Anáhuac México

Procedimiento de gestión de incidentes en materia de Protección de Datos Personales de la Universidad Anáhuac México

Documento aprobado el 5 de octubre de 2020

Comisión de Protección de Datos Personales

CONTENIDO

Objetivo

Identificación

Detección

Registro del incidente

Categorización

Tiempo de atención

Equipo de respuesta

Recolección de evidencia

Contención

Notificación

Informe de contención

Mitigación

Transitorio

<< Volver al inicio

1. Objetivo

El presente procedimiento tiene el objetivo de gestionar incidentes de seguridad y privacidad de la información (lo que se denominará incidentes de seguridad), teniendo en cuenta los lineamientos y estándares definidos a través de una oportuna identificación, atención y respuesta, con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de los datos personales en posesión de la Universidad Anáhuac México.

La gestión de incidentes de seguridad inicia en la identificación, detección, contención y mitigación de estos, finalizando con la generación de pruebas y la documentación del proceso.

2. Identificación

El personal que identifique el posible incidente de seguridad debe reunir la información que lo llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención de este, como pueden ser capturas de pantalla, correos electrónicos, fotografías, videos, entre otros. Dicho incidente deberá notificarlo inmediatamente a la Comisión de Protección de Datos Personales de la Universidad Anáhuac México mediante el formato del Anexo 1, ya sea de forma física en la oficina o a los correos electrónicos privacidad.norte@anahuac.mx o privacidad.sur@anahuac.mx, según sea el caso.

3. Detección

Una vez recibido el reporte del posible incidente de seguridad, la Comisión de Protección de Datos Personales debe realizar la primera categorización del incidente para iniciar con la atención del mismo, de acuerdo con los siguientes criterios:

I. La pérdida o destrucción no autorizada.
II. El robo, extravío o copia no autorizada.
III. El uso, acceso o tratamiento no autorizado.
IV. El daño, bloqueo, alteración o modificación no autorizada.

<< Volver al inicio

4. Registro de incidente

Todos los incidentes de seguridad deberán ser registrados y contabilizados con un número de folio consecutivo, asignado por el encargado de la Comisión de Protección de Datos Personales de la Universidad Anáhuac México.

5. Categorización

Una vez clasificado el incidente de seguridad, este deberá ser categorizado de acuerdo con su impacto y urgencia, basándose en la siguiente tabla:

Impacto	Descripción	Valoración
Catastrófico	Extremadamente dañino: Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la Universidad Anáhuac México, cuando se presente alguno de los siguientes casos: • Pérdidas económicas superiores a los $500,000.00 (quinientos mil pesos). • Afectación de la imagen de la Universidad Anáhuac México a nivel nacional e internacional. • Se actualice algún delito. • Daños totales de la infraestructura de la Universidad Anáhuac México. • Se vulneren los datos personales de más de quinientas a mil personas, tratándose de datos personales sensibles.	**ALTA**
Mayor	Dañino (Mayor): Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la Universidad Anáhuac México cuando se presente alguno de los siguientes supuestos:	

	• Pérdidas económicas entre $250,000.00 (doscientos cincuenta mil pesos) y $500,0000.00 (quinientos mil pesos). • Afectación de la imagen de la Universidad Anáhuac México a nivel nacional. • Daños parciales de la infraestructura de la Universidad Anáhuac México. • Se vulneren los datos personales de más de doscientas a quinientas personas, tratándose de datos personales sensibles.	
Moderado	Moderado: Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la Universidad Anáhuac México cuando se presente alguno de los siguientes supuestos: • Pérdidas económicas entre $100,000.00 (cien mil pesos) y $250,000.00 (doscientos cincuenta mil pesos). • Afectación de la imagen de un proceso o área de la Universidad Anáhuac México. • Daños parciales a la infraestructura que afecten la denegación de dos o más servicios de la Universidad Anáhuac México. • Se vulneren los datos personales de más de cincuenta a cien personas, tratándose de datos personales sensibles.	**MEDIA**
Menor	Menor: Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la Universidad Anáhuac México cuando se presente alguno de los siguientes supuestos: • Pérdidas económicas de entre $50,000.00 (cincuenta mil	**BAJA**

	pesos) y $100,000.00 (cien mil pesos). • Afectación de la imagen de un grupo de personas que pueda vincularse a la Universidad Anáhuac México. • Daños pequeños a la infraestructura de la Universidad. • Se vulneren los datos personales de diez a cincuenta personas, tratándose de datos personales sensibles.	
Insignificante	Ligeramente dañino: Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la Universidad Anáhuac México cuando se presente alguno de los siguientes supuestos: • Pérdidas económicas entre $100,000.00 (cien mil pesos) y $250,000.00 (doscientos cincuenta mil pesos). • Se vulneren los datos personales de diez a cincuenta personas, tratándose de datos personales sensibles.	

