistemas UPS.
- Servidores en jaulas con cerradura.

Este lugar se describe con mayor amplitud en el Anexo I.

PARTE 3. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. Transmisiones de datos personales

I. Transmisiones mediante el traslado físico de soportes electrónicos:

El traslado físico de soportes electrónicos se realiza sobre los siguientes elementos:

Cintas de respaldo. - Información en unidades de disco extraíble. En el caso de las cintas de respaldo, la información que se encuentra es almacenada desde su origen en archivos cifrados mediante compresión con contraseña, por lo que el simple acceso a la cinta no permite extracción de la información. Los detalles de este cifrado son los siguientes:

> *Algoritmo de encripción: AES* - Tamaño de la clave: 256 bits. En el caso de las unidades de disco extraíble, la información a trasportar aparte de normalmente encontrarse cifrada mediante la compresión con contraseña, es trasportada en unidades lógicas cifradas con las siguientes características: - *Algoritmo de encripción:* AES - Tamaño de la clave: 256 bits - Tamaño del bloque: 128 bits. - Modo de operación: XTS.

En el caso de las cintas de respaldo, es necesario que se realice la forma de un documento de entrega/recepción donde se registran la siguiente información:

> Fecha. - Cantidad de cintas entregadas. - Etiqueta de cada cinta. - Descripción del contenido de cada cinta. - Nombre de la persona que entrega. - Cargo de la persona que entrega. - Nombre de la persona que recibe. - Cargo de la persona que recibe.

I.2 Transmisiones mediante el traslado físico de soportes electrónicos.

El traslado de los medios físicos es realizado por personal de departamento de Centro de Datos (*encargados*), se anota en una bitácora del SITE externo el soporte electrónica extraído y porque persona normalmente en vehículos proporcionados por el Instituto o en vehículos particulares.

I.3 Transmisiones mediante el traslado sobre redes electrónicas:

El tipo de transmisiones sobre redes electrónicas que se realiza con información de datos personales es alguno de los siguientes:

Transmisiones internas son todas las comunicaciones que se realizan sin abandonar la red privada. Por ejemplo: comunicaciones con servidores de dominio o bases de datos, transmisiones de control de sesiones, etc. - Transmisiones hacia oficinas centrales son comunicaciones que se realizan hacia la red ubicada en Oficinas Centrales. Por ejemplo: copiado de información de respaldo. - Transmisiones hacia el exterior. Son transmisiones que abandonan la red privada y van destinadas hacia un lugar diferente de las Oficinas Centrales del Instituto. Por ejemplo: accesos a sistemas desde los diferentes estados.

Las transmisiones internas se consideran seguras debido a lo siguiente: - Se realizan entre redes confiables - Las transmisiones son realizadas entre equipos bajo estricto monitoreo. - Se cuenta con detectores de intrusos cuando la información fluye de una red a otra.

Las trasmisiones hacia oficinas centrales se realizan tomando las siguientes precauciones en lo relacionado con la seguridad:

Para las transmisiones automáticas (como transmisiones de respaldos nocturnos), la información de origen se cifra utilizando compresión con contraseña con el algoritmo AES con longitud de 256 bits. Por lo que en caso de interceptación la información no es accesible directamente. - Para las transmisiones automáticas, se encuentran integrados en los scripts de respaldo la detección y notificación de problemas, por lo que en caso de éxito o fracasos son enviados correos electrónicos a personal del departamento de Centro de Datos informando la situación. - Adicionalmente se almacena en un log lo realizado por el script de respaldo. - Las transmisiones manuales se realizan utilizando túneles SSH a través de Internet con criptografía de clave pública por lo que toda la transmisión se realiza de forma segura.

Las trasmisiones de datos personales hacia el exterior son realizadas después de que se comprueba que el usuario que accesa autenticado y autorizado. Normalmente estas transmisiones utilizan el protocolo HTTPS mediante una página Web. En este caso las comunicaciones pasan por un proceso de inspección realizado por el sistema de detección/prevención de intrusiones. Adicionalmente, se realiza un registro del acceso en dos lugares diferentes: - Logs de la aplicación. - Logs del servidor Web.

II. Resguardo de sistemas de datos personales con soportes electrónicos

Los sistemas de datos personales están alojados en medios electrónicos cuyas características son las siguientes:
Alojados en discos duros de servidores y cintas magnéticas cuya protección principal es la siguiente:
Seguridad física: Control de acceso por zonas, de acuerdo al perfil e identificación presentada.
Descripción: Para accesar al área física donde se encuentran los servidores ser requiere de lo siguiente:

- Autorización por escrito en la cual el Responsable del sistema autorice al personal que requiere accesar al espacio físico de los servidores o en su caso a la bóveda de cintas.
- Presentarse en el área de recepción del SITE externo con el oficio de autorización, o en su caso de estar ya autorizado con el gafete correspondiente.
- Autentificarse con el personal del seguridad del SITE externo para el acceso
- Solicitar al personal del SITE externo, previa verificación de identidad, que abran la jaula para el acceso a los servidores o en su caso a la bóveda de cintas.

Seguridad lógica: El acceso a los servidores para la transmisión o respaldo del sistema se realiza de forma indirecta, es decir vía una VPN a la red de datos del Instituto Nacional para la Educación de los Adultos (equipo externo al SITE externo que aloja este sistema) y solo de esta red (limitada) es posible acceder a los servidores del SITE externo.

Asimismo para el acceso a los servidores se requiere de un login y contraseña que integra al menos 9 caracteres conjuntando, letras, número y caracteres especiales.

Este proceso se describe con mayor amplitud en el Anexo I

III. Bitácoras para accesos y operación cotidiana

1. Los datos que se registran en las bitácoras son los siguientes:
    - El nombre del usuario que accede
    - Fecha y hora
    - La modificación o consulta realizada
    - Fecha y hora de salida.
2. El lugar en donde se almacenan las bitácoras es en los discos duros de los servidores de las aplicaciones y controlados únicamente por el personal *encargado* de la Dirección de Acreditación y Sistemas
3. El personal que en caso de requerirse realiza el análisis de las bitácoras es el personal *encargado* de la Dirección de Acreditación y Sistemas

IV. Registro de incidentes

El registro de incidentes es llevado por personal *encargado* de la Dirección de Acreditación y Sistemas como consecuencia de:

- Si en la auditoría realizada por la Subdirección Técnica se detecta un intento recurrente no autorizado
- Si el área titular de los datos percibe alguna incongruencia en la información.

Con lo anterior se realizará un análisis y auditoria a la bitácora de eventos.

V. Acceso a las Instalaciones del SITE externo e interno

1. **Seguridad perimetral:** Se cuenta con políticas y procedimientos de seguridad para el acceso a las instalaciones que alojan los soportes físicos y electrónicos del Instituto en el SITE externo, este procedimiento y sus características se describen con mayor amplitud en el Anexo I, numeral 8 y numeral II.1
2. **Seguridad perimetral interior:** Se cuenta con políticas y procedimientos de seguridad para el acceso a la jaula y/o bóveda que alojan los soportes físicos y electrónicos del Instituto en el SITE externo, este procedimiento y sus características se describen con mayor amplitud en el Anexo I, numeral 8.

VI. Actualización de la información contenida en el sistema

La actualización contenida en el sistema es realizada de acuerdo a lo siguiente:
Encargados: Realizan depuración, ajustes y manipulación de datos de acuerdo a normas establecidas, los cambios realizados se registran en la bitácora de eventos de la aplicación.
Usuarios: Capturan información conforme se va generando.

VII. Perfiles de usuario y contraseñas

Modelo de control de acceso y perfiles de usuario y contraseña en el sistema operativo de red

El Instituto observa lo siguiente en cuanto al uso de perfiles de usuario y contraseña:

Para todas las contraseñas que sean utilizadas para algún dispositivo ubicado en el SITE externo y/o interno se cumplen los puntos presentados a continuación.

Responsabilidad del usuario

Cada contraseña es responsabilidad del usuario al que se le asigna, por lo que el usuario será responsable de la utilización de la misma.

El usuario no deberá proporcionar la contraseña a terceros.

Longitud de la contraseña

La longitud mínima de las contraseñas a ser utilizadas en dispositivos en el SITE externo es de 9 caracteres.

Complejidad de la contraseña

La contraseña deberá incluir por lo menos uno de cada uno de los siguientes grupos de caracteres:

- Letras mayúsculas (A, B, C,...)

- Letras minúsculas (a, b, c,...)
- Números (1, 2, 3,...)
- Caracteres especiales (", #, $, .)

