Medidas de seguridad nivel Alto

Documento de seguridad

El responsable del sistema elaborará, difundirá e implementará la normativa de seguridad mediante el documento. Será de observancia obligatoria para todas las autoridades y funcionarios de la Universidad Veracruzana, así como para toda aquella persona que debido a la prestación de un servicio tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos. Deberá contener, como mínimo:

I. Nombre del Sistema de Datos Personales (SDP)

Nombre del Sistema de Datos Personales, debe coincidir con el reportado en el Anexo I (encabezado) para el Acuerdo y con el Registrado en el Instituto

II. Cargo y adscripción del responsable del sistema de datos personales

Cargo y adscripción del Responsable del Sistema de Datos Personales registrado en el Anexo I (fracción VII) para la creación del acuerdo y ante el IVAI

III. Ámbito de aplicación

Nombre de la Dependencia(s) en donde se aplique el sistema y describir brevemente las áreas o departamentos a los que les aplica este documento (basándose en las personas que intervengan en el tratamiento de los SDP)

IV. Estructura y descripción del sistema de datos personales y V. Especificación detallada de la categoría de datos personales

Estructura básica del Sistema, debe coincidir con el reportado en el Anexo I (fracción V) para el Acuerdo y con el Registrado en el IVAI.

Datos identificativos:	
Datos electrónicos:	
Datos laborales:	
Datos patrimoniales:	
Datos sobre procedimientos administrativos y/o jurisdiccionales:	
Datos académicos:	
Datos de tránsito y movimientos migratorios:	
Datos sobre la salud:	
Datos biométricos:	
Datos especialmente protegidos (sensibles):	

VI. Funciones y obligaciones del responsable del sistema de datos personales, del encargado del tratamiento de datos personales y de toda persona que intervenga en el tratamiento de los sistemas de datos personales.

Las funciones y obligaciones de todos los que intervengan en el tratamiento de datos personales deben estar claramente definidas en el documento de seguridad. El responsable del sistema de datos personales adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

* Responsable del SDP:
* Encargados del tratamiento de DP (secretarias, asistentes, administradores, etc.)

Nombre	Cargo	Funciones	Obligaciones

VII. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido por la Ley 581

Identificación y autentificación

El responsable del sistema de datos personales tendrá a su cargo la elaboración de una relación actualizada de servidores públicos que tengan acceso autorizado al sistema de datos personales y de establecer procedimientos que permitan la correcta identificación y autenticación para dicho acceso.
El responsable del sistema de datos personales establecerá un mecanismo que permita la identificación, de forma inequívoca y personalizada, de toda aquella persona que intente acceder al sistema de datos personales y la verificación de que está autorizada.
Cuando el mecanismo de autenticación se base en la existencia de contraseñas se establecerá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y se conservarán cifradas.
Asimismo, se establecerá un procedimiento de creación y modificación de contraseñas (longitud, formato, contenido).

Control de acceso

El responsable del sistema de datos personales deberá adoptar medidas para que los encargados del tratamiento de datos personales y usuarios tengan acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
El responsable del sistema de datos personales deberá mantener actualizada una relación de personas autorizadas y los accesos autorizados para cada una de ellas. Asimismo, deberá establecer los procedimientos para el uso de bitácoras respecto de las acciones cotidianas llevadas a cabo en el sistema de datos personales.
Solamente el responsable del sistema de datos personales podrá conceder, alterar o anular la autorización para el acceso a los sistemas de datos personales.

Gestión de soportes

Al almacenar los soportes físicos y electrónicos que contengan datos de carácter personal se deberá cuidar que estén etiquetados para permitir identificar el tipo de información que contienen, ser inventariados y sólo podrán ser accesibles por el personal autorizado para ello en el documento de seguridad.

La salida de soportes y documentos que contengan datos de carácter personal, fuera de las instalaciones u oficinas bajo el control del responsable del sistema de datos personales, deberá ser autorizada por éste, o encontrarse debidamente autorizada en el documento de seguridad. En el traslado de soportes físicos y electrónicos se adoptarán medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Siempre que vaya a desecharse cualquier soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

VIII. Procedimientos de notificación, gestión y respuesta ante incidencias

Los procedimientos de notificación gestión y respuesta ante incidencias contarán necesariamente con un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las acciones implementadas.

Tipo de incidencia (descripción)	Fecha y hora en que se produjo	Nombre de quien notifica la incidencia	A quien se reporta (persona que recibe la notificación)	Efectos/consecuencias derivados de la incidencia	Acciones implementadas

IX. Procedimientos para la realización de copias de respaldo y recuperación de los datos, para los sistemas automatizados;

Copias de respaldo y recuperación

Deberán establecerse procedimientos para la realización de copias de respaldo y su periodicidad. En caso de que los datos personales se encuentren en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos.

Asimismo, para soportes electrónicos se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental.

El responsable del sistema de datos personales se encargará de verificar, al menos, cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

X.-Procedimiento para la realización de auditorías, en su caso.

Además deberá cumplir con lo siguiente:

Responsable de seguridad
El responsable del sistema de datos personales designará uno o varios responsables de seguridad para coordinar y controlar las medidas definidas en el documento de seguridad. Esta designación podrá ser única para todos los sistemas de datos en posesión del ente público, o diferenciada, dependiendo de los métodos de organización y tratamiento de los mismos. En todo caso dicha circunstancia deberá especificarse en el documento de seguridad.
En ningún caso esta designación supone una delegación de las facultades y atribuciones que corresponden al responsable del sistema de datos personales de acuerdo con la Ley y los Lineamientos.

Auditoría
Las medidas de seguridad implementadas para la protección de los sistemas de datos personales se someterán a una auditoría interna o externa, mediante la que se verifique el cumplimiento de la Ley, de los presentes Lineamientos y demás procedimientos vigentes en materia de seguridad de datos, al menos, cada dos años. La auditoría interna podrá realizarse a través del órgano de control interno del ente público.
El informe de resultados de la auditoría deberá dictaminar sobre la adecuación de las medidas de seguridad previstas en los Lineamientos, así como en las recomendaciones, que en su caso, haya emitido el Instituto. Además, deberá identificar sus deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias.
El informe de auditoría deberá ser comunicado por el responsable del sistema de datos personales al Instituto dentro de los veinte días hábiles siguientes a su emisión. Asimismo, se deberá informar al Instituto de la adopción de las medidas correctivas derivadas de la auditoría en el plazo referido, a partir de que éstas hayan sido atendidas.

Control de acceso físico
El acceso a las instalaciones donde se encuentren los sistemas de datos personales, ya sea en soporte físico o electrónico, deberá permitirse exclusivamente a quienes estén expresamente autorizados en el documento de seguridad.

Pruebas con datos reales
Las pruebas que se lleven a cabo con efecto de verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados.
Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo.

Distribución de soportes

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos, o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión.

Registro de acceso

El acceso a los sistemas de datos personales se limitará exclusivamente al personal autorizado, estableciendo mecanismos que permitan identificar los accesos realizados en el caso en que los sistemas puedan ser utilizados por múltiples autorizados.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad correspondiente, sin que se permita la desactivación o manipulación de los mismos.

De cada acceso se guardarán, al menos, la identificación del usuario, la fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si éste fue autorizado o denegado.

El periodo de conservación de los datos consignados en el registro de acceso será de, al menos, dos años.

Telecomunicaciones

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.