6. Tiempo de atención

De acuerdo con la valoración de los incidentes, estos deberán atenderse antes de los siguientes plazos:

I. Tratándose de incidentes con el nivel de valoración Alta, deberá atenderse en un plazo menor de dos horas naturales.

II. Tratándose de incidentes con el nivel de valoración Media, deberá atenderse en un plazo menor de ocho horas naturales.

III. Tratándose de incidentes con el nivel de valoración Baja, deberá atenderse en un plazo menor de doce horas naturales.

Los tiempos expresados son el plazo máximo en los que los incidentes deben ser atendidos, y no los tiempos en los que deben ser solucionados. Esto se debe a que la solución de los incidentes puede variar, dependiendo del caso.

<< Volver al inicio

7. Equipo de respuesta

Una vez recibido el informe del incidente de seguridad, el encargado de la Comisión de Protección de Datos Personales solicitará reunir al equipo de respuesta, que estará integrado por una persona del área que custodie los datos personales, el profesional de la Dirección de Tecnologías de la Información y el encargado de la Comisión de Protección de Datos Personales.

El equipo de respuesta podrá solicitar información o la participación de otros colaboradores, procesos, especialistas y/u operadores estratégicos requeridos para la atención del incidente de seguridad, quien solo tendrá derecho de voz.

8. Recolección de evidencia

El equipo de respuesta deberá recopilar evidencia y ponerla bajo su custodia, con el fin de reducir la probabilidad de que esta se modifique y sea considerada no admisible ante la autoridad competente. Dependiendo de la evidencia que se genere en el tratamiento del incidente, el equipo de respuesta determinará el lugar en donde se conservarán. En todo caso, las evidencias recolectadas deberán permanecer en formatos físicos o dispositivos de almacenamiento extraíble, sellados y firmados por el responsable del área vulnerada.

9. Contención

El equipo de respuesta deberá realizar las acciones necesarias para realizar la contención de la vulneración, con el objetivo de evitar que se continúe ejecutando la vulnerabilidad. Las acciones podrán ser, de forma enunciativa más no limitativa, las siguientes:

<< Volver al inicio

Tipo de incidente	Causas comunes	Posibles acciones de contención
Acceso no autorizado	**Acceso físico:** Las causas comunes son la permisividad e inexistencia de control de instalaciones internas. Estas pueden ser por personas internas y externas. **Acceso digital:** Configuraciones por defecto, errores de aplicación, vulnerabilidades o parches de seguridad no aplicados, error humano en el acceso no autorizado o divulgación no autorizada de datos personales, entre otros.	Identificar a la persona que infringe la normativa interna, indagar motivos por los cuales se encuentra en instalaciones sin autorización, identificar las causas que permitieron su ingreso. Para el acceso digital es algo más complejo: las acciones a tomar dependerán del tipo y gravedad del incidente. Revisión de registros, recuperar el servicio afectado, correlación de accesos, permisos, horas, nombres de usuario, origen y otros.
Ataques por vulnerabilidades	Vulnerabilidades de día cero, versiones de aplicación desactualizadas o descontinuadas, entre otros.	Identificar el sistema y/o servicio afectado; activar los respaldos de información, dependiendo de la gravedad; detener el servicio; restaurar las configuraciones y la información anterior.
Código malicioso	Campañas de phishing, uso descontrolado de dispositivos de almacenamiento, acceso a páginas sospechosas, vulnerabilidades a nivel de red que faciliten la propagación.	Identificar el tipo de código malicioso, aislar equipos comprometidos de la red, monitorear el tráfico de red, analizar el comportamiento del código malicioso, entre otras acciones.

