Universidad Nacional Autónoma de México

Secretaría de Desarrollo Institucional

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Lineamientos y recomendaciones para el resguardo de información electrónica

Junio de 2023

Contenido

Objetivo

Definir los lineamientos, elementos de referencia y buenas prácticas para la protección y resguardo de la información electrónica que se gestiona a través de los sistemas de la Universidad Nacional Autónoma de México bajo un marco de disponibilidad e integridad de los datos.

Alcance

Este documento está dirigido al personal universitario responsable de los sistemas o fuentes de información electrónica de la universidad. Su finalidad es orientar los procedimientos para resguardar y proteger la información a través de la definición de criterios y buenas prácticas que apoyen la toma de decisiones y acciones al respecto.

Términos y definiciones

Criticidad de la información. Elemento de clasificación que permite definir cómo ha de ser tratada y protegida la información, de acuerdo con su importancia e impacto en una organización.

Copia de seguridad (respaldo). Reproducción electrónica de los programas, datos e información de interés en un medio de almacenamiento. Un respaldo puede implicar la copia de todos los programas, datos y archivos de configuración en un dispositivo específico, como puede ser cinta, disco magnético, CD, DVD, disco duro externo, entre otros (Domínguez, 2005:42).

Firma digital. Consiste en una técnica matemática que nos permite verificar la autenticidad. (S. Gillis, s.f.)

Inmutabilidad. Característica de los datos o archivos digitales. Indica que no se puede o no se deben eliminar o modificar.

Disponibilidad. Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada (Glosario ISO 27001:2013).

Nivel de servicio. Definición que establece los niveles de calidad con los que operará y estará disponible un sistema o servicio digital conforme a los objetivos de negocio.

Punto objetivo de recuperación (Recovery Point Objective, RPO). Consiste en definir el período de tiempo en que se tolera la pérdida de datos sin afectación a los objetivos de negocio del servicio, es decir, el intervalo de tiempo entre dos copias de seguridad. Por ejemplo: una semana, un día, seis horas.

Replicación. Proceso de copiado y mantenimiento de datos, archivos u objetos digitales en un medio de almacenamiento alterno al que contiene estos datos, archivos u objetos originales con un período de tiempo definido para la sincronía (copia) de éstos.

Respaldo completo. Copia de seguridad que resguarda la totalidad de la información de interés.

Respaldo diferencial. Copia de seguridad que resguarda toda la información modificada o creada en una fecha posterior al último respaldo completo realizado.

Respaldo incremental. Copia de seguridad que resguarda toda la información modificada o creada en una fecha posterior al último respaldo realizado, sin importar que éste haya sido completo o diferencial.

Snapshot (almacenamiento). Copia completa del estado de un sistema, volumen o de datos en un punto en el tiempo.

Tiempo objetivo de recuperación (Recovery Time Objective, RTO). Tiempo establecido que puede transcurrir antes de la recuperación completa de los datos a partir de una copia de seguridad o respaldo. Por ejemplo: dos horas.

Marco legal

- Acuerdo por el que se establecen los lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México.
- Lineamientos generales para la organización, administración y conservación de los archivos de la Universidad Nacional Autónoma de México.
- Reglamento de transparencia y acceso a la información pública de la Universidad Nacional Autónoma de México.
- Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
- Anexo de las Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.
- Catálogo de disposición documental.
- Lineamientos y recomendaciones para la Administración de Bases de Datos.
- Lineamientos generales y políticas sobre almacenamiento e información compartida entre los sistemas existentes.
- Reglamento de responsabilidades administrativas de las y los funcionarios y empleados de la Universidad Nacional Autónoma de México.

1. Sobre la información de la universidad

En concordancia con los “Lineamientos generales y políticas sobre almacenamiento e información compartida entre los sistemas existentes”, las áreas universitarias deben observar lo siguiente:

- Dado el valor de la información como activo universitario y propiedad de la institución, deben establecerse formalmente y cumplirse procedimientos de operación claros en todas las áreas sustantivas de la actividad de la UNAM, para contar con respaldos periódicos de los datos que sean adecuados y cumplir con los principios de resguardo, recuperación, continuidad y acceso, determinados por la naturaleza, criticidad y variabilidad de la

información. En caso de que la información sea de terceros, se deberá contar con los permisos necesarios por los respectivos titulares de la información.