Adicionalmente no se deben utilizar palabras de diccionario de cualquier idioma o variaciones sencillas de las mismas.

Duración de la contraseña.

La contraseña deberá ser cambiada cada 60 días y no será posible utilizar ninguna de las 4 contraseñas anteriormente usadas.

Otras políticas

Adicionalmente a las políticas antes mencionadas, se deben respetar las siguientes:

- La contraseña podrá ser escritas siempre y cuando se mantenga el escrito en un lugar seguro.
- Para evitar ataques de fuerza bruta, una cuenta podrá ser deshabilitada temporalmente después de un cierto número de intentos de acceso fallidos.
- Las contraseñas no deben ser enviadas usando servicios que no utilicen encriptación. Por lo anterior, las contraseñas no deben ser enviadas en mensajes de correo, conversaciones de Chat, etc.
- No utilizar una misma contraseña para dos servicios diferentes en el SITE externo.

El departamento de administración de centro de datos está autorizado para, de manera periódica, realizar auditorías y asegurarse de que las contraseñas son lo suficientemente robustas.

En la medida de lo posible, se deben utilizar mecanismos tecnológicos que, de manera automática, impongan las políticas antes mencionadas.

Perfiles de usuario y contraseña manejados por el software aplicativo del sistema de datos personales

Para el establecimiento de contraseñas al aplicativo del sistema de datos personales aplican los mismos numerales antes descritos, además de cumplir con el llenado del *"Formato de notificación de acceso a sistemas de información" (Anexo II)*

Responsabilidad del usuario

Cada contraseña es responsabilidad del usuario al que se le asigna, por lo que el usuario será responsable de la utilización de la misma, asimismo la definición de perfiles de usuario y la creación de las mismas de estos aplicativo recae exclusivamente en el ***encargado*** de la aplicación.

El usuario no debe proporcionar la contraseña a terceros.

Administración de perfiles de usuario y contraseñas

Los perfiles de usuario para administración de sistemas operativos de red, la asigna el ***encargado*** (Subdirector Técnico) de la aplicación.

Los perfile de usuario para el manejo y/o consulta de datos personales de la aplicación la asigna cada **encargado** del sistema. (Distinto a la Subdirección Técnica)

VIII. Procedimiento de respaldo y recuperación de datos

Este procedimiento es realizado por el personal "***encargado***" de la Subdirección Técnica de acuerdo a lo siguiente:

- Definición de archivos de datos a respaldar (se define en conjunto con el responsable u encargados por parte del área de la aplicación)
- Definición de horarios en los que se procederá con el respaldo de la información
- Tipo de respaldo
- Resguardo del respaldo electrónico

Para la recuperación de datos se realiza lo siguiente:

- Solicitud por escrito del respaldo a generar en el que indique, periodo y tipo del respaldo para recuperar, tipo de medio electrónico en que se realizará la recuperación de los datos.

IX. Plan de contingencia

El Plan de contingencia se encuentra en actualización debido a los constantes cambios en la optimización de los sistemas de datos personales.

Sin embargo dado que los sistemas sustantivos del Instituto se encuentran hospedados en un SITE externo con un proveedor de servicios y dado que el Instituto paga por servicios recibidos, este proveedor cuenta con otro SITE externo el cual tiene la capacidad para alojar los sistemas del Instituto si existiera un problema mayor con su SITE ubicado en la Ciudad de México.

PARTE 4. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE DATOS PERSONALES.

Actualmente todos los sistemas que se describen en este documento se encuentran operando, sin embargo el procedimiento que se solicitará para la cancelación de datos personales es el siguiente, a través de un oficio generado por el "responsable" de la aplicación que contenga:

- Fecha en el que el sistema dejará de operar
- Cancelación de perfiles de usuario para "encargados" y "usuarios"
- Respaldo de datos del sistema en soporte electrónico
- Respaldo del sistema en soporte electrónico
- Respaldo de la bitácora generada

Los respaldos quedarán a resguardo del ***responsable*** de la aplicación, asimismo el personal que realizará lo aquí indicado será el personal "***encargado***" de la Subdirección Técnica a petición de la responsable (Director(a) de la Dirección de Acreditación y Sistemas,

PARTE 5. RESPONSABILIDADES GENERALES

Para integrar la cobertura total en la protección de datos el Instituto establece de acuerdo a lo indicado en los puntos anteriores de forma general las siguientes responsabilidades:

De la Dirección de Acreditación y Sistemas

Establecer, implementar y asegurar la operación de la infraestructura del SITE externo e interno en cuanto a las siguientes características:

- Seguridad física del SITE externo e interno
- Seguridad lógica del SITE externo e interno
- Establecer la infraestructura de hardware y software de los bienes TIC, integrados en los SITE's
- Establecer la infraestructura de comunicaciones y servicios de Internet en los SITE's
- Establecer procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación de los sistemas operativos de la infraestructura de servidores y/o bienes TIC que alojan los sistemas de datos personales.
- Actualizar y controlar este documento, así como verificar que todos los sistemas que integren datos personales este incluidos en él y alineados a lo establecido en el numeral Trigésimo tercero de los Lineamientos de protección de datos personales, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.
- Establecer procedimientos para almacenar (medios físicos y/o electrónicos) y realizar transmisiones de datos de los medios electrónicos que contienen los datos personales.
- Continuidad de las operaciones. Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación.

Lo anterior considerando en todo momento los preceptos legales que correspondan, así mismo el Director de ésta área será el *Responsable* del *sistema de datos personales*

De la Dirección correspondiente al área usuaria del sistema que integra datos personales

- Acceder, manipular, consultar los sistemas de datos personales alojados en el SITE externo e interno, de acuerdo a perfiles de usuario establecidos, en cuanto a las siguientes características:

- Establecer procedimientos para generar, asignar, distribuir, modificar, almacenar (definir archivos para almacenar y medios físicos) y dar de baja usuarios y claves de acceso para la operación en el Sistema de Datos personales.
- Acceder, manipular, consultar, distribuir los sistemas de datos personales
- Garantizar la confidencialidad de los datos a los que se tiene acceso, estableciendo controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes y después de finalizar la relación laboral.

Lo anterior considerando en todo momento los preceptos legales que correspondan, así mismo el Director de ésta área será considerado también *Responsable* del *sistema de datos personales.*

PARTE 6. CATÁLOGO DE SISTEMAS DE DATOS PERSONALES (EXPEDIENTES FÍSICOS DE TRABAJADORES)

ÁREA: Dirección de Planeación, Administración, Evaluación y Difusión, Subdirección de Recursos Humanos, Departamento de Admisión y Movimientos

A.5.1 NOMBRE DEL SISTEMA: Expedientes Físicos de Trabajadores y Prestadores de Servicios Profesionales por Honorarios

Responsable

Nombre: Rebeca Josefina Molina Freaner

Cargo: Directora de Área

Funciones: Directora de Planeación, Administración, Evaluación y Difusión

Obligaciones: Responsable del tratamiento del Sistema

Nombre: Víctor L. Beltrán Sánchez de Aparicio

Cargo: Subdirector de Área

Funciones: Subdirector de Recursos Humanos

Obligaciones: Designar a los encargados del Sistema

Nombre: Adriana Laura Abúndez Arreola

Cargo: Jefe de Departamento

Funciones: Jefa del Departamento de Admisión y Movimientos

Obligaciones: Proponer los criterios de operación del Sistema y coordinar las actividades de integración de documentos a los expedientes físicos y las actividades de resguardo del Sistema.

Encargados

Nombre: Elsa Salazar González

Cargo: Analista Administrativo

Funciones: Archivista

Obligaciones: 1.- Integrar documentos personales, laborales y de asistencia en los expedientes personales

de los trabajadores y prestadores de servicios profesionales por honorarios del Instituto, activos e inactivos 2.- Resguardo de los expedientes físicos señalados en la obligación 1.

Nombre: Claudia Stephany López Ramírez

Cargo: Técnico Superior

Funciones: Archivista

Obligaciones: 1.- Integrar documentos personales, laborales y de asistencia en los expedientes personales de los trabajadores y prestadores de servicios profesionales por honorarios del Instituto, activos e inactivos 2.- Resguardo de los expedientes físicos señalados en la obligación 1.

Nombre: Francisco Mendoza Avendaño

Cargo: Jefe de Oficina

Funciones: Archivista

Obligaciones: 1.- Integrar documentos personales, laborales y de asistencia en los expedientes personales de los trabajadores y prestadores de servicios profesionales por honorarios del Instituto, activos e inactivos 2.- Resguardo de los expedientes físicos señalados en la obligación 1.

