



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Sistema de Gestión de Seguridad de Datos Personales

Marzo 2020

Presentación.

La Unidad de Transparencia fue creada a través del Acuerdo por el que se constituyen la Unidad de Transparencia y el Comité de Transparencia de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 18 de abril de 2016.

Desde su creación, ha fomentado la transparencia y accesibilidad a la información al interior de la Universidad, posibilitando la rendición de cuentas, con información sobre el ejercicio de sus facultades y recursos, los resultados obtenidos y las razones de sus decisiones.

Este documento tiene el objetivo de documentar las actividades realizadas para integrar nuestro Sistema de Gestión de la Seguridad de Datos Personales en la Unidad de Transparencia. Se trata de la primera versión del documento, el cual se enriquecerá conforme se vayan cumpliendo las tareas trazadas en el mismo, se hagan verificaciones de medidas implantadas o se cree o modifique sustancialmente algún sistema de tratamiento de datos personales.

El alcance de este sistema se centra en proteger “Todos los datos personales y datos personales sensibles que recabe y trate la Unidad de Transparencia” de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados.

Sistemas de Tratamiento de Datos Personales

Uno de los procesos más importantes en la Unidad de Transparencia es la de recibir y dar trámite a las solicitudes de acceso a la información, así como a las de acceso, rectificación, cancelación y oposición de datos personales (ARCO), en cumplimiento de lo dispuesto por el artículo 6°, apartado A, fracciones III y IV de la CPEUM:

“III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos. IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados e imparciales que establece esta Constitución.”

El mandato constitucional es recogido por la LGTAIP, la LFTAIP y el RTAIP, en los cuales se detalla el procedimiento de acceso a la información. Para apoyar estas actividades, en la Unidad se cuenta con el siguiente sistema:

Sistema de gestión de solicitudes de acceso a la información y de datos personales.

Este sistema se encarga de dar seguimiento a las solicitudes de acceso a información pública y de datos personales o de recursos de revisión que se presenten ante la UNAM a través de la Plataforma Nacional de Transparencia y a través del correo electrónico institucional de la Unidad.

A este sistema tienen acceso todo el personal de la Unidad de Transparencia que se dedica a dar seguimiento de cada solicitud de información

En el sistema de gestión se guarda la información del solicitante y de la propia solicitud en la cual puede o no traer información de datos personales. La información derivada del seguimiento a la solicitud, como son las respuestas de las áreas universitarias, deliveraciones con estas y la respuesta final se guarda en 3 herramientas adicionales:

Repositorio de Archivos. Aquí se guarda todo el registro documental electrónico de una solicitud incluyendo la información relacionada a recursos de revisión

Archivo físico de la Unidad. Aquí se guardan los expedientes físicos de las solicitudes de información y copia de las respuestas de las áreas cuando estas son enviadas en un soporte físico

Correo institucional. En esta herramienta se recibe la información electrónica que un área institucional proporciona para atender una solicitud de información o un recurso de revisión en específico, no en todos los casos, dicha documentación contiene datos personales.

El detalle de los datos personales que se manejan en cada componente del sistema se describe en los *Anexos 1.1 Inventario de sistemas de tratamiento de datos personales*

Roles y responsabilidades de los involucrados en el tratamiento de datos personales.

Sistema de gestión de solicitudes de acceso a la información y de datos personales

Los perfiles de personas que participan en el tratamiento de datos personales son los siguientes:

Titular de la Unidad. **Revisa y asigna cada solicitud al personal de la Unidad encargada del seguimi**

Subdirectores. **Daseguimiento al trabajo realizado por sus colaboradores en la gestión de cada solicitud de información.**

Coordinadora de Protección de Datos Personales. **Encargada de definir políticas de protección de datos personales y atender solicitudes de derechos ARCO.**

Ejecutivos de cuenta. **Da seguimiento a cada solicitud, recaba las respuestas dadas por las áreas universitarias, integra la respuesta final, comunica la respuesta al solicitante y a la Plataforma Nacional de Transparencia**

Secretaria del Titular. **Encargada de capturar la información de de las solicitudes en el sistema de gestión.**

Personal de Unidad Administrativa. **Encargado de resguardar el archivo físico de la Unidad de transparencia**

Coordinador de sistemas. **Encargado de resguardar la información de las bases de datos y de los documentos de respuestas y de los servidores que contienen dicha información.**

Personal de sistemas de la Unidad. **Encargados de desarrollar actualizaciones al sistema de gestión, elaborar respaldos y actualizar los servidores que contienen dicha información.**

El detalle con las funciones y reponsabilidades de cada perfil está descrito en el *Anexo 2 Funciones y obligaciones de quienes traten datos personales*

Análisis de riesgos en el tratamiento de datos personales.

El detalle del análisis de riesgos está descrito en el *Anexo 3 Análisis de riesgos en el tratamiento de datos personales*

Análisis de Brecha.

Una vez identificado los controles necesarios para mitigar los riesgos encontrados en nuestros activos de información, se hace un Análisis de Brecha por medio del cual se identifica lo siguiente:

- I. Las medidas de seguridad existentes y efectivas;
- II. El nivel óptimo de medidas de seguridad y
- III. Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

El detalle de las actividades de esta análisis está descrito en el *Anexo 4 Análisis de Brecha*

Plan de Trabajo.

Una vez realizado el análisis de riesgos y haber identificados los controles faltantes para mitigar cada riesgo, se hace un plan para implementar los controles de seguridad faltantes, en cual se identifican estos controles, las actividades a realizar para implementar el control, el tiempo estimado para completar las actividades, la prioridad que se dará a dicho control y finalmente, las áreas responsable(s) de su implementación.

El detalle de las actividades de esta plan está descrito en el *Anexo 5 Plan de Trabajo*

Ruta Crítica para cumplimiento de las medidas de seguridad técnicas (MST).

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de

información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional .unam.mx.

A) Etapa 1. Corto plazo. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.

B) Etapa 2. Mediano plazo. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.

C) Etapa 3. Largo plazo. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses.

En esta versión del documento se registran las actividades realizadas para cumplir con lo dispuesto para la etapa 1 en el Anexo 6. Formatos para cumplimiento de las MST.

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Alfredo Alonso Peña Coordinador de Sistemas Tel. 5556228660 ext. 41661 alfredo.alonso@comunidad.unam.mx	
Revisó:	Lorena Pichardo Flores Coordinadora de Protección de Datos Personales Tel. 5556228660 ext. 41661 lpichardo@unam.mx	
Autorizó:	José Meljem Moctezuma Titular de la Unidad de Transparencia Tel. 5556220472 jmeljem@unam.mx	
Fecha de aprobación:		13/03/2020
Fecha de actualización:		21/04/2021



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Anexos

Marzo 2020



¡Universidad Abierta y Transparente!