- La forma de organización, conservación y control de los medios de almacenamiento empleados será establecida dentro de cada entidad o dependencia considerando la clasificación de la información, la trazabilidad y lo establecido en las "Normas complementarias sobre medidas de seguridad, técnicas administrativas y físicas para la protección de datos personales en posesión de la Universidad".
- Toda información almacenada digitalmente, transmitida por correo o por medios electrónicos, debe protegerse de acuerdo con la normatividad, sin importar la forma que tome o los medios por los que se comparta o almacene.
- La información almacenada en las áreas universitarias necesita conservarse durante los plazos estipulados en la normatividad vigente antes de poder ser eliminada, como pueden ser bajo la consideración del ciclo vital de los documentos señalado en los "Lineamientos generales para la organización, administración y conservación de los archivos de la UNAM" y en el "Catálogo de disposición documental". Dado el ciclo de vida de la información, tras extinguirse sus plazos de conservación establecidos, deben relacionarse los documentos para verificar que ya prescribieron sus valores primarios (administrativos, legales, fiscales o contables) y que no tienen valores secundarios previo a su eliminación.

De acuerdo con los "Lineamientos y recomendaciones para la administración de bases de datos", las áreas universitarias necesitan:

- Establecer sus planes de respaldo y recuperación considerando la importancia de la información, el tipo de respaldo y la frecuencia con que se realizará, seleccionando el medio de almacenamiento, haciendo la verificación de la restauración fiable de los respaldos y documentándolos. Para ello establecerán un punto objetivo de recuperación (RPO) y tiempo objetivo de recuperación (RTO) de la información en cada base de datos que tengan bajo su responsabilidad.
- Efectuar un registro que sirva de control de los respaldos realizados a las bases de datos que tenga como datos mínimos: el nombre de la base de datos, tipo de respaldo realizado, descripción de la base de datos, sistemas o plataformas relacionadas con la base de datos, medio de almacenamiento y fecha.

Para clasificar la información (pública, confidencial, reservada, etc.), las áreas universitarias deben observar lo establecido en la normatividad vigente, así como el tipo de información a la que da tratamiento su entidad o dependencia.

De igual forma deberán establecer procedimientos para permitir el acceso y recuperación de los datos (tanto en el medio de almacenamiento como la lectura de los formatos utilizados) a través de todo el período de retención de la información, de acuerdo con la normatividad aplicable.

Las áreas universitarias también deben establecer procedimientos para eliminar la información y/o los medios de almacenamiento una vez concluido el período de retención, permitiendo su trazabilidad al interior del área y ante una auditoría.

2. Recomendaciones para la protección y resguardo de la información

2.1. Plan de continuidad

El objetivo de un plan de continuidad es asegurar el mínimo impacto al área universitaria en caso de una interrupción en los servicios de TI que soportan los sistemas de información.

Para ello es necesario la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de estos recursos, el procesamiento alternativo de la información y los *principios de respaldo y recuperación*, considerando los requerimientos de resistencia a fallas, procesamiento alternativo, y capacidad de recuperación.

Se aconseja al responsable TIC establecer, documentar, implementar y mantener los procesos, procedimientos y controles que conforman el plan de continuidad para garantizar el nivel requerido de continuidad de las operaciones que requiere el área universitaria. Como parte del plan de continuidad se elabora un plan de recuperación de desastres (*Disaster Recovery Plan, DRP*) que ayude a reestablecer los servicios importantes para el área universitaria (ver anexo 1).

Se recomienda definir y ejecutar procedimientos de control de cambios para asegurar que el plan de continuidad de TI se mantenga actualizado y refleje de manera continua los requerimientos actuales del área universitaria.

Los responsables TIC deberán asegurarse que se hagan las actualizaciones apropiadas en los planes de continuidad después de cambios en las plataformas operativas que soportan los sistemas de información.

Se recomienda que el área universitaria verifiqué los procesos, procedimientos y controles de continuidad establecidos e implementados a intervalos regulares a fin de asegurar que son válidos y eficaces durante situaciones adversas.

Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

Asegurarse de que todas las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.

Para medir la eficiencia del plan de continuidad se puede hacer uso de algunos indicadores, como son:

- Número de horas perdidas por usuario cada mes, debido a interrupciones no planeadas.

- Número de procesos críticos de negocio que dependen de TI y no están cubiertos por un plan de continuidad.
- Porcentaje de niveles de servicio sobre disponibilidad que se cumplen.
- Frecuencia en la interrupción de servicios de sistemas críticos.
- Frecuencia de revisión del plan de continuidad de TI.