Usuarios

Nombre: Personal del Departamento de Admisión y Movimientos

Funciones: Administrativas

Obligaciones: 1.- Consultar los expedientes físicos sólo para cumplir con las funciones que tienen encomendadas 2.- Hacer buen uso y manejo del expediente físico que en su momento se encuentre bajo su resguardo.

Nombre: Personal del Departamento de Remuneraciones

Funciones: Administrativas

Obligaciones: 1.- Consultar los expedientes físicos sólo para cumplir con las funciones que tienen encomendadas 2.- Hacer buen uso y manejo del expediente físico que en su momento se encuentre bajo su resguardo.

Datos contenidos en el sistema de expedientes físicos

Datos de Personales:

- Nombre completo
- CURP
- RFC
- Acta de nacimiento
- Domicilio
- Hoja de datos personales
- Fotografía

- Certificado Médico
- Cartilla
- Credencial de Elector
- Curriculum Vitae

Datos laborales:

- Nombramientos y/o Contratos
- Oficios referentes a su relación con el INEA
- Constancias de Habilidades Laborales
- Control de asistencia

Datos académicos:

- Datos escolares (documentación que acredita su nivel escolar)
- Constancias de Cursos

ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE DATOS PERSONALES PARA ESTE SISTEMA (PARTE 6)

Finalidad: Contar con un expediente personal de los trabajadores y prestadores de servicios profesionales por honorarios que contenga documentación personal, laboral y de control de asistencia.

Tipo de soporte: Físico

Descripción: Los expedientes físicos de los trabajadores y prestadores de servicio profesiones por honorarios, se resguardan en un área cerrada ubicada dentro de la Subdirección de Recursos Humanos

Características del Lugar donde se guardan los datos:

El área de Archivo que resguarda los expedientes físicos posee las siguientes características

- Área cerrada de 1.85 ms x 8.76 ms que cuenta con un solo acceso, 11 anaqueles y 192 gavetas
- Iluminación artificial
- Sistema de aire lavado
- Control de acceso limitado

MEDIDAS DE SEGURIDAD IMPLEMENTADAS PARA ESTE SISTEMA (PARTE 6)

Transmisión de datos personales

La transmisión de datos personales y expedientes físicos se realiza previa solicitud por escrito y se atiende la requisición por escrito y se clasifica la información de conformidad con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Personal con Acceso al Área de Archivo:

- Personal adscrito al Departamento de Admisión y Movimientos previa designación por escrito
- Personal adscrito al Departamento de Remuneraciones previa designación por escrito

Bitácoras

En el área de Archivo lleva una bitácora de acceso de los usurarios a los expedientes físicos, que contiene:

- N° de cobro y nombre del titular del expediente físico,
- Fecha de préstamo,
- Nombre y firma de quien recibe el expediente,
- Fecha y firma de devolución
- Motivo por el cual se solicita el acceso

Registro de incidentes

Cuando se presente un incidente como el daño, extravío o robo de datos personales y/o expedientes físicos, se realizarán las siguientes acciones:

- El encargado informará por escrito al responsable del incidente presentado, señalando la fecha del acontecimiento y el motivo que dio origen.
- En caso de comprobarse el daño, extravío o robo, se informará a la Unidad de Asuntos Jurídicos para los efectos que correspondan.
- El encargado llevará una bitácora de los incidentes presentados.

Acceso a las Instalaciones del área de archivo

En el área de archivo se resguardan los expedientes físicos, cuya seguridad consiste:

3. **Seguridad perimetral:** Se cuenta con políticas y procedimientos de seguridad para el acceso a las instalaciones del Instituto
4. **Seguridad perimetral interior:** Se cuenta con políticas para el acceso al área de archivo dentro de la Subdirección de Recursos Humanos, limitando el acceso exclusivamente al personal autorizado.

Actualización de la información contenida en el sistema

La información contenida en el sistema de Expedientes Físicos de Trabajadores y Prestadores de Servicios Profesionales por Honorarios, se actualiza diariamente al integrar los documentos que derivan de la relación del Instituto con los trabajadores y prestadores.

Los encargados del sistema, tienen bajo su resguardo un determinado número de expedientes físicos, de los cuales realizan su actualización conforme al ingreso de los documentos al área de archivo.

PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE DATOS PERSONALES DE ESTE SISTEMA (PARTE 6)

No aplica para el Sistema de Expedientes Físicos de Trabajadores y Prestadores de Servicios Profesionales por Honorarios.

ANEXO I

I. ESPECIFICACIÓN DE LOS SISTEMAS ALOJADOS EN EL SITE EXTERNO

I.1 ANTECEDENTES

El Instituto Nacional para la Educación de los Adultos cuenta con aplicaciones de gran demanda como el SASA en línea, Administrador de cursos, Servidores de Bases de Datos, etc. las cuales por sus características de disponibilidad, seguridad de datos (confidencialidad) y capacidad de procesamiento se requiere que se encuentren alojadas en un sitio capaz de proveer, tanto en infraestructura, comunicaciones, seguridad así como en nivel de servicio, las características descritas con anterioridad con los más altos estándares de calidad. Todo esto con la finalidad de mejorar los niveles de servicio y acceso de la población a la información y los servicios en beneficio de los usuarios.

I.2 DESCRIPCIÓN DEL SERVICIO

El INEA cuenta con un contrato de servicios que provee la infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y Extranet de la entidad.

El contrato de servicios contempla como mínimo el servicio de Hospedaje dedicado de aplicaciones en servidores dedicados, lo cual permite alojar aplicaciones críticas para tener acceso vía Internet. Incluye todo el soporte necesario para implementar, instalar, reinstalar las aplicaciones del INEA durante todo el tiempo que dura el contrato y soporte, e instalación de equipo de comunicaciones y almacenamiento solicitado. Así mismo cuenta con el personal dedicado al INEA en servicios 7x24 los 365 días para soporte y asesoría de todas las plataformas que conforman el contrato que el INEA define durante la vigencia.

A través de los servicios de Hosting de EL PROVEEDOR, el INEA cuenta con una infraestructura de clase mundial para hospedar de forma remota aplicaciones complejas de uso crítico alojadas en el SITE externo.

I.3 OBJETIVOS GENERALES

Los objetivos generales que se deben alcanzar son los siguientes:

- Contar con una solución en la cual el proveedor integra todo lo requerido para alojar, instalar, migrar, operar, monitorear, soportar y mantener las aplicaciones en los Servidores, equipos de comunicaciones y seguridad requeridos.
- Obtener mediante medios físicos, electrónicos y de software los más altos índices de seguridad de datos.

I.4 CARACTERÍSTICAS

- La plataforma de servidores y comunicación interna que ofrece el proveedor son dedicados de forma exclusiva para el INEA.
- El SITE externo permite el acceso de personal técnico autorizado del INEA, para supervisar los procesos realizados dentro del SITE o área del proveedor de servicios destinada al INEA.

I.5 UBICACIÓN

- El SITE externo cuenta con una infraestructura de alojamiento diseñado para operar como un SITE externo de alta disponibilidad ubicado en la ciudad de México o hasta 150 Km alejado del centro de la misma.

I.6 GARANTÍA DE DISPONIBILIDAD

- Mínima de 99.99% en el SITE externo.

I.7 CARACTERÍSTICAS GENERALES DEL INMUEBLE

- Ubicado en una zona antisísmica o de baja sismicidad.
- Es una construcción con estructuras principales que soporte niveles sísmicos de alta intensidad.
- No corre riesgos por cualquier tipo de desastres naturales y deberá contar con mecanismos de protección en caso de siniestros.
- Cuenta con los sistemas de protección necesarios de pararrayos.
- Provee un espacio físico de trabajo para dos personas equipado con mesa, silla, teléfono, consola, acceso a Internet y a los servidores, equipos y servicios descritos en este documento. Así mismo se deberán proveer credenciales de acceso permanente para tres personas que definirá el Instituto, en un esquema de trabajo de 7x24x365.
- El espacio destinado para albergar la infraestructura integral de servicios es delimitada de instalaciones de terceros y áreas comunes a través de una estructura de aislamiento perimetral que puede ser habitación separada o jaula con chapa de seguridad, así como contar con racks de 42 unidades instalados para soportar de forma justa los equipos del INEA.
- Cuenta con la infraestructura integral así como los dispositivos necesarios para alojar todos los equipos de cómputo, comunicaciones y seguridad contenidos en este anexo.