Unidad de Transparencia

Anexo 1

Inventario de sistemas de tratamiento de datos personales

Marzo 2020

Sistema de Gestión de Solicitudes de Acceso a la Información y Protección de Datos Personales

Unidad de Transparencia	
Identificador único	UT/SGSAIDP
Nombre del sistema	<u>Sistema de Gestión de Solicitudes de Acceso a la Información y de Datos Personales</u>
Datos personales (sensibles o no) contenidos en el sistema	<p>Los datos personales contenidos son los solicitados en el formulario para hacer una solicitud de información y ejercicio de derechos ARCO en la Plataforma Nacional de transparencia.</p> <p>Nombre completo del solicitante o, en su caso, de su representante legal;</p> <p>Datos proporcionados en la descripción de la asesoría o solicitud o recurso respectivo;</p> <p>En su caso, nombre completo y domicilio del tercero interesado;</p> <p>Datos proporcionados en la documentación que en su caso adjunte (podrían contener datos sensibles);</p> <p>Datos contenidos en los documentos que se presenten y para acreditar la identidad del titular y del representante legal;</p> <p>Domicilio o medio para recibir notificaciones;</p> <p>En algunos casos, los siguientes datos sensibles: lengua indígena, la solicitud para no cubrir el pago de reproducción y envío y si tiene alguna discapacidad y desea proporcionar especificaciones de las preferencias de accesibilidad (lugar de estacionamiento para persona con discapacidad, acceso para perros o animales de apoyo, apoyo de lectura a documentos).</p>
Responsables	
Nombre	Ing. Gustavo Ernesto Ramírez Rodríguez
Cargo	<u>Subdirector de Acceso a la Información</u>
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información.</p> <p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar asignaciones de los colaboradores que atienden una solicitud.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud.</p> <p>Generar reportes estadísticos de los seguimientos a los folios.</p> <p>Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información.</p> <p>Efectuar las notificaciones a los solicitantes en los procedimientos de acceso a la información, constituyéndose como el vínculo entre la Universidad y el solicitante.</p>

Obligaciones*:	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p> <p>Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.</p>
Encargados	
Nombre del Encargado 1	Esther Vicente González
Cargo	Subdirectora de Obligaciones de Transparencia.
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información.</p> <p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar asignaciones de los colaboradores que atienden una solicitud.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud.</p> <p>Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información.</p> <p>Efectuar las notificaciones a los solicitantes en los procedimientos de acceso a la información, constituyéndose como el vínculo entre la Universidad y el solicitante.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo</p> <p>Utilizar el sistema de gestión de acuerdo a los permisos que les fueron otorgados y no más allá.</p>
Nombre del Encargado 2	Lorena Pichardo Flores
Cargo	Coordinadora de Protección de Datos Personales

Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información y en especial las de ejercicio de derechos ARCO.</p> <p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar asignaciones de los colaboradores que atienden una solicitud.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud.</p> <p>Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información.</p> <p>Efectuar las notificaciones a los solicitantes en los procedimientos de acceso a la información, constituyéndose como el vínculo entre la Universidad y el solicitante.</p> <p>Solicitar apoyo a otras áreas de la Unidad de Transparencia para agilizar el trámite de una solicitud de información.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo</p> <p>Utilizar el sistema de gestión de acuerdo a los permisos que les fueron otorgados y no más allá.</p>
Nombre del Encargado 3	Alfredo Alonso Peña
Cargo	Coordinador de Sistemas
Funciones	<p>Captura de información relacionada a los recursos de revisión.</p> <p>Generar Reportes ad hoc de la información contenida en la base de datos a petición del Subdirector de Acceso a la Información.</p>
Obligaciones	<p>Proteger los datos personales contenidos en el sistema de accesos no autorizados.</p> <p>Dictar políticas para el aseguramiento de los datos personales en los servidores y Bases de Datos de la Unidad de Transparencia</p> <p>Generar los respaldos de la información contenida en el sistema, siguiendo la política de respaldos de la Unidad de Transparencia.</p> <p>Generar respaldos del Sistema de Gestión, siguiendo la política de respaldos de la Unidad de Transparencia.</p> <p>Mantener actualizado el servidor donde se aloja el sistema de gestión.</p>
Usuarios:	
Coordinación de Sistemas	
Nombre de usuario 1	José Manuel Chicho Ortiz
Cargo	Jefe de Departamento

Funciones	<p>En caso de error en la captura de datos, apoyar a los usuarios en la modificación de los registros de datos, siempre y cuando no sea diferente a lo que está en la Plataforma Nacional de Transparencia.</p> <p>Generar Reportes ad hoc de la información contenida en la base de datos a petición del Subdirector de Acceso a la Información.</p> <p>Crear nuevos usuarios y asignar privilegios de acceso.</p>
Obligaciones	<p>Proteger los datos personales contenidos en el sistema de accesos no autorizados.</p> <p>Generar los respaldos de la información contenida en el sistema, siguiendo la política de respaldos de la Unidad de Transparencia.</p> <p>Generar respaldos del Sistema de Gestión, siguiendo la política de respaldos de la Unidad de Transparencia.</p> <p>Mantener actualizado el servidor donde se aloja el sistema de gestión.</p>
Dirección	
Nombre de usuario 2	Karla Hernández Ortega
Cargo	Secretaria particular de Dirección
Funciones	Capturar las nuevas solicitudes de información y ejercicio de derechos ARCO en el sistema de gestión.
Obligaciones	<p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p>
Subdirección de Acceso a la Información	
Nombre del Usuario 3	Elisa Funoy Cardenas
Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información.</p> <p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud.</p> <p>Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo</p>
Nombre del Usuario 4	Julio Cesar Laydes Villegas

Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud. Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo</p>
Nombre del Usuario 5	Daniel Alejandro Álvarez Palacios
Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud. Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p>
Coordinación de Protección de Datos Personales	
Nombre del Usuario 6	Verónica Lucrecia Rodríguez Martínez
Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información y en especial las de ejercicio de derechos ARCO.</p> <p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud. Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>

Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p> <p>Recibir a solicitantes en el Centro de Atención a Solicitantes y orientarlos para que puedan ejercer su derecho de acceso a la información.</p> <p>Entregar previa identificación las respuestas que dieron las áreas universitarias a los solicitantes</p>
Nombre del Usuario 7	Maria Guadalupe Pérez Mendoza
Cargo	Ejecutivo de cuenta
Funciones	<p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud.</p> <p>Recibir a solicitantes en el Centro de Atención a Solicitantes y orientarlos para que puedan ejercer su derecho de acceso a la información.</p> <p>Entregar previa identificación las respuestas que dieron las áreas universitarias a los solicitantes</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p> <p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas.</p> <p>Reconducir las solicitudes cuando lo que soliciten sean datos personales.</p> <p>Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p>
Subdirección de Obligaciones de Transparencia	
Nombre del Usuario 8	Ana Delia Vázquez Paz
Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información.</p> <p>Consulta información de datos personales (si los hay) de las solicitudes de información.</p> <p>Cambiar el área universitaria a la que será turnada una solicitud.</p> <p>Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes</p> <p>No modificar la información de datos personales contenidos en las solicitudes de información.</p>

	<p>No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p>
Nombre del Usuario 9	Patricia Guzmán Hernández
Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información. Cambiar el área universitaria a la que será turnada una solicitud. Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes No modificar la información de datos personales contenidos en las solicitudes de información. No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p>
Nombre del Usuario 10	Dolores J. Hernández Cortés
Cargo	Ejecutivo de cuenta
Funciones	<p>Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información. Cambiar el área universitaria a la que será turnada una solicitud. Notificar al solicitante las respuestas que se dio a una solicitud y si es el caso indicarle la forma de recoger la información de datos personales que solicitó.</p>
Obligaciones	<p>Proteger los datos personales de los solicitantes No modificar la información de datos personales contenidos en las solicitudes de información. No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Mantener la información de datos personales en el servidor de archivos de la Unidad y no generar copias de los documentos en sus equipos de trabajo.</p>



¡Universidad Abierta y Transparente!