2.2. Respaldos y recuperación de la información

El objetivo de generar un respaldo es permitir la recuperación de la información en caso que haya sido eliminada, dañada o alterada de forma intencional o accidental. Para proteger la información se recomienda establecer un plan o política de respaldos y recuperación que incluya, como mínimo, lo siguiente:

a) Definición de qué información se va a respaldar, niveles, frecuencia y número de copias de seguridad (respaldos). Establecer estos parámetros de acuerdo con los objetivos de recuperación del área universitaria considerando la criticidad e importancia de la información y el cumplimiento de la normatividad aplicable.

   i) Frecuencia. Consiste en la cantidad de veces que se realizan los respaldos planeados en un periodo. Por ejemplo: un respaldo diario, dos respaldos por semana, un snapshot diario (generalmente utilizado para máquinas virtuales o bases de datos).

   ii) Retención. Periodo para mantener almacenados los datos en los respaldos antes de eliminarlos, de acuerdo con la normatividad y utilidad. Por ejemplo: se conservan los respaldos del último mes o los últimos diez días por seis meses.

   iii) Tipo de respaldo. Se refiere a la estrategia de resguardo que utiliza la organización para asegurar su información. Por ejemplo: completo, incremental o diferencial (como control de versiones de archivos, diario o envío y archivado de registros, replicación, copias puntuales) por mencionar los tipos más utilizados.

   Es recomendable identificar qué tanto cambia la información en un período o la cantidad de información que se puede perder con respecto a la fuente original, para realizar un respaldo completo de la misma y definir respaldos parciales (incrementales) o diferenciales en el tiempo que cambie. Así mismo, se debe considerar dentro de la estrategia de respaldos el nivel de servicio comprometido para cada servicio específico.

   iv) Número de respaldos. Se sugiere tener más de una copia de los datos, debido a que los medios de almacenamiento son susceptibles a daños ambientales y físicos. Por ello se debe evitar su exposición a temperaturas altas, polvo, luz solar y humedad.

   Se aconseja seguir la regla 3-2-1. Conserva tres copias de tus datos en al menos dos medios diferentes (por ejemplo, un disco duro interno y otro externo, o disco duro y cinta, etc.) y aloja la tercera copia en un lugar físico distinto que esté totalmente fuera del lugar donde reside el original.

   v) Tipo de protección. En el caso de cualquier respaldo, se sugiere comprimirlo (zip, rar, tar) y cifrarlo convencionalmente con algoritmos acordes a su criticidad.

b) Tipos de medios que se utilizarán para almacenar los respaldos.

Se puede optar por dispositivos de almacenamiento tradicional: tarjetas de memoria, unidades flash, discos duros externos, cintas magnéticas; otra opción es el almacenamiento en red, como NAS (*Network Attached Storage*), SAN (*Storage Area Network*), nube o bóveda digital. En cualquier caso se debe considerar la cantidad de información almacenada, la frecuencia con que será consultada, si debe estar disponible por normativa y el período de retención específico según el tipo de información.

c) Gestión integral del ciclo de vida. Contempla el seguimiento a las copias de datos y copias de seguridad contra políticas de protección y retención, incluida la eliminación de las que no se necesitan.

Debido al espacio que demanda la retención de los respaldos de información, es necesario cambiar de un tipo de almacenamiento a otro y considerar el tiempo de retención marcado en la normatividad para el tipo de información contenida.

Una vez que la información deje de ser útil o llegue al final de su período de retención, deberá ser eliminada de manera segura. Para ello es necesario seguir los pasos marcados en la guía "Borrado seguro de información", disponible en este enlace https://www.seguridad.unam.mx/borrado-seguro-de-informacion

d) Procedimientos de respaldo y restauración de la información. Se deben documentar los procedimientos para el respaldo y restauración de los sistemas, aplicaciones, datos y documentos en línea que sean importantes para el área universitaria.

Si los respaldos se automatizan o realizan de forma remota, se deberá considerar la supervisión de eventos y la capacidad disponible de recursos: memoria, procesador, espacio libre en disco, entre otros. Por ejemplo, el uso del CPU deberá ser menor al 70% para detectar cualquier falla de manera temprana y rectificarla.

Se sugiere considerar pruebas de restauración de los respaldos realizados para garantizar la integridad de los datos y que se encuentren en buen estado.

No siempre será factible probar cada respaldo, por lo cual se recomienda priorizar las copias de seguridad críticas y verificar su dependencia con otras, de manera que permitan recuperar el servicio brindado por el sistema o la totalidad de la información que se requiere para la operación del área.

Se aconseja probar periódicamente los respaldos para verificar su integridad y su capacidad para restaurarse. Esto debe realizarse al menos una vez al mes cuando se trata de datos críticos.