I.8 CARACTERÍSTICAS DE SEGURIDAD FÍSICA DEL SITE EXTERNO:

- Estructura contra sismos integrada.
- Piso falso: modular con capacidad de soportar carga mínima de 500 Kg/m2, con cámara plena entre losa y piso falso de acuerdo a las normas internacionales que rigen estos sistemas.
- Cobertura antiestática.
- Cuenta con un arreglo de aires acondicionados de precisión dentro de las instalaciones donde se alberguen los equipos descritos en este anexo con controles automáticos de humedad y temperatura para mantener un rango de temperatura máxima de 21°C con variaciones máximas de +/- 1 grados.
- Sistema de prevención y detección de incendio de manejo de zonas.
- Sistema de supresión de fuego exterior.
- Seguridad de acceso al SITE externo, el cual permita acceso únicamente mediante tarjetas u otro medio de control electrónico registrando el evento y alarma de intrusos.
- Vigilancia 7x24x365 a través de sistemas de monitoreo de video cámaras de seguridad, con al menos una vista al espacio que ocupará el SITE externo del INEA.

I.9 CARACTERÍSTICAS DE LA INFRAESTRUCTURA ELÉCTRICA

- El SITE externo cuenta con un sistema eléctrico que garantiza el soporte al 100% de los dispositivos que conformen la infraestructura integral de servicios del SITE externo INEA, así como los dispositivos propios del SITE externo que brinden servicio a dicha infraestructura (conectividad, telecomunicaciones y acceso a la red Internet).

CONTAR CON INFRAESTRUCTURA ELÉCTRICA REDUNDANTE:

- Fuente de poder de AC.
- Salida de Voltaje: 110-220 VAC, 60 Hz.
- UPS redundante con las protecciones correspondientes de supresión de picos, con capacidad para soportar toda la infraestructura de equipos relacionados en este anexo.
- Capacidad de 8 horas de backup de batería
- Planta de emergencia de diesel con capacidad de soporte de la infraestructura relacionada en este anexo, y la de todo el SITE externo por tiempo ilimitado, con tiempos de recarga para el combustible de al menos 60 horas.
- Cuenta con un sistema interno que permite aterrizar los dispositivos de cómputo y comunicaciones, racks y/o gabinetes y demás equipos necesarios, donde máximo el diferencial de voltaje entre Tierra y Neutro sea 1 volt.

I.10 CARACTERÍSTICAS DE SEGURIDAD LÓGICA:

- La solución de seguridad lógica es realizada con equipos en alta disponibilidad.
- La solución de seguridad no es factor de latencia adicional en las redes por razones de su desempeño.
- La configuración y operación de este sistema de seguridad, en lo que respecta al servicio que servirá al SITE externo INEA es coordinado en todo momento por personal de la Subdirección Técnica del INEA y del proveedor del servicio, esto con la intención de optimizar su desempeño y adecuarlo a las necesidades del Instituto en todo momento.

SEGURIDAD EN EL SITE EXTERNO

- El proveedor es el encargado de instalar, administrar, monitorear, mantener y actualizar, los dispositivos en Disposición antes mencionados
- El SITE externo cuenta con línea de defensa, que al menos ofrece servicios de firewall, antivirus, antispam, VPN y detección y prevención de intrusos. Estos servicios cuentan con las siguientes características:

Firewall

- Firewall (Stateful inspection Firewall) en esquema de alta disponibilidad y con balanceo de cargas con interfaces suficientes para la solución de sistemas del Instituto.
- Soporta la creación de VPN's usando los algoritmos más comunes de encripción (DES, 3DES, AES, etc.) y en esquemas site-to-site y client-to-site
- Es capaz de manejar al menos 250,000 conexiones concurrentes o al menos 300Mbps.
- Incluye prevención de ataques de negación de servicios distribuidos (DDoS)

Sistema de Detector de Intrusos

Ofrece un sistema de detección y prevención de intrusos que permite la correcta y oportuna identificación de ataques, que por lo menos proporciona lo siguiente:

- El sistema de prevención y detección de intrusos esta en un esquema de alta disponibilidad y de balanceo de cargas con interfaces suficientes para la los servicios del INEA.

- **Detección de ataques e intrusos:** Basada en firmas, anomalías estadísticas, protocolos, de situaciones de negación de servicio y basados en Host.
- **Rechazo de intrusos:** Posibilidad de configurar el sistema para rechazar o eliminar automáticamente las conexiones no deseadas.

Protección contra virus y antispam

- Protección de antivirus de gateway para la infraestructura del SITE externo INEA contra código malicioso que sea capaz de explorar al menos en los protocolos http, ftp, smtp, y pop3.
- Los servidores de correo de INEA y CONEVyT estan protegidos con antispam y antivirus de gateway en los protocolos smtp y pop3.
- Es posible utilizar reglas diferenciadas para los dominios de correo @inea.gob.mx y @conevyt.org.mx así como que sea posible enviar los correos identificados como spam a una cuenta en el dominio correspondiente para su revisión.
- El antispam, cuenta con los siguientes métodos para detección de SPAM:
  - Listas blancas y negras.
  - Filtrado por contenido (asunto y cuerpo del mensaje).
  - DNS-based Blackhole Lists
  - Reputation Filtering o similar.

I.11 CABLEADO ESTRUCTURADO

- La interconexión de los dispositivos que integren la infraestructura propuesta, se realiza respetando la norma de cableado estructurado, que dependiendo de la interface de red de los equipos es mínimo del tipo UTP categoría 6 o fibra óptica según sea el caso.
- El cableado está debidamente identificado tanto en el panel de distribución como en los cables de interconexión.

I.12 COMUNICACIONES

Equipamiento de Conectividad para la red LAN

- El proveedor del servicio provee el equipamiento (en Disposición) de Switching necesario para la interconexión de toda la infraestructura del SITE externo INEA y la disponibilidad en la misma debe es al menos el 99.99%.
- El esquema de conexión es coordinado con la Subdirección Técnica del Instituto y el área técnica del proveedor del servicio de tal forma que la solución sea la óptima para el desempeño de las aplicaciones.
- El equipo de switching, contiene al menos las siguientes características:
  - 24 puertos 10/100
  - 2 puertos 10/100/1000TX Uplinks
  - Fuente de poder redundante
  - Capa 3 con manejo de VLANs y calidad de servicio, listas de acceso y validación vía Radius o TACACS+ y trabajar en capas 2-4.
  - Deberá tener la posibilidad de limitar el ancho de banda por cada puerto del switch.
  - Estándares soportados: IEEE 802.1x, 802.1w, 802.1s, 802.1D, 802.1Q VLAN, 802.1p, 802.3 10BASE-T, 802.3u, 802.3ab, y 802.3ad
  - Soportar UDP, IP, ICMP Y TCP.
  - Administración vía WEB, Telnet.
  - Procesadores y fuentes de poder redundantes

- 1 RU

Acceso a la red de Internet

- El backbone principal de proveedor hacia Internet esta soportado por al menos 2 conexiones independientes y redundantes, con carriers diferentes.
- El nivel de servicio requerido para este servicio es de 99.99%
- El servicio es entregado a través del SITE externo del proveedor en esquema redundante.
- Las conexiones cuentan con al menos los dos de los principales proveedores de servicios de Internet de la República Mexicana, deberán tener a su vez las siguientes características:
    - Los prestadores de servicios de Internet tienen conexión directa a por lo menos dos puntos de acceso a la red de Internet en Estados Unidos y/o NAP's (Network Access Points, por sus siglas en Inglés) con una capacidad del orden de un STM1 como mínimo.
    - Cobertura a nivel nacional mediante infraestructura robusta con esquemas de alta disponibilidad y redundancia automática entre sus puntos de presencia POP's (points of presence, por sus siglas en inglés) y ubicación.

I.13 SERVICIO DE ALMACENAMIENTO

- El proveedor es responsable de la configuración, administración y dispositivos necesarios para la conexión de los servidores de aplicaciones del Instituto a la SAN del proveedor.
- El proveedor cuenta con el servicio integral de SAN (Storage Area Network), para tener espacio adicional para almacenamiento de información a través de líneas de fibro canal (FC-switch o FC-AL) 4 puertos a 2Gb/s, configurado en RAID 5 y con un espacio utilizable de 930 GB, para la aplicación SASAOL y 30GB para la aplicación Control de Gestión, este deberá poder crecer con solo incluir discos para poder proveer crecimiento en menos de 2 horas conforme a requerimiento del INEA.
- El proveedor proporciona un dispositivo de respaldo, no necesariamente exclusivo para el servicio al INEA, además de cintas para respaldo requeridas para almacenar 1.5 terabytes de almacenamiento. Por lo cual, se cuenta de 2 terabytes para almacenamiento en bóveda.