Unidad de Transparencia

Anexo 2

Funciones y obligaciones de quienes traten datos personales

Marzo 2020



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Anexo 3.

Análisis de riesgos

Marzo 2020



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Anexo 4. Análisis de brecha

Marzo 2020



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Anexo 5.

Plan de Trabajo

Marzo 2020



¡Universidad Abierta y Transparente!

Unidad de Transparencia

Anexo 6

Formatos para cumplimiento de las MST

Marzo 2020



Sistema de gestión de solicitudes de acceso a la información y de datos personales - Desarrollo				SGSAIDP	
Formato	1	Verificación	ANUAL	Acción concluida	()
Medida de seguridad técnica:	Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.				
Aplicable en:	I. Bases de datos y sistemas de tratamiento.				
Tiempo estimado:	Un día hábil.				
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.				
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información, por medio de formato o comandos.</p> <p>C) Verificar que los datos usados en el desarrollo no correspondan a personas identificables.</p> <p>D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B.</p> <p>E) Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>				
Mejores prácticas, referencias:	<ol style="list-style-type: none"> 1. Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. 2. Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba. 				
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.				
Ejecución					
				Fecha inicio	
Alfredo Alonso Peña		Jose Manuel Chicho Ortiz		24/02/2020	
Nombre y firma				Fecha término	
Programador, desarrollador o diseñador del sistema de información				25/02/2020	
Observaciones / anotaciones					

Acciones realizadas

Las acciones realizadas para el Sistema de gestión de solicitudes de acceso a la información pública y de datos personales, fueron:

- Verificación de las siguientes tablas:
 - Solicitantes
 - Solicitudes
 - Recursos_revision
 - Enlaces
 - Dependencias
 - Usuario
 - Responsables_datos_personales
- Ingreso de datos aleatorios en los campos de las siguientes tablas:
 - Solicitantes
 - Soli_nom
 - Soli_ap_pat
 - Soli_ap_mat
 - Soli_calle
 - Soli_cp
 - Soli_razon_social
 - Soli_email
 - Solicitudes
 - Sol_desc
 - Sol_desc_add
 - Sol_med_ent_com
 - Sol_ruta_arc_adj
 - Sol_ruta_adj_ria
 - Recursos_revision
 - Recurso_acuerdo_admision
 - Recurso_pantalla_admision
 - Recurso_anexos
 - Enlaces
 - Enl_nombre
 - Enl_tel1
 - Enl_email1
 - Enl_email2
 - Enl_notas
 - Dependencias
 - Dep_titular
 - Dep_tel
 - Dep_email_titular
 - Dep_notas
 - Usuario
 - Usu_nombre
 - Usu_primerApellido
 - Usu_segundoApellido
 - Usu_email
 - Responsables_datos_personales

- Nombres
- primerApellido
- segundoApellido
- Telefono
- Extension
- Email
- Eliminación de Archivos (pdf,doc,docx,zip) de las siguientes carpetas:
 - Documentos
 - Adjuntos
 - Recursos
 - Seguimiento
- Se crea un archivo vacío como default para prueba de descarga de archivos.

Sistema de gestión de solicitudes de acceso a la información y de datos personales - Desarrollo				
Formato:	2	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.</p> <p>C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.</p> <p>D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B.</p> <p>E) Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<ol style="list-style-type: none"> 1. Definir niveles de acceso adecuados para cada perfil o tipo de usuario. 2. Tener un mínimo de administradores o usuarios con altos privilegios en el sistema. 			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
		Fecha inicio		
Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	25/02/2020		
Nombre y firma		Fecha término		
Programador, desarrollador o diseñador del sistema de información		25/02/2020		
Observaciones / anotaciones				



Acciones realizadas

- Se crea un usuario específico para la base de datos del Sistema de gestión de solicitudes de acceso a la información y de datos personales con los siguientes permisos:
 - SELECT
 - UPDATE

➤ DELETE



➤ INSERT

- Se eliminan usuarios con los mismos permisos en el Sistema de gestión de solicitudes de acceso a la información y de datos personales.
- Se revisaron los permisos otorgados a los usuarios en el sistema de desarrollo.

Sistema de gestión de solicitudes de acceso a la información y de datos personales			
Formato:	2	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:	<p>F) Realizar respaldo completo de la base de datos.</p> <p>G) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.</p> <p>H) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.</p> <p>I) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B.</p> <p>J) Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>		
Mejores prácticas, referencias:	<p>3. Definir niveles de acceso adecuados para cada perfil o tipo de usuario.</p> <p>4. Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.</p>		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	José Manuel Chicho Ortiz	25/02/2020	
Nombre y firma		Fecha término	
Programador, desarrollador o diseñador del sistema de información		25/02/2020	
Observaciones / anotaciones			



Acciones realizadas

- Se crea un usuario específico para la base de datos del Sistema de gestión de solicitudes de acceso a la información y de datos personales con los siguientes permisos:
 - SELECT
 - UPDATE
 - DELETE
 - INSERT
- Se deshabilitan usuarios que ya no se encuentran en uso o del personal que deja de laborar para a la Unidad de Transparencia.
- Se revisaron los permisos otorgados a los usuarios en el Sistema de gestión de solicitudes de acceso a la información y de datos personales.

Sistema de gestión de solicitudes de acceso a la información y de datos personales			
Formato:	3	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:	<p>A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación.</p> <p>B) El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo).</p> <p>C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx.</p> <p>D) Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.</p>		
Mejores prácticas, referencias:	<ol style="list-style-type: none"> 1. Los certificados SSL deben tener una vigencia de al menos un año. 2. En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (<i>wildcard</i>). 3. Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento. 		
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	Jose Manuel Chicño Ortiz	26/02/2020	
Nombre y firma		Fecha término	
Programador, desarrollador o diseñador del sistema de información		27/02/2020	
Observaciones / anotaciones			

Acciones realizadas

- Se instaló un certificado SSL/TLS trimestral de la certificadora Let's Encrypt; esto hasta contar con el presupuesto suficiente para la compra de un certificado SSL/TLS anual con alguna certificadora, tales como: Symantec, Comodo, GeoTrust, RapidSSI, Sectigo, Entrust, Thawte.
- Configuración de un cron para la renovación automática del certificado SSL/TLS.