Entre los problemas más comunes con los respaldos están los siguientes:

- Falla física (mecánica, eléctrica, magnética, etc.) en los medios de almacenamiento: disco, cinta, entre otros.

- Error humano. Es posible elegir mal el medio de almacenamiento (cinta en lugar de discos), realizar un respaldo incompleto o sobrescribir respaldos accidentalmente.
- Actualizaciones de software que generen incompatibilidades entre el software de los respaldos y las nuevas versiones de las aplicaciones o del sistema operativo.
- Ciberataques: ransomware, daño intencionado a los respaldos, etc.
- Fallas en la infraestructura, por ejemplo: en las unidades o bibliotecas de cintas, arreglos de discos, servidores de respaldo y problemas en la red (como la latencia), etc.

Se recomienda mantener un catálogo de recuperación actualizado para rastrear cada copia: la de seguridad, la replicación o las copias de un momento específico; además de registrar las herramientas antimalware con las que se han escaneado y los resultados del análisis. También es necesario documentar la forma en que se recupera la información.

Adicionalmente se recomienda diseñar y documentar un plan de contingencia que describa el procedimiento de recuperación ante desastres, capacitar al personal involucrado respecto de sus responsabilidades y actividades, probar el proceso y mantenerlo actualizado al menos una vez al año.

e) Requisitos de cifrado para datos sensibles o confidenciales en reposo y para datos en tránsito (los métodos de cifrado aplicados a los datos de respaldo deben ser tan seguros como los utilizados en su almacenamiento). Se debe considerar la retención de claves de cifrado y la rotación de claves.

Es necesario cifrar la información sensible o que contenga datos personales, en especial los que se guarden en servicios de nube pública, como lo indica el Artículo 21 de las “Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad”.

La fuerza del cifrado tiene en cuenta el período específico durante el cual debe preservarse la confidencialidad de los datos personales cifrados. Así mismo, los datos personales se deben tratar mediante un cifrado fuerte antes de su transmisión.

Se recomienda que el cifrado de los respaldos almacenados en la nube pública no sea de menor capacidad al equivalente a AES (Advanced Encryption Standard), de 128 bits.

f) Otros requisitos de protección pueden ser la firma digital, el tipo de almacenamiento, la ubicación de resguardo, la seguridad de las instalaciones (incluida la protección contra incendios, explosiones e interferencias magnéticas), la inmutabilidad y el bloqueo, la cantidad mínima de copias por conjunto de respaldo y la distribución geográfica de dichas copias.

Para reducir los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, será necesario proteger de manera física y lógica el equipamiento, los medios de almacenamiento y los respaldos.

g) Revisión y mantenimiento del plan. Se debe definir el proceso para revisar y mantener el plan y los procedimientos operativos, al menos anualmente.

h) Referencia a los marcos regulatorios aplicables con los controles apropiados. Consultar la sección Marco legal.

2.2.1. Sobre el nombre de los archivos

Es recomendable no guardar archivos de respaldos con nombres largos (más de 64 caracteres), ya que pueden ocasionar problemas al ser interpretados por diferentes sistemas operativos y/o aplicaciones de descompresión.

También se aconseja nombrar los respaldos de manera que permitan reconocer su contenido. Por ejemplo: bd_rua_produccion_20230504.backup

En el nombre de los archivos o carpetas de los respaldos se sugiere no dejar espacios en blanco y evitar el uso de caracteres especiales, como son *#$%&?¡'¿<>:|*/()*, o acentos, debido a que algunos sistemas no los permiten o pueden ocasionar diversos problemas cuando se requiere utilizar el archivo o carpeta.

2.2.2. Sobre el almacenamiento de la información

Se recomienda revisar los “Lineamientos generales y políticas sobre almacenamiento e información compartida entre los sistemas existentes” y las “Recomendaciones para el almacenamiento de información”, disponibles en la Normateca de TIC de la UNAM. A ésta se puede ingresar mediante el sitio https://www.red-tic.unam.mx/

Los respaldos y la documentación relacionada deben ser almacenados en sitios diferentes a donde reside la información primaria (regla 3-2-1); también es necesario protegerlos contra modificaciones. De este modo se evita la pérdida cuando un desastre (terremoto, incendio, inundación, etc.) afecta la ubicación de trabajo.

Para evitar afectaciones sobre los soportes físicos, se deben revisar periódicamente las condiciones ambientales y la seguridad física de los lugares donde se almacenen. Se sugiere hacerlo cada seis meses, al menos.

Se debe considerar que los dispositivos de almacenamiento se deterioran con el tiempo, son susceptibles a fallos mecánicos, pueden sufrir las consecuencias de