I.14 SERVICIOS ADICIONALES DE HOSPEDAJE

- Licenciamiento en 4 servidores para contar con servicios de Verificación SSL de 128bits con una entidad verificadora internacional ampliamente aceptada en el mercado mundial.

I.15 SERVICIOS PROFESIONALES Y PERSONAL CAPACITADO

- El proveedor ofrece un centro de atención telefónica con un control de llamadas y reportes de seguimiento y solución de los mismos. Los reportes de seguimiento deberán contener como mínimo y se cuenta con una *bitácora* de seguimiento.

    - Número de reporte
    - Fecha
    - Hora
    - Tipo de falla
    - Tipo de escalamiento
    - Fecha y hora de solución
    - Quién reporta la falla y quién atendió

I.16 MONITOREO DEL SERVICIO

- Los servidores solicitados cuentan con monitoreo en hardware y software.
- El proveedor genera reportes de uso y monitoreo de los servicios en línea mediante una ventana gráfica accesible por Internet (WEB), la cual brindará información sobre los siguientes parámetros:
    - Utilización de recursos de hardware.
    - Utilización de ancho de banda de salida y de entrada.
    - Reportes de tráfico y desempeño en cada uno de los puertos de acceso a Internet.
    - Filtros de reportes por día, semana, mes.
    - Monitoreo de los servidores de base de datos del Sistema SASA en Línea.
    - El proveedor deberá contar con personal técnico que tenga por lo menos un año de experiencia trabajando para un Hosting Center de un ISP o Carrier de Internet.
    - El área del Instituto que interactuarán con la del proveedor de servicios es la Subdirección Técnica.
- El proveedor informa inmediatamente sobre problemas detectados en el funcionamiento de servidores y el servicio al personal designado por el INEA y deberá catalogar este procedimiento como de alta prioridad.
- *Reportes de incidentes de seguridad.*

I.17 SOPORTE TELEFÓNICO (CONTACT CENTER)

- Soporte 24 horas al día, los 7 días de la semana, todo el año. Con un número 01 800.

El servicio del proveedor deberá tener las siguientes características distintivas:

- A través del sitio WEB del proveedor del servicio se puede solicitar en línea cualquier servicio de ayuda y apoyo técnico, opciones adicionales y modificaciones a sus servicios, así como verificar el estatus de sus órdenes.
    - Cuenta con un centro de monitoreo NOC (Network Operation Center) que monitorea el estado de la red 7X24 los 365 días del año.
    - Atención del técnico asignado en forma directa para la solicitud de servicios y asesoría técnica.

I.18 POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD PARA CLIENTES E INSTALACIONES DEL SITE EXTERNO

General:

El SITE externo se reserva el derecho de seleccionar áreas específicas dentro de sus instalaciones como áreas propietarias. A partir de este punto, a estas áreas se les denominará AREAS RESTRINGIDAS. El acceso no autorizado a cualquier área restringida está prohibido y cualquier individuo que entre a estas áreas sin autorización, será sometido a medidas judiciales acordes al tipo de violación.
El personal no autorizado encontrado en estas áreas, será inmediatamente identificado y acompañado fuera del Área Restringida. El Supervisor de Seguridad emitirá un reporte de entradas no autorizadas que entregará a la Gerencia de Infraestructura. En caso de que la persona o personas no autorizadas opongan resistencia, la policía local será requerida para manejar la situación. Se levantará un reporte del incidente con la autoridad policiaca correspondiente.

Traspaso:

En las instalaciones del SITE externo se colocarán letreros prohibiendo el paso, de acuerdo a las leyes y reglamentos municipales. Estos señalamientos estarán en el perímetro de las instalaciones, de acuerdo a lo requerido por las leyes locales. Estarán exhibidos de tal manera, que definan con claridad los límites de la propiedad y que alerten a las personas de su entrada a la propiedad del SITE externo. La colocación de estos señalamientos, de acuerdo a lo requerido por ley y reglamento, será la base legal sobre la que se emitirá una queja de entrada no autorizada en o dentro de áreas Restringidas y no restringidas, propias o rentadas del proveedor.

Aplicación:

Estas políticas y procedimientos aplican a todos los empleados, clientes, contratistas, consultores, proveedores y todo el personal desconocido.

Área de SITE externo.- Se denomina al área que está destinada para el alojamiento y producción de racks / gabinetes de computo para el uso del SITE externo y sus clientes. Dicha área está diseñada y construida bajo altos estándares par procesos exclusivos de cómputo.

Personal del SITE externo.- Es el personal que labora de manera regular e indefinidamente en las instalaciones de que pertenecen a la nómina del mismo.

Personal Autorizado por el Cliente.- Es el personal que trabaja para el Cliente, que por sus labores y funciones, están autorizados para entrar en las instalaciones del Cliente. Esta autorización deberá ser concedida por escrito por el personal responsable del Cliente y deberá estar presente sin excepción por lo menos un representante autorizado (con gafete) por parte del cliente.

Visitantes.- Son las personas que no son personal del SITE externo y que tampoco son Personal Autorizado por el Cliente.

Proveedores Autorizados por el SITE externo.- Son los proveedores contratados por el proveedor que, por sus labores que desempeñan, tienen que permanecer un período razonable en las instalaciones del SITE externo. Estos proveedores tienen que firmar un contrato y cumplir con los requisitos para poder realizar las labores. Estos proveedores siempre estarán sujetos a revisión en el momento en que el SITE externo lo demande.

Área Controlada.- Por lo general todas las áreas se consideran controladas, con la excepción de la recepción al frente de las instalaciones, durante el día.

Controles de acceso.- Definido como dar de alta a un individuo a través del sistema de tarjetas de identificación y de manera opcional en un sistema biométrico de exploración de huellas digitales. El acceso está restringido al otorgamiento de permisos en el grupo de acceso al cual la persona está asignada.

Gafete de Identificación.- Todo el personal está obligado a portar el gafete de identificación mientras permanezca en las instalaciones del SITE externo. Los gafetes tendrán que estar en un lugar visible sobre la persona. Esto es una obligación que será estrictamente vigilada por todo el personal de seguridad y de operaciones de las instalaciones. De la misma manera se requiere que los visitantes y proveedores porten una etiqueta que los identifique, misma que será provista en la recepción y tendrá una vigencia limitada al día de emisión.

Acceso de Empleados y de Clientes.- Las instalaciones están protegidas por un control de acceso y sistemas de vigilancia a través de cámaras, diseñado para ofrecer un cercano y constante monitoreo y control de todas las actividades dentro de las instalaciones. Todo acceso a las instalaciones estará restringido a aquellas categorías del personal cuyo acceso está autorizado, a través del alta en la estación de control de gafetes de identificación, localizada en las oficinas de operaciones. Todos los clientes y empleados serán dados de alta. Los proveedores, consultores y visitantes portarán una etiqueta auto adherible con un código especial que los identifique. El alta especificará el nivel de acceso, no sólo para clientes, sino también para nuestros empleados. Además, se contará con un sistema de control biométrico utilizado para los empleados y clientes. Los exploradores biométricos estarán ubicados en la esclusa del edificio de operaciones y en los puntos de entrada a las áreas en niveles superiores. No habrá ninguna excepción a esta política. Por definición, una persona sin alta biométrica no podrá entrar a las instalaciones sin ser acompañado.

Seguridad Física:

El SITE externo proporcionará a cada cliente seguridad perimetral, tal como se define en el control de acceso y sistema de vigilancia con cámaras. Además de que cada pasillo del área del SITE externo y cada puerta de acceso al mismo serán vigilados por un sistema de cámaras, las puertas de las jaulas de los clientes tendrán la opción de controles de acceso de tarjeta de proximidad o bien biométricas según el caso. El monitoreo central del perímetro, de las áreas restringidas estará ubicado en la oficina de seguridad de las instalaciones. El personal de seguridad mantiene estados de vigilancia de 7 x 24 x 365 para responder y reportar condiciones de anormales y/o de alarma.