Sistema de gestión de solicitudes de acceso a la información y de datos personales			
Formato:	4	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:	<p>A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:</p> <ol style="list-style-type: none"> Diario – incremental. Semanal – incremental. Mensual – total. <p>B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:</p> <ol style="list-style-type: none"> En línea: mismo equipo donde se ejecuta el sistema. Respaldo como servicio: otro equipo de almacenamiento. Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. <p>C) Incluir en el plan:</p> <ol style="list-style-type: none"> Responsables de cada tipo y medio de respaldo. Rotación de respaldos y medios. Áreas de resguardo. Métodos de cifrado. RTO: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. RPO: <i>Recovery Point Objective</i>: Punto objetivo de recuperación. <p>D) Concluir este documento, adjuntarlo a SGDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	28/02/2020	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
		03/03/2020	



Observaciones anotaciones	/	
------------------------------	---	--



Correo transparencia@unam.mx			
Formato:	4	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:	<p>A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:</p> <ul style="list-style-type: none"> a. Diario – incremental. b. Semanal – incremental. c. Mensual – total. <p>B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:</p> <ul style="list-style-type: none"> a. En línea: mismo equipo donde se ejecuta el sistema. b. Respaldo como servicio: otro equipo de almacenamiento. c. Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. <p>C) Incluir en el plan:</p> <ul style="list-style-type: none"> a. Responsables de cada tipo y medio de respaldo. b. Rotación de respaldos y medios. c. Áreas de resguardo. d. Métodos de cifrado. e. RTO: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. f. RPO: <i>Recovery Point Objective</i>: Punto objetivo de recuperación. <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			
Alfredo Alonso Peña			Fecha inicio

	Jose Manuel Chicho Ortiz	28/02/2020
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término 03/03/2020
Observaciones anotaciones	/	

Acciones realizadas



- Se desarrolló el documento para las políticas de respaldo y restauración de los sistemas de la Unidad de Transparencia, el cual contiene previstos los siguientes puntos:
 - Creación de respaldos del correo electrónico institucional de la Unidad de Transparencia.
 - Creación de respaldo de los servidores de la Unidad de Transparencia.
 - Creación de respaldo de los sistemas desarrollados por la Unidad de Transparencia.
 - Creación de respaldo de archivos y bases de datos de los sistemas de la Unidad de Transparencia.
- Los atributos que se consideran para cada una de las políticas de los respaldos son:
 - Inventarios de activos de información.
 - Control de acceso.
 - Nivel de criticidad
 - Periodicidad de los respaldos.
 - Caducidad de los respaldos.
 - Ubicación de los respaldos
 - Procedimientos de restauración.
 - Verificación de los respaldos.
 - Proceso para la destrucción
 - Cifrado de los respaldos

Sistema de gestión de solicitudes de acceso a la información y de datos personales			
Formato:	5	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:	<p>A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos.</p> <p>B) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo.</p> <p>C) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores.</p> <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1. Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/download/formato_responsiva_borrado_datos.pdf</p> <p>2. Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar <i>DOD-5220.22-M</i>.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	28/02/2020	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
		03/03/2020	
Observaciones anotaciones	/		

Equipo de cómputo de la Unidad de Transparencia			
Formato:	5	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:	<p>E) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos.</p> <p>F) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo.</p> <p>G) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores.</p> <p>H) Concluir este documento, adjuntarlo a SGDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>3. Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf</p> <p>4. Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar <i>DOD-5220.22-M</i>.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	28/02/2020	
Nombre y firma		Fecha término	
Programador, desarrollador o diseñador del sistema de información		03/03/2020	
Observaciones / anotaciones			


Acciones realizadas

- Se desarrolló el documento para las políticas de borrado seguro de archivos que contenga datos personales.
- El documento de borrado seguro contiene:
 - Proceso y herramientas para el borrado seguro de documentos.
 - Proceso y herramientas para el borrado seguro de respaldos.
 - Proceso y herramientas para el borrado seguro de información en base de datos.
 - Proceso y herramientas para el borrado seguro de equipo de cómputo en proceso de baja.

Servidores y equipos de red de la Unidad de Transparencia			
Formato:	6	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:	<p>A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.</p> <p>B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. <u>Por ejemplo</u>, en el caso del sistema operativo Linux:</p> <ol style="list-style-type: none"> a. Verificar la existencia del archivo <code>/etc/ntp.conf</code> b. Editar el archivo <code>ntp.conf</code> incluyendo en la primera línea: <ol style="list-style-type: none"> i. <code>server ntpdgtic.redunam.unam.mx ó</code> ii. <code>server 132.247.169.17</code> c. Reiniciar el demonio del cliente NTP con el comando <code>sudo service ntp reload</code>. <p>C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<ol style="list-style-type: none"> 1. Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. 2. No se deben usar otros servidores de NTP distintos al de UNAM. 		
Conocimientos requeridos:	Administración de sistema operativo.		
Ejecución			
			
Alfredo Alonso Peña		Jose Manuel Chicho Ortiz	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha inicio	
		04/03/2020	
		Fecha término	
		04/03/2020	
Observaciones / anotaciones			



Acciones realizadas



- Se crea el documento donde se establecen los equipos de cómputo que se encuentran configurados con el NTP de la UNAM



Servidores y equipo de cómputo de la Unidad de Transparencia			
Formato:	7	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de <i>malware</i> (<i>rootkits</i> , <i>backdoors</i> o códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:	<p>A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. <u>Por ejemplo</u>, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como <i>chkrootkit</i>, <i>rootkit hunter</i>, <i>bothunter</i>, <i>clamAV</i>, <i>avast</i>, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso.</p> <p>B) Disponer de comandos para la localización de amenazas. <u>Por ejemplo</u>, para el caso de Linux, se recomienda usar el comando <i>grep</i> para la detección de cadenas regulares de texto en las invocaciones al <i>shell</i>.</p> <p>C) Una vez instalada la solución, verificar periódicamente su actualización</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1. UNAM-CERT puede asesorar en la selección de las herramientas <i>anti malware</i> más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
 Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	Fecha inicio	
		04/03/2020	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
		05/03/2020	
Observaciones / anotaciones			

Acciones realizadas

- Se crea el documento donde se establecen las herramientas antimalware instaladas en cada uno de los servidores y equipos de cómputo de la Unidad de Transparencia. Dicho archivo contiene:
 - Tipo de sistema operativo.
 - Nombre de la herramienta.
 - Periodicidad de actualización.
 - Procedimientos en caso de detección de una amenaza.
 - Tipo de licenciamiento.
 - Bitácora
 - Responsable del equipo



Servidores, PC's, Laptops, equipos de red de la Unidad de Transparencia			
Formato:	8	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:	<p>A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. <i>Por ejemplo</i>, en el sistema operativo Linux ejecutar <i>apt-get update</i> para obtener la lista de actualizaciones, especialmente en el repositorio <i>security</i> de la respectiva distribución.</p> <p>B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad.</p> <p>C) Instalar las actualizaciones en el sistema operativo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1. Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	06/03/2020	
Nombre y firma		Fecha término	
Programador, desarrollador o diseñador del sistema de información		06/03/2020	
Observaciones / anotaciones			