Denegación de servicio que no permita el acceso a los datos personales	Generalmente ocurren por motivos intencionados que buscan restringir el acceso y la disponibilidad de servicios, aprovechando cambios incontrolados de configuración, mal funcionamiento de *hardware,* incidentes no intencionados, errores incontrolados en sistemas y otros.	Identificar el origen del ataque y bloquear el mismo, esto si no se trata de una denegación distribuida. Para su prevención se recomienda implementar reglas para identificar y bloquear automáticamente estos ataques.
Divulgación de información	Accesos no autorizados a instalaciones con información confidencial o datos personales expuestos en lugares visibles sin seguridad.	Este tipo de incidentes debe tener tratamiento especial, porque la finalidad no es restablecer servicios. Las acciones deberían estar orientadas al análisis de las causas, origen y responsables, para prevenir futuros incidentes.

10. Notificación

Después de la contención se deberá informar al titular de los datos personales las vulneraciones cuando sean catalogadas como mayor y catastróficas en un plazo menor a 72 horas naturales, con la intención de que el titular pueda tomar las medidas correspondientes para proteger sus intereses.

Dicha notificación deberá tener mínimo la siguiente información:

I. La naturaleza del incidente.
II. Los datos personales comprometidos.
III. Las recomendaciones al titular acerca de las medidas que pueda adoptar para proteger sus intereses.

IV. Las acciones correctivas realizadas de forma inmediata.

V. Los medios donde puede obtener más información al respecto.

Las notificaciones podrán realizarse por teléfono, correo electrónico, correo postal o en persona. En caso de que exista urgencia por contactar al titular, puede resultar oportuno utilizar más de un medio de contacto a la vez.

Se puede optar por la notificación indirecta a través de sitios web o medios de comunicación masivos solamente cuando la notificación directa pueda causar más afectaciones al titular, sea muy costosa o no se tenga información de contacto.

11. Informe de contención

El equipo de respuesta deberá realizar un informe en el que se especifiquen y documenten todas las acciones de la contención. Dicho informe deberá ser firmado por todos los integrantes del equipo. La experiencia adquirida deberá permitir mejorar las acciones de respuesta para futuros incidentes con similar característica.

El equipo de respuesta podrá solicitar la colaboración de las personas internas o externas necesarias para la contención, mitigación y resolución del incidente de seguridad.

12. Mitigación

Una vez realizada la contención, se deberá realizar un informe que establezca las medidas de mitigación o erradicación, con el objeto de reforzar las medidas de seguridad en el área o sistema vulnerado. En dicho informe se deberán establecer las medidas de seguridad existentes y la mejora que se realizará, así como el plazo para realizarlas.

El informe de mitigación deberá ser notificado a la Comisión de Protección de Datos Personales de la Universidad Anáhuac México para darle seguimiento al cumplimiento.

La experiencia adquirida en la atención al incidente de seguridad, así como toda la información obtenida durante la atención, deberá permitir elaborar un plan semestral de acción de mejora continua en materia de seguridad de la información y protección de datos personales, con el objeto de fortalecer la seguridad de la Universidad Anáhuac México para evitar la repetición de incidentes similares en el futuro.

En caso de que el incidente de seguridad actualice posiblemente algún delito previsto en la normatividad competente, el encargado de la Comisión de Protección de Datos le dará aviso a la Gerencia Jurídica quien a su vez informará al Vicerrector de Administración y Finanzas, con el objeto de iniciar las acciones correspondientes.

En caso de que el personal de la Universidad Anáhuac México haya actuado en la realización de la vulneración con acciones u omisiones, se deberá hacer de conocimiento a la Comisión de Protección de Datos Personales para que, a su vez, se le informe a la Comisión Consultiva y Disciplinaria de la Universidad.

Lo anterior no exime al personal de responsabilidades administrativas, civiles, penales o de cualquier otra índole externa de la Universidad.

Transitorio

Único.

El presente Procedimiento entrará en vigor al día siguiente de la aprobación de dos tercios de los integrantes de la Comisión de Protección de Datos Personales de la Universidad.

Anáhuac
México

Campus Norte
Av. Universidad Anáhuac núm. 46,
col. Lomas Anáhuac, Huixquilucan,
Estado de México, C.P. 52786
Tel.: 55 56 27 02 10

Campus Sur
Av. de los Tanques núm. 865,
col. Torres de Potrero, Álvaro Obregón,
Ciudad de México, C.P. 01840
Tel.: 55 56 28 88 00

Departamento de Datos Personales
Tel.: 55 56 27 02 10 ext. 8675
privacidad.norte@anahuac.mx
privacidad.sur@anahuac.mx

anahuac.mx/mexico