Protección de la Propiedad Intelectual:

Los empleados y clientes del SITE externo son responsables de proteger toda la información y materiales propiedad de la compañía. El acceso no autorizado, extracción o divulgación de dicha información está prohibida por la protección de Secreto Comercial. Todo el personal debe estar consciente de su responsabilidad de proteger y salvaguardar la información propiedad de la compañía. Todos los documentos, datos, materiales, correos electrónicos, FAX y transmisiones inalámbricas generados, deberán ser marcados con claridad para especificar a todos los usuarios / receptores que los materiales son confidenciales y deben ser protegidos.

Por motivos de seguridad, y dado a que hay áreas comunes dentro del edificio de operaciones, el proveedor tiene una política de escritorios limpios. Esta política establece que no debe haber papeles confidenciales sueltos sobre los escritorios de trabajo del personal de del SITE externo, así como las impresiones y faxes deberán ser recogidos por su dueño de manera continua.

Procesamiento de las violaciones a la seguridad:

Cualquier tipo de violación de la seguridad será reportado al Supervisor de Seguridad, quien a su vez lo escalará a la Gerencia de Infraestructura con un reporte escrito del incidente. Las violaciones a la seguridad del cliente seguirán el mismo proceso, pero además, se generará un reporte del incidente para el Responsable de la Cuenta del Cliente.

Evaluación de Amenaza y Vulnerabilidad:

La Gerencia de Infraestructura es la responsable de realizar Evaluaciones de Amenazas de manera recurrente. La evaluación se hará de manera anual y se generará un reporte para la dirección. Esta evaluación debe incluir pruebas de todos los sistemas, reportes de todos los incidentes de seguridad y la recomendación de cualquier nuevo concepto o ideas para mejorar la integridad de nuestras instalaciones

Planeación e Implementación de Evacuaciones de Emergencia:

El Supervisor de Seguridad debe participar como el líder del comité de
Seguridad y deberá convocar a miembros para el equipo. El supervisor generará planes de evacuación de emergencia de las instalaciones y deberá realizar prácticas de evacuación anuales. A través del sistema de tarjetas de identificación, se llevará una bitácora electrónica central, la cual reflejará en cualquier momento, al personal que esté en las instalaciones.
Es importante considerar que el Supervisor de Seguridad por parte de del SITE externo será el líder del Comité de Seguridad, y que este mismo deberá de hacer público los planes de evacuación y de seguridad en caso de contingencia. De esta manera, los guardias internos del SITE externo deberán de apoyar y por consiguiente deberán contar con entrenamiento especial en estas situaciones.

Terminaciones:

Cliente.- En caso de una terminación involuntaria o voluntaria de un cliente, el Área de Administración del SITE externo deberá notificar inmediatamente al Supervisor de Seguridad. Bajo ninguna circunstancia un cliente cuyo contrato ha terminado, podrá entrar al área restringida sin acompañamiento. Una vez que el cliente ha sacado sus propiedades de su área de alojamiento asignada, será acompañado a la salida. Se le deberán retirar tantas tarjetas de acceso como personas tenga registradas en la lista de personal autorizado por el cliente. De la misma manera, se deberá exigir la entrega del control de acceso al área del cliente en el SITE externo.

Empleado.- Ante una terminación voluntaria o involuntaria de un empleado, el Área de Administración del SITE externo deberá notificar inmediatamente al Supervisor de Seguridad, quien eliminará su autorización de acceso de los sistemas de control y retirarle las tarjetas de acceso que pueda tener. Si el empleado cuyo contrato ha terminado muestra disgusto o insurrección, el Supervisor de Seguridad deberá acompañarlo a la salida y puede optar por notificar a las autoridades locales del incidente.

Control de las llaves de las Instalaciones:

El Supervisor de Seguridad será responsable de las llaves de todas las puertas de las instalaciones. Las llaves de las instalaciones serán tantas como lo ordene el Director de Operaciones. El Supervisor de Seguridad entregará llaves a los empleados que así la requieran para sus labores, tal como oficinas privadas, gavetas, cajones, etc, firmando los últimos de recibido y haciéndose responsables de las mismas.

Control de la llave del Cliente:

Cada jaula estará equipada con una llave única. Todas las llaves estarán marcadas y asociadas con el cliente en particular. La llave es proporcionada a los clientes haciéndose este último responsable del uso y de la misma llave. En caso de extravío, el SITE externo proporcionará los costos correspondientes al cambio de la chapa en la puerta de su jaula. Si el cliente viene sin su llave correspondiente, el personal de seguridad del SITE externo podrá abrir el gabinete o área de alojamiento siempre y cuando se identifique como personal autorizado del cliente.

Proceso de Gafetes:

Los 'Gafetes de identificación con fotografía' serán producidos en las instalaciones de operaciones por el Oficial de Seguridad o Recepcionista. El Supervisor de Seguridad será el responsable de procesar todas las solicitudes de gafetes, de incluir la fotografía al gafete, de mantener copias de todas las fotos, de asegurarse que se genere un registro para todos los gafetes emitidos. Los gafetes serán asignados con base en la 'necesidad de acceso', sin embargo habrá que reducir las categorías para que este sea un proceso manejable.

Categorías de Gafetes:

Empleado.– Cada empleado contratado por el SITE externo deberá portar un gafete con fotografía con esta clasificación. El gafete no expira, pero puede estar programado para limitar el tiempo de acceso a las instalaciones.

Contratistas y/o proveedores.- Se les entregará una etiqueta de visitante con fotografía y con la asignación del personal del SITE externo que autoriza su acceso, manteniendo su trabajo bajo observación así como su comportamiento en el SITE externo.

Cliente.- A cada cliente autorizado se le entregará un gafete con fotografía sin fecha de expiración, pero con acceso limitado al SITE externo. También serán registrados en el sistema de exploración biométrica.

Visitante.- Cada visitante recibirá una etiqueta de identificación, mencionando al visitante y la fecha y hora de validez. Se le asignará un acompañante.

Seguridad.- Todos los elementos de seguridad deberán portar sus gafetes, con acceso a todas las instalaciones y con la leyenda 'SEGURIDAD' visible.

Control de acceso a las instalaciones

Generales:

Todos los empleados y clientes autorizados tendrán acceso a las instalaciones del SITE externo a través del sistema de dispositivos de exploración de lectoras de proximidad y de biometría de ola digital controlada. Estos dispositivos serán programados por el personal de Infraestructura del SITE externo y monitoreados por el personal de Seguridad. Existen tres puntos de seguridad antes de entrar al área del SITE externo:

Entrada vehicular.- Acceso Custodiado 7 x 24 x 365 por dos elementos del personal de seguridad. Los guardias deberán contar con comunicación vía radio con los demás elementos del grupo de seguridad para notificar los accesos; además de extensiones telefónicas para la comunicación con las demás áreas del SITE externo. La entrada vehicular está controlada por un sistema de lectoras de proximidad magnética por ambos frentes (exterior e interior). En la entrada peatonal (adjunta a la entrada vehicular) se encuentra instalada una esclusa equipada con lectoras de proximidad magnética por ambos frentes (exterior e interior). En este punto de acceso se encuentran instaladas cámaras externas fijas y de movimiento con la cobertura adecuada para monitorear los eventos que puedan ocurrir en el acceso y sus alrededores.

Entrada de la recepción principal.- Acceso custodiado por un guardia. La entrada de visitantes está siendo protegida por el guardia y la recepcionista es quien registra y anuncia al visitante. De igual manera, la entrada es controlada por lectoras de exploración de proximidad magnética y además se cuenta con sistema de CCTV con cámaras digitales externas e internas.

Entrada al edificio de operaciones.- Esta entrada está controlada por un sistema de puertas exclusas, blindadas y controladas por controles biométricos de acceso.

Registro y Alta en Biométrica de ola digital:

Este es el proceso de alta de registro en el sistema de control de acceso:

Al momento que el cliente realice su primera visita a las instalaciones, deberá contar con acceso autorizado por parte del Responsable de la cuenta.

Al llegar a las instalaciones, el cliente deberá identificarse con una credencial con fotografía y la afiliación de su compañía.
El / la recepcionista deberá cotejar la identificación contra las base de datos de clientes. Si coincide, se acepta la autorización.

El supervisor de seguridad tomará una foto del cliente y generará el gafete apropiado con fotografía.

Después, el cliente tendrá que pasar el dedo que sea de su elección por el explorador biométrico. Este proceso autentifica el permiso de acceso del cliente y sirve como un segundo nivel de seguridad.