Sistema de gestión de solicitudes de acceso a la información y de datos personales				
Formato:	9	Verificación anual	Acción concluida ()	
Medidas de seguridad técnicas:	Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.			
Proceso recomendado:	<p>A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema.</p> <p>B) Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. <i>Por ejemplo:</i> el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema.</p> <p>C) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	<ol style="list-style-type: none"> 1. Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (<i>Active Directory</i>), <i>LDAP</i> u <i>OpenAIM</i>. 2. Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números. 			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
 Alfredo Alonso Peña		 Jose Manuel Chicho Ortiz		Fecha inicio
				06/03/2020
Nombre y firma Programador, desarrollador o diseñador del sistema de información				Fecha término
				09/03/2020
Observaciones / anotaciones				

Sistema de gestión de solicitudes de acceso a la información pública y de datos personales			
Formato:	10	Verificación anual	Acción concluida ()
Medida de seguridad técnica:	Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:	<p>A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. <i>Por ejemplo:</i> en sistemas Linux desactivar la instalación de versiones <i>beta, test, debug, non-official</i>.</p> <p>B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones <i>TSR (Terminal and Stay Resident)</i>. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. <i>Por ejemplo:</i> En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo.</p> <p>C) Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. <i>Por ejemplo,</i> si el servidor Linux no proporcionará direcciones IP, el demonio o servicio <i>dchpd</i> no debe estar instalado.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1. En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña	Jose Manuel Chicho Ortiz	06/03/2020	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
		06/03/2020	
Observaciones / anotaciones			



Acciones realizadas PARA LOS FORMATOS 8, 9 y 10

- Se crea el documento donde se establecen las políticas de configuración y actualización para los servidores, PC's y equipos de red de la Unidad de Transparencia. Dicho archivo contiene:
 - Tipo de sistema operativo.
 - Versión del sistema operativo
 - Periodicidad de actualización.
 - Procedimientos en caso una actualización errónea.
 - Bitácora
 - Responsable del equipo.
 - Usuarios
 - Permisos por usuario.
 - Método de autenticación.
 - Programas instalados.
 - Tipo de licenciamiento de cada uno de los programas instalados.
- Realiza la verificación y acciones requeridas en los equipos de la Unidad de Transparencia conforme a lo establecido en las políticas de configuración y actualización para los servidores, PC's y equipos de red de la Unidad de Transparencia
- Se realiza la verificación y listado de usuarios registrados en el Sistema de gestión de solicitudes de acceso a la información pública y de datos personales. El listado contiene:
 - Nombre de usuario
 - Fecha de verificación
 - Perfil de usuario
 - Permisos otorgados.

Sistema de gestión de solicitudes de acceso a la información pública y de datos personales			
Formato:	13	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:	<p>A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. <i>Por ejemplo: SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy).</i></p> <p>B) Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. <i>Por ejemplo,</i> en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando <i>apt-get install openssh-server.</i></p> <p>C) Activar los protocolos de comunicación encriptada en el servidor. <i>Por ejemplo:</i> en Linux con el comando <i>sudo systemctl enable ssh.</i></p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<ol style="list-style-type: none"> 1. Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2. El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red. 		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			
		Fecha inicio	
Alfredo Alonso Peña		09/03/2020	
		Fecha término	
Jose Manuel Chicho Ortiz		11/03/2020	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			
Observaciones / anotaciones			

Acciones realizadas

- Se revisaron los protocolos para compartir archivos al interior de la Unidad de Transparencia y se deshabilitaron los métodos no seguros, tales como:
 - SMBv1
 - SSH protocol 1
 - NetBIOS sobre TCP/IP

Sistema de gestión de solicitudes de acceso a la información pública y de datos personales			
Formato:	14	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.		
Aplicable en:	Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:	<p>A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <i>Por ejemplo:</i> máquina virtual directorio temporal en el servidor.</p> <p>B) Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando.</p> <p>C) Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa.</p> <p>D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. <i>Por ejemplo:</i> en Linux se dispone de <i>shred, wipe, secure-delete, srm, sfill, sswap, sdmem</i>, que se pueden instalar desde el administrador de aplicaciones.</p> <p>E) Llenar y firmar este formato.</p>		
Mejores prácticas, referencias:	1. Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			
			
Alfredo Alonso Peña		Jose Manuel Chicho Ortiz	
Nombre y firma		Fecha inicio	
Programador, desarrollador o diseñador del sistema de información		11/03/2020	
Nombre y firma		Fecha término	
Programador, desarrollador o diseñador del sistema de información		13/03/2020	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	15	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas	Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:	<p>A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas.</p> <p>B) Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <i>Por ejemplo:</i> La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes.</p> <p>C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa.</p> <p>D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <i>Por ejemplo: Webservices, transferencia SFTP.</i></p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
		Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1	
Formato:	16	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	<p>A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles.</p> <p>B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).</p> <p>C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo</p> <p>D) Activar bitácoras de acceso (<i>log</i>) hacia el equipo central de desarrollo.</p> <p>E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales.</p> <p>F) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución				
			Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			Fecha término	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	17	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.			
Proceso recomendado:	<p>A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia).</p> <p>B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo.</p> <p>C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			Fecha inicio	
Nombre y firma Administrador del sistema de información o servidor			Fecha término	
Observaciones / anotaciones				

(Nombre del sistema A1)		Identificador único A1		
Formato:	18	Verificación anual	Acción concluida	()
Medidas de seguridad técnica:	Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.			
Proceso recomendado:	<p>A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos.</p> <p>B) Designar responsables de respaldos y responsables de verificación de respaldos.</p> <p>C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución			Fecha inicio	
Nombre y firma Administrador del sistema de información o servidor			Fecha término	
Observaciones / anotaciones				

(Nombre del sistema A1)		Identificador único A1		
Formato:	19	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.			
Proceso recomendado:	<p>A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. <i>Por ejemplo:</i> En caso de consultar vía un <i>Webservice</i> a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema.</p> <p>B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. <i>Por ejemplo:</i> Si la cuenta de acceso a un <i>Webservice</i> – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.</p> <p>C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. <i>Por ejemplo:</i> si la identificación para acceder a un respaldo remoto es del tipo xxx@google.com, deberá cambiarse por una cuenta del tipo xxxx@unam.mx</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución				
			Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			Fecha término	
Observaciones / anotaciones				