Gafete perdido u olvidado:

El principal control de acceso es el gafete con fotografía. Sin el gafete, nadie puede entrar a las instalaciones. Cuando se sabe que un gafete con foto se perdió o fue robado, a la persona se le emitirá uno nuevo y el antiguo será marcado en el sistema como invalido. el proveedor emitirá una factura por el nuevo gafete otorgado al cliente o empleado. Si la persona olvido el gafete con fotografía, solamente se le podrá dar acceso al SITE externo previa identificación y autorización. Antes de emitir un nuevo gafete, la persona deberá ser autenticada en el sistema de seguridad.

Visitantes:

Los visitantes, solos o en grupo, deberán estar siempre acompañados por un empleado del SITE externo. El acompañante del SITE externo deberá registrar a todos los visitantes en el Registro de Visitas, anotando su nombre y el de la compañía que representan. También debemos considerar que llenen y firme una forma de confidencialidad, si van a acceder al área del SITE externo.
Una vez terminado el registro, se les entregará una etiqueta de Visitante con Acompañante mostrando el nombre de la persona y la fecha. El gafete se debe portar en un lugar visible. El acompañante usará su gafete y la exploración biométrica para abrir la puerta principal y dar paso a los visitantes al sistema de puertas exclusas. El acompañante será el último en entrar a la trampa y cerrar la puerta. Una vez cerrada la puerta principal, el acompañante procede a abrir la puerta de salida de la trampa y permite a los visitantes entrar al área controlada de la recepción. Todos los visitantes deberán estar a la vista del acompañante todo el tiempo. No se permitirá tomar video ni fotografías dentro de la propiedad del SITE externo. Al salir de las instalaciones, el acompañante o la recepcionista deberá recoger todas las etiquetas y anexarlas a sus correspondientes contratos de confidencialidad (en caso de ser requeridos). Se debe anotar la salida de los visitantes en el Registro de Visitas.

Entrada a las Instalaciones

Todo el Personal:

Cualquier persona que ha sido registrada y dada de alta en el sistema de acceso y control biométrico, puede pasar directamente a la puerta de entrada del edificio de operaciones en donde se encuentra el sistema de puertas esclusas. La persona pasará su gafete con fotografía por el explorador de proximidad magnética y recibirá una luz verde indicando que fue aceptada, después bioexplorará el dedo seleccionado y la puerta de la esclusa se liberará para su apertura. La persona entra al cubo de seguridad y la puerta deberá cerrarse detrás de ella; a continuación pasará su gafete por el explorador de proximidad magnética de la segunda puerta para la liberación de la misma y su consecuente apertura, acción con la cual ya podrá ingresar al interior del edificio operativo.

El otro punto de entrada a las instalaciones es el área de Envío & Recepción. Ninguna persona, empleado o no, usará este punto de entrada / salida como entrada principal a las instalaciones. El uso de estas puertas como primer intento de entrada será considerado VIOLACIÓN DE SEGURIDAD.

Sistema de control de acceso:

El sistema de control de acceso será administrado por la Gerencia de
Infraestructura del SITE externo. Éste llevará el control de las altas, bajas y cambios en los registros de cada empleado y/o cliente o proveedor. La Gerencia de Infraestructura definirá y controlará los grupos de acceso y permisos a los que tenga derecho el individuo por la naturaleza de sus funciones.

Se deberá tener un control de horario para realizar estas modificaciones, las cuales serán en horas de oficina entre semana. El procedimiento está descrito en las páginas anteriores. En caso de que haya un incidente en el cual los permisos no sean los correctos, el equipo de seguridad deberá validar la identidad del individuo y escalar el caso con el Supervisor para que sea resuelto el problema de manera inmediata.

Sistema de Circuito Cerrado de Televisión (CCTV):

Todas las entradas que están siendo controladas por el sistema de acceso, ya sea por tarjetas lectoras o biométricas, son vigiladas por un sistema de circuito cerrado de TV. Este sistema, concentra todos sus controles, monitores y grabadoras en el cuarto de seguridad en el edificio de operaciones.

Es obligación del equipo de seguridad estar vigilando los monitores en busca de algún incidente que pudiera ocurrir. La operación del sistema también va a estar a cargo del equipo de seguridad. En el caso de ocurrir algún problema, este se debe de reportar de inmediato con el Supervisor y acudir a atender la situación. Siempre debe haber un elemento de seguridad en el cuarto de seguridad.

Las imágenes captadas serán grabadas por un sistema de grabación digital y serán almacenadas por un espacio de treinta días. Esta administración la llevará el Supervisor de Seguridad y la operación es por los diferentes elementos de seguridad.

Seguridad General

Prevención de Incidentes en el lugar de trabajo:

La dirección del SITE externo se compromete a ofrecer un lugar de trabajo seguro para sus empleados, clientes y visitantes. La gerencia de infraestructura implementará un Programa General de Prevención de Incidentes en el Lugar de Trabajo, el cual deberá abarcar la capacitación necesaria para el personal de seguridad como responsable de los operativos y al demás personal del SITE externo para que conozca sus alcances. El programa deberá ser aprobado por la Dirección de Operaciones y la Dirección General y será documentado para que se lleve a cabo dentro de las instalaciones.

Incidentes con los Empleados:

Todos los incidentes reportados de mala conducta de un empleado del SITE externo o cualquier amenaza dirigida contra cualquier empleado, serán investigados y reportados al Director de Operaciones. La primera línea de acción de la Dirección para con un empleado que reportó una amenaza o incidente, será realizar una investigación para determinar la naturaleza y magnitud del incidente. La Dirección de Administración deberá ser notificada inmediatamente del incidente para levantar el acta administrativa correspondiente y buscar apoyo en la materia. Bajo ninguna circunstancia se dejará una situación de amenaza sin reporte y sin investigación. En caso de extremo alboroto o cuando se percibe que una persona puede ser lastimada,

todos los empleados serán entrenados para llamar de inmediato a las autoridades locales de emergencias, en caso de que el Supervisor no esté disponible.

Incidentes con los Clientes:

En la inducción de seguridad con los clientes, el Supervisor de Seguridad deberán notificar al cliente que el SITE externo no tolerará irreverencias o comportamiento rudo y ofensivo contra cualquier empleado del SITE externo. De la misma manera, es el espíritu de cualquier empleado del SITE externo y personal externo laborando en el SITE externo, tener una actitud de servicio con el cliente. Es muy importante que esta actitud se mantenga y nunca debe haber un comportamiento grosero o rudo hacia el cliente. Dichos casos los examinará directamente el Director de Operaciones y se levantará un caso de investigación. En caso de que ocurra un acto o incidente de dicha naturaleza, el Supervisor de Seguridad o un representante del cliente, deberán reportarlo inmediatamente para que sea investigado y tomarán de común acuerdo las acciones conducentes para corregir el asunto y aplicar las sanciones necesarias dependiendo de la gravedad y magnitud del incidente en cuestión.

Seguridad en el envío y recepción de mercancía.

Dada la naturaleza de nuestro negocio, muchas de nuestras actividades cotidianas están intrínsecamente relacionadas con la logística de envío y recepción de mercancías; para este proceso será importante asegurar que exista un esquema logístico debidamente organizado y estructurado para gestionar adecuadamente el tráfico de los bienes en el interior de nuestras instalaciones.

Instalaciones

La entrada exterior al área de recepción de mercancía está vigilada por cámaras digitales del sistema de CCTV y por una alarma en el acceso de la cortina metálica enrollable; el control del sistema se ubicará por la parte interior del recinto de almacenaje. La entrada al área desde el interior de las instalaciones estará restringida y controlada por lectoras de exploración de proximidad magnética. El área de almacenaje y maniobras se encuentra equipada con un montacargas con capacidad para 2000 Kg., una plataforma de carga mecánica y otros medios de apoyo para el traslado de las mercancías. Se cuenta con los contenedores necesarios para depositar los desechos de los embalajes y los desperdicios propios del equipo ingresado al almacén. Deberá existir un lugar para almacenamientos de corto plazo, para la recepción del equipo de los clientes. Dicho lugar deberá contar con anaqueles abiertos y gavetas cerradas para guardas pequeñas partes electrónicas de valor.

Sistema de Notificación:

La metodología para poder notificar y llevar el registro de lo que se recibe es a través del correo electrónico (Email) por medio del cual se notifica a las áreas involucradas para su conocimiento de que ya se encuentra a disposición el equipo, materiales y/o accesorios en tráfico; además de que se cuenta con un registro contable de entradas y salidas de almacén para control del inventario activo.

II. ESPECIFICACIÓN DE LOS SISTEMAS ALOJADOS EN EL SITE INTERNO

II.1 Seguridad Física:

Para el acceso al SITE interno ubicado en Oficinas Centrales del Instituto se integra por los siguientes controles de seguridad:

Acceso general al edificio: Seguridad perimetral cuenta con personal de seguridad, control de acceso a base de torniquetes operados por control de tarjeta de identificación de proximidad y código HID por usuario.

Acceso al SITE interno: Ubicado en el primer piso del edificio, protegido con control de acceso biométrico,

personal de seguridad y circuito cerrado de televisión (CCTV) con 6 cámaras que cubren todo el sitio.
Se cuenta con 3 extintores de incendio para circuitos electrónicos como medida de protección contra incendio.
La instalación eléctrica es independiente y se encuentra integrada a un sistema de protección y respaldo de energía regulada redundante, así como respaldado por una planta de energía de 500 KVA.

II. 2 Características de seguridad lógica:

- La solución de seguridad lógica es realizada con equipos en alta disponibilidad.
- La solución de seguridad no es factor de latencia adicional en las redes por razones de su desempeño.
- La configuración y operación de este sistema de seguridad, en lo que respecta al servicio que servirá al SITE interno de Datos INEA es administrado en todo momento por personal de la Subdirección Técnica del INEA.

SEGURIDAD EN EL SITE INTERNO DE DATOS

- La Subdirección Técnica es la encargada de instalar, administrar, monitorear, mantener y actualizar, los dispositivos en Disposición antes mencionados
- El SITE interno de datos cuenta con línea de defensa, que al menos ofrece servicios de firewall (dispositivo perimetral de protección de datos), antivirus, antispam, VPN y detección y prevención de intrusos. Estos servicios cuentan con las siguientes características:

Firewall

- Firewall (Stateful inspection Firewall) en esquema de alta disponibilidad y con balanceo de cargas con interfaces suficientes para la solución de sistemas del Instituto.
- Soporta la creación de VPN's usando los algoritmos más comunes de encripción (DES, 3DES, AES, etc.) y en esquemas site-to-site y client-to-site
- Incluye prevención de ataques de negación de servicios distribuidos (DDoS)

Sistema de Detector de Intrusos

Ofrece un sistema de detección y prevención de intrusos que permite la correcta y oportuna identificación de ataques, que por lo menos proporciona lo siguiente:

- El sistema de prevención y detección de intrusos esta en un esquema de alta disponibilidad y de balanceo de cargas con interfases suficientes para la los servicios internos del INEA.

- **Detección de ataques e intrusos:** Basada en firmas, anomalías estadísticas, protocolos, de situaciones de negación de servicio y basados en Host.
- **Rechazo de intrusos:** Posibilidad de configurar el sistema para rechazar o eliminar automáticamente las conexiones no deseadas.

Protección contra virus y antispam (correo no deseado)

- Protección de antivirus de gateway para la infraestructura del SITE interno de datos del INEA contra código malicioso que sea capaz de explorar al menos en los protocolos http, ftp, smtp, y pop3.
- El antispam, cuenta con los siguientes métodos para detección de SPAM:

- Listas blancas y negras.
- Filtrado por contenido (asunto y cuerpo del mensaje).
- DNS-based Blackhole Lists
- Reputation Filtering o similar.

II.3 Acceso a Sistemas de protección de datos ubicado en el SITE interno del Instituto

Solo el personal "*responsable*" y "*encargado*" de la infraestructura y sistemas operativos está autorizado para acceder lógicamente a los servidores de las aplicaciones que contienen los sistemas que alojan datos personales, además de los usuarios de las mismas aplicaciones.

II.4 Respaldos Físicos y lógicos:

El respaldo de la información en medios físicos es realizada por un robot de cintas en medio magnético, discos duros de servidores, integrados en el SITE interno.

ANEXO II

DIRECCIÓN DE ACREDITACIÓN Y SISTEMAS
SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN

FORMATO DE NOTIFICACIÓN DE CONTRASEÑA DE ACCESO A SISTEMAS DE INFORMACIÓN

Centro de Trabajo:	**Nombre del Centro de Trabajo:**	**Fecha de Elaboración:**
Clave del Sistema:	**Nombre del Sistema:**	
Área de Adscripción:	**Puesto o cargo:**	

Nombre:	**Apellido Paterno:**	**Apellido Materno:**
Número de Empleado:	**Clave de Usuario del Sistema:**	**Tipo de Usuario:** **Administrador ( ) Operativo ( ) Consulta (x)**
Nombre del Responsable del Sistema y/o Módulo:	**Puesto o Cargo:**	

ATRIBUTOS ASIGNADOS PARA OPERAR LOS MOVIMIENTOS EN EL SISTEMA

Altas:	Bajas:	Modificar:	Consultar:
Rol Operativo			

FUNCIONES GENERALES

FUNCIONES QUE REALIZA EN EL SISTEMA

De conformidad con lo dispuesto en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2005, manifiesto estar de acuerdo como usuario del sistema y al perfil que me fue asignado de las siguientes responsabilidades:

- La **Clave de Acceso será secreta y conocida solo por el Usuario Responsable.**
- El Usuario del sistema tiene la **responsabilidad de cambiar la clave de acceso al menos cada tres meses y solicitar su cancelación en caso de rotación del personal.**
- Es **responsabilidad total del usuario del sistema, el mal uso que se pueda dar a la clave de acceso al sistema y sancionado de acuerdo a la normatividad aplicable dentro de la organización.**

Autoriza: **Acepto:**

Se debe proporcionar una copia para el expediente del Usuario del Sistema y el Original obrará en poder del Titular del Área. Anexar Copia de identificación del usuario del site

ANEXO III

RELACIÓN DE FIRMAS DE ENCARGADOS

ÁREA: DIRECCIÓN DE ACREDITACIÓN Y SISTEMAS

NOMBRE	FIRMA	FECHA
JUAN FROYLAN LÓPEZ MORALES		
LAURA ELENA MARIN BASTARRACHEA		
JUAN GABRIEL MERCADO ESCOBAR		
CARLOS ALBERTO GUTIÉRREZ GUTIÉRREZ		

ÁREA: DIRECCIÓN ACADÉMICA

NOMBRE	FIRMA	FECHA
MARIA DE LOURDES ARAVEDO RESENDIZ		

ÁREA: DIRECCIÓN DE PLANEACIÓN, ADMINISTRACIÓN, EVALUACIÓN Y DIFUSIÓN

NOMBRE	FIRMA	FECHA
VICTOR BELTRÁN SÁNCHEZ DE APARICIO		
BETZABE PRIETO ESCUTIA		

ÁREA: DIRECCIÓN DE ASUNTOS INTERNACIONALES

NOMBRE	FIRMA	FECHA
JORGE ALBERTO DÍAZ STRINGEL		

ANEXO IV

Nombre: Alma Delia García Altamirano
Cargo: PB3
Funciones: Registrar datos personales, laborales, percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales.
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Sofía Gutiérrez Aguirre
Cargo: Técnico Superior
Funciones: Registrar datos personales, laborales, percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales
Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Maria del Rosario de León García
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar datos personales, laborales, percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales
Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Nelly Velázquez Gallegos
Cargo: Jefe de Oficina
Funciones: Registrar datos personales, laborales, percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales
Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: María Eugenia Parrilla Luna
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales
Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Mónica Reyes Zamora
Cargo. Técnico Superior
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales
Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Mariana Zamora Ocampo
Cargo: Analista Administrativo
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales

Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Nidia Sánchez Orozco
Cargo. Secretaria C
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto y Prestadores de Servicios Profesionales
Obligaciones: Confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Laura Gutiérrez Arias
Cargo: Técnico Superior
Funciones: Procesamiento de nómina
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Cecilia López Sánchez
Cargo: Técnico Superior
Funciones: Procesamiento de nómina
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Margarita Sánchez de Aparicio y Duhalt
Cargo: Técnico Superior
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Jorge Lagunas García
Cargo: Analista Administrativo
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: José Alejandro Herrero Robles
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Mireya Martínez Asiain
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Flor Silvestre Saavedra Martínez
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto

Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Rosa Ángela Arellano Carrillo
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.

Nombre: Israel Ávila Reyes
Cargo: Profesional Dictaminador de Servicios Especializados
Funciones: Registrar percepciones y deducciones de los trabajadores del Instituto
Obligaciones: confiabilidad y discrecionalidad sobre la información que se registra y se encuentra en el Sistema.