(Nombre del sistema A1)		Identificador único A1	
Formato:	20	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:	<p>A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. <u>Por ejemplo:</u> En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (<i>logs</i>), de forma física las bitácoras de acceso al área donde está el equipo de cómputo.</p> <p>B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. <u>Por ejemplo:</u> diario, semanal, mensual.</p> <p>C) Establecer en el documento el procedimiento de resguardo de las bitácoras. <u>Por ejemplo:</u> respaldo y protección de <i>logs</i> en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	21	Verificación anual	Acción concluida ()
Norma Complementaria Técnica	Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:	<p>A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones.</p> <p>B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red.</p> <p>C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable.</p> <p>D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento.</p> <p>E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:	Administración de redes de datos.		
Ejecución			
		Fecha inicio	
		Fecha término	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	22	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:	<p>A) Revisar los puertos de comunicación (<i>TCP</i> y <i>UDP</i>) que requiera el sistema de información para su operación. <u>Por ejemplo</u>: para servicios <i>Web</i> los puertos 80 y 8080 son los convencionales.</p> <p>B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. <u>Por ejemplo</u>, en Linux puede tratarse de un <i>firewall</i> a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo.</p> <p>C) Dejar activos solamente los puertos necesarios para la operación del sistema.</p> <p>D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. <u>Por ejemplo</u>: Permitir el acceso al puerto de <i>SSH</i> solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
		Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	23	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:	<p>A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión.</p> <p>B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador.</p> <p>C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.		
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.		
Ejecución			
		Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	24	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:	<p>A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx .</p> <p>B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A.</p> <p>C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.		
Ejecución			
		Fecha inicio	
		Fecha término	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	25	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	de	Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.	
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.		
Proceso recomendado:	<p>A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información.</p> <p>B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática.</p> <p>C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico.</p> <p>D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El mantenimiento preventivo debe contar con medidas de verificación.		
Conocimientos requeridos:	Administración de infraestructura.		
Ejecución			
		Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información		Fecha término	
Observaciones / anotaciones			

(Nombre del sistema A1)		Identificador único A1	
Formato:	26	Verificación anual	Acción concluida ()
Medidas de seguridad técnicas:	Artículo 18. III. b) Definir el programa de mantenimiento preventivo.		
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:	<p>A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento.</p> <p>B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.</p> <p>C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.		
Conocimientos requeridos:	Administración de infraestructura.		
Ejecución			
		Fecha inicio	
		Fecha término	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			
Observaciones / anotaciones			

(Nombre del sistema A1)			Identificador único A1	
Formato:	27	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad.</p> <p>B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo.</p> <p>C) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
			Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			Fecha término	
Observaciones / anotaciones				

(Nombre del sistema A1)			Identificador único A1	
Formato:	28	Verificación anual	Acción concluida	()
Medidas de seguridad técnicas:	Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.			
Aplicable en:	Servicios en la nube pública.			
Tiempo estimado:	Hito.			
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.			
Proceso recomendado:	A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.			
Mejores prácticas, referencias:	1.- La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.			
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.			
Ejecución				
			Fecha inicio	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			Fecha término	
Observaciones / anotaciones				



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Políticas



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Marzo 2020

Políticas de respaldo

Versión 0.4

Marzo 2020

Contenido

Objetivo	41
Alcance	41
Responsabilidades	41
Respaldos.....	41
Periodicidad.....	41
Cifrado.....	42
Verificación.....	42
Ubicación	42
Control de Acceso	42
Consolidación	43
Supresión.....	43
Proceso de borrado	43
Restauración	43
Recuperación	43
Control de cambios	44



¡Universidad Abierta y Transparente!

Unidad de Transparencia

Políticas de actualización

Versión 0.5

Marzo 2020

Contenido

Objetivo	47
Alcance	47
Responsabilidades	47
Actualizaciones.....	47
Servidores.....	47
Equipo administrativo	48
Periodicidad.....	48
Software	49
Control de cambios	49

Objetivo

Definir las políticas y procedimientos para la actualización de sistemas operativos, software y software antimalware de los principales sistemas y equipos de cómputo (servidores, equipos de red, PC's) de la Unidad de Transparencia.

Alcance

Las presentes políticas definen la periodicidad para la actualización de sistemas operativos, software y software antimalware conforme a los niveles de criticidad de los equipos de cómputo de la Unidad de Transparencia.

Responsabilidades

Es responsabilidad de la Coordinación de Sistemas de la Unidad de Transparencia configurar inicialmente los equipos de cómputo dedicado a los usuarios de la Unidad de Transparencia con las siguientes características:

- Establecer los periodos de actividad del equipo para la instalación de actualizaciones de software
- Instalar software antimalware
- Instalar software para el desempeño de las funciones diarias del usuario que utilizará el equipo.

La actualización de los servidores y equipos de red estará bajo la responsabilidad de la Coordinación de Sistemas.

La responsabilidad de los trabajadores que cuenten con un equipo proporcionado por la Unidad de Transparencia, son:

- Contactar a la Coordinación de Sistemas cuando el equipo indique la necesidad de actualizar.
- Analizar los dispositivos extraíbles que conecten a sus máquinas.
- Solamente conectar dispositivos extraíbles de confianza.
- Informar a la Coordinación de Sistemas cuando se desee instalar algún software.

Actualizaciones

Todo sistema operativo y software es susceptible a tener fallos y mejoras. Por ello, es indispensable que se instalen de forma periódica las actualizaciones que proporciona el fabricante.

Se debe de tener en cuenta que entre más tiempo pase entre actualizaciones, se está expuesto a que algún tipo de virus o malware pueda explotar alguna vulnerabilidad.

Servidores

Las actualizaciones de los servidores de producción se darán conforme a los siguientes puntos:

- Se prohíbe el uso de actualizaciones en versiones beta o similares.
- Las actualizaciones se deberán de probar con antelación en un ambiente similar.

- En caso de requerir reiniciar el equipo, dicha actualización se deberá aplicar en un horario que no afecte con las actividades del personal.
- En caso de necesitar instalar una actualización urgente, se deberá realizar una copia de seguridad completa del equipo antes de realizar la instalación.

Equipo administrativo

Los usuarios que cuenten con sistemas operativos Windows en sus equipos, deberán de atender lo siguiente:

- Verificar que las actualizaciones automáticas se encuentren activadas. Esto se puede consultar de la siguiente forma:
 - Presionando el botón de inicio
 - Escribe “Windows Update” o “Buscar actualizaciones”
 - Hacer clic en el botón <<Buscar actualizaciones>> y en caso de tener una actualización

Usuarios que cuenten con sistemas operativos Mac, deberán de revisar las actualizaciones en:

- Para realizar una actualización en equipos Apple se debe de ingresar al apartado <<Actualización de Software>> o <<Software Update>>, el cual se encuentra en el Menú Apple de la barra principal.

Usuarios que cuenten con sistemas operativos Linux, deberán de realizar las siguientes acciones:

- Abrir una terminal y ejecutar las siguientes instrucciones:
 - Para derivaciones de Debian
 - apt update o apt-get update
 - apt upgrade o apt-get dist-upgrade
 - Para derivaciones de Red Hat
 - dnf update
 - yum update
 - Para derivaciones de Arch
 - pacman -Syy
 - aptitude update
 - pacman -Sulinux zypper
 - Para derivaciones de Suse
 - Zypper update

En caso de que se detecte que existen fallos en las actualizaciones para algún sistema operativo, se deberá avisar a cada uno de los responsables de las áreas de la Unidad de Transparencia para que no se ejecuten actualizaciones, hasta nuevo aviso por parte de la Coordinación de Sistemas.

Periodicidad

La periodicidad nos indica la frecuencia con que las actualizaciones serán aplicadas. Para el equipo administrativo se deberán de realizar conforme a la siguiente periodicidad:

- Sistema operativo Windows

- Verificar al menos una vez al mes si existe un nuevo parche de seguridad mediante la herramienta de Windows Update. En caso de existir un nuevo parche de seguridad, este se deberá dejar el equipo actualizando durante la noche.
- Verificar al menos una vez cada semestre si existe una actualización de primer nivel. En caso de existir, se deberá de avisar a la Coordinación de Sistemas para que sea valorada la instalación de dicha actualización
- Sistema operativo MacOS, Linux, FreeBSD
 - Verificar mínimo una vez al mes.

Software

Para la instalación de nuevo software en el equipo de cómputo, el responsable del equipo deberá de contar con la licencia de activación en caso de requerirse y dar aviso a la Coordinación de Sistemas para que realice la instalación de dicho software.

Para las actualizaciones de software en equipo administrativo, la Coordinación de Sistemas dejara activa la actualización automática. En caso de que la actualización requiera reiniciar el equipo, el encargado del equipo decidirá el horario en el cual desea que se realice dicho reinicio.

En instalación y actualización de programas en servidores, la Coordinación de Sistemas primero instalará el nuevo software o actualización en un servidor de preproducción o QA, antes de pasar a producción, para evitar problemas de compatibilidad y disponibilidad de los servicios.

Control de cambios

Motivo del cambio	Autor del cambio	Descripción	Fecha	Versión
Creación	Alejandro Camacho Torres	Creación de las políticas de actualización.	06/03/2020	0.1
Actualización	Jose Manuel Chicho Ortiz	Se actualizan las responsabilidades.	10/03/2020	0.2
Actualización	Alejandro Camacho Torres	Se actualiza el documento.	10/03/2020	0.3
Actualización	Jose Manuel Chicho Ortiz	Se actualiza el apartado de software.	10/03/2020	0.4
Revisión	Diego Benítez Colín	Revisión de documento	11/03/2020	0.5



¡Universidad Abierta y Transparente!

Unidad de Transparencia

Políticas de borrado seguro

Versión 0.4

Marzo 2020

Contenido

Objetivo	52
Alcance	52
Responsabilidades	52
Borrado seguro.....	52
Aplicabilidad.....	52
Motivos.....	53
Herramientas	53
Bases de datos.....	54
Control de cambios	54

Objetivo

Definir las políticas y procedimientos para el borrado de archivos de los principales sistemas y equipos de cómputo (servidores, equipos de red, PC's) de la Unidad de Transparencia.

Alcance

Las presentes políticas definen el procedimiento para el borrado de archivos conforme a los niveles de criticidad de la información que se desee eliminar.

Responsabilidades

Es responsabilidad de cada uno de los jefes de las áreas funcionales de la Unidad de Transparencia dar aviso a la Coordinación de Sistemas sobre la transferencia de equipo entre personal, y es responsabilidad de la Unidad Administrativa de la Unidad de Transparencia avisar a la Coordinación de Sistemas con antelación sobre los equipos de cómputo que se darán de baja.

La Coordinación de Sistemas tiene como responsabilidad borrar la información de forma segura de los equipos que se van a dar de baja y de los equipos que van a ser traspasados; dicha información puede ser: fotos, documentos, música, videos o cualquier otro tipo de archivo de los equipos de cómputo de la Unidad de Transparencia.

Es responsabilidad del encargado del equipo de cómputo realizar el borrado seguro conforme a las presentes políticas de archivos con información sensible, reservada y/o que contenga datos personales.

Borrado seguro

El borrado seguro consiste en eliminar la información de cierta forma para que esta no pueda ser recuperada. Existen tres tipos de borrado seguro:

- Física: consiste en la destrucción total del dispositivo para que no sea recuperado por ningún medio la información que contuviese este. Este método es válido para cualquier tipo de dispositivo como: USB, SSD, HDD, CD, DVD, Blue-ray Disc, etc.
- Desmagnetización: consiste en exponer el dispositivo a un campo magnético. Este método de borrado seguro solo se puede utilizar en HDD, disquetes, cintas magnéticas, etc.
- Sobreescritura: consiste en la utilización de un software, el cual va a realizar una escritura de datos con ciertos patrones sobre el documento que se desea borrar. Este procedimiento no es aplicable para dispositivos que no son regrabables como CD, DVD, Blue-ray Disc, etc.

Aplicabilidad

Los tres métodos de borrado seguro no son aplicables a los diferentes dispositivos con los que se cuentan hoy en día. A continuación, se presenta la tabla de métodos de borrado seguro que se pueden aplicar a los diferentes dispositivos.

Dispositivo	Tipo de dispositivo	Destrucción física	Desmagnetización	Sobreescritura
Discos duros o HDD	Magnético	Aplica	Aplica	Aplica
Discos flexibles (floppies o disquetes)	Magnético	Aplica	Aplica	Aplica
Cintas	Magnético	Aplica	Aplica	Aplica
CD, DVD, Blue-ray disc	Óptico	Aplica	No aplica	No aplica
Pen driver o USB	Electrónico	Aplica	No aplica	Aplica**
Discos de estado sólido o SSD	Electrónico	Aplica	No aplica	Aplica**

**Para los dispositivos electrónicos se deben de utilizar herramientas que cuenten con estándares que aseguren el borrado seguro de la información.

Motivos

El borrado seguro se aplicará en los siguientes casos:

- Baja de equipo
- Archivos que sean trasladados al Sistema de Archivos.
- Equipo transferido a personal interno de la Unidad de Transparencia.
- Equipo transferido a una Área Universitaria diferente la Unidad de Transparencia.
- Solicitante exigiendo la cancelación de sus datos personales.

Herramientas

Las herramientas para el borrado seguro de archivos deben de contar como mínimo el método DoD5220.22-M para dispositivos magnéticos y el método NIST 800-88 para dispositivos como USB, SSD, etc.

Algunas de las herramientas que se pueden utilizar para realizar el borrado seguro, son:

- Windows
 - SDelete
 - Wipe My Disks de HDDGURU

- Eraser
- MacOS
 - Permanent eraser
 - Disk Utility
- Linux
 - srm
 - wipe
- Multiplataforma
 - dban
 - Blancco Driver Eraser

Bases de datos

El borrado seguro de la información contenida en cualquier tipo de motor de base de datos (MySQL, SQL, Oracle, etc) se deberá realizar mediante un método de sobrescritura de la información contenida en el registro o registros, posteriormente se procederá a realizar el borrado del registro: en caso de que el registro afecte la integridad de la información contenida en la base de datos solamente se realizará la anonimización o seudonimización de los datos.

Control de cambios

Motivo del cambio	Autor del cambio	Descripción	Fecha	Versión
Creación	Alejandro Camacho Torres	Creación de las políticas de respaldo	06/03/2020	0.1
Actualización	Jose Manuel Chicho Ortiz	Revisión del documento	10/03/2020	0.2
Actualización	Jose Manuel Chicho Ortiz	Cambio en la redacción de una nota y se ajusta el texto	11/03/2020	0.3
Revisión	Diego Benítez Colín	Revisión de documento	11/03/2020	0.4



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Políticas de contraseñas

Versión 0.3

Abril 2021

Contenido

Contenido	56
Objetivo	57
Alcance	57
Creación	57
Gestión	57
Buenas prácticas	58
Fuentes	58
Control de cambios	59

Objetivo

Definir las políticas y procedimientos para la creación, gestión y uso de contraseñas para sistemas y equipos de la Unidad de Transparencia.

Alcance

Las presentes políticas la forma correcta para la creación de contraseñas robustas, buenas prácticas y la sugerencia para el almacenaje de estas.

Creación

Las contraseñas son las llaves con las cuales se puede acceder a los diferentes sistemas que contienen información personal o asuntos laborales, también nos permite acceder a herramientas de trabajo tales como, correo electrónico, sitios institucionales, etc. Por ello es importante que una contraseña sea robusta y contenga como mínimo los siguientes puntos:

1. Incluir letras mayúsculas y minúsculas (a-z A-Z),
2. Incluir números (0-9)
3. Incluir caracteres especiales, tales como: °! "#\$%& /()=? |0¿
4. Debe de tener una longitud mínima de 10 caracteres

Además, puede tomar en cuenta alguno de los siguientes puntos:

1. Elegir una frase que le resulte fácil de recordar o
2. Combinar dos o más palabras
3. Incluir mayúsculas y minúsculas en un orden específico para usted,
4. Escoge frases o palabras sin vocales
5. Cambia las vocales de las palabras por su representación numérica
6. Escoge algún número que te sea fácil de recordar y entre cada dígito una sucesión de letras
7. Usar una combinación de mayúsculas y minúsculas en las palabras

Para saber si la contraseña creada es segura, puede utilizar alguna de estas herramientas.

- <https://lowe.github.io/tryxcvbn/>
- <https://www.uic.edu/apps/strong-password/>
- <https://password.kaspersky.com/es/>
- <https://www.security.org/how-secure-is-my-password/>

Gestión

De ser posible, utilice alguna herramienta de almacenamiento y gestión de contraseñas:

- KeePass (Gratuito - <https://keepass.info>)
- LastPass (Gratuito / Paga <https://www.lastpass.com/es>)
- Enpass (Gratuito / Paga <https://www.enpass.io/>)
- Keeper (Paga https://www.keepersecurity.com/es_ES/)
- 1Password (Paga <https://1password.com/es/>)
- RoboForm (Gratuito / Paga <https://www.roboform.com/es>)

Las herramientas antes mencionadas cuentan con diferentes funcionalidades extras, la elección de dicha herramienta dependerá de las necesidades de cada uno.

Buenas prácticas

Evite usar alguna de las siguientes malas prácticas en el manejo de contraseñas:

1. Apuntar las contraseñas en lugares no apropiados, tales como: libretas, post-its, pizarrones, papelitos o lugares poco seguros.
2. Enviar contraseñas a través de un medio inseguro
3. Usar una contraseña para todos los sistemas (correo, finanzas computadora, teléfono, etc)
4. Utilizar datos personales en la creación de contraseñas (nombre, fecha de nacimiento, nombre de mascotas, etc)
5. Utilizar contraseñas por defecto.
6. Difundir la contraseña con personal no autorizado.
7. Usar patrones predecibles o usar contraseñas poco seguras, tales como:
 - a. Qwerty
 - b. 1234567890
 - c. 123456
 - d. Password
 - e. password1
 - f. iloveyou

Ya que se sabe que practicas se deben de evitar, ahora veremos las practicas que se deben de realizar para mantener las diferentes cuentas seguras.

1. Cambiar las contraseñas de forma periódica (cada 6 o 12 meses en sistemas no críticos y cada 2 o 3 meses en sistemas críticos)
2. Uso de contraseñas únicas para cada sistema al que se tenga acceso
3. Uso de gestores de contraseñas
4. Uso de autenticación de doble factor (A2F) en los sistemas que lo permitan, como el correo institucional y para manejo de licencias de adobe.
5. Acceder a los sitios mediante equipos seguros o confiables.

Fuentes

<https://www.uic.edu/apps/strong-password/>

<https://www.pandasecurity.com/es/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/>

<https://lowe.github.io/tryzxcvbn/>

<https://dropbox.tech/security/zxcvbn-realistic-password-strength-estimation>

<https://www.welivesecurity.com/la-es/infographics/infografia-como-elegir-contrasena-segura/>

<https://lifehacker.com/use-this-infographic-to-pick-a-good-strong-password-5876541>

Control de cambios

Motivo del cambio	Autor del cambio	Descripción	Fecha	Versión
Creación	Alejandro Camacho Torres	Creación de las políticas de contraseñas	20/03/2020	0.1
Actualización	Jose Manuel Chicho Ortiz	Se modifican los temas	20/04/2021	0.2
Actualización	Alfredo Alonso Peña	Modificación en la redacción	20/04/2021	0.3



¡Universidad Abierta y Transparente!
Unidad de Transparencia

Bitácoras



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Formato de Bitácora de vulneraciones a los Sistemas de Información

Nombre Sistema de Tratamiento		
Fecha del incidente		
Nombre de quien reporta el incidente		
Cargo		
Área universitaria		
Responsable del área		
Causa de la vulneración		
Componente(s) del sistema vulnerado(s)		
Cantidad de titulares de datos personales afectados		
Soporte de la información vulnerada	<input type="checkbox"/> Físico <input type="checkbox"/> Electrónico <input type="checkbox"/> Mixto	
Seleccione el tipo de vulneración	<input type="checkbox"/> Pérdida o extravío <input type="checkbox"/> Destrucción no autorizada	
	<input checked="" type="checkbox"/> Robo <input type="checkbox"/> Copia no autorizada	
	<input type="checkbox"/> Uso, acceso o tratamiento no autorizado	
	<input type="checkbox"/> Daño, alteración o modificación no autorizada	
Tipo de titular afectado	<input type="checkbox"/> Extranjeros <input type="checkbox"/> Trabajadores <input type="checkbox"/> Menores de edad <input type="checkbox"/> Alumnos <input type="checkbox"/> Estudiantes de movilidad nacional <input type="checkbox"/> Profesores de asignatura <input type="checkbox"/> Profesores de tiempo completo <input type="checkbox"/> Investigadores <input type="checkbox"/> Técnicos Académicos <input type="checkbox"/> Proveedores o contratistas <input type="checkbox"/> Terceros (visitantes, etc.)	
Tipo de datos personales Comprometidos	<input type="checkbox"/> Identificativos <input type="checkbox"/> Laborales	
	<input type="checkbox"/> Datos Académicos	
	<input type="checkbox"/> Procedimientos administrativos / Judiciales / Procedimientos seguidos en forma de juicio	
	<input type="checkbox"/> Patrimonial <input type="checkbox"/> Salud <input type="checkbox"/> Afiliaciones políticas o ideológicas	
	<input type="checkbox"/> Origen étnico <input type="checkbox"/> Características Personales	
	<input type="checkbox"/> Vida Sexual <input type="checkbox"/> Discapacidades	
Las acciones correctivas implementadas de forma inmediata y definitiva.	<hr/> <hr/>	
Nombre y firma de quién reporta	Nombre y firma del administrador del sistema	Nombre y firma del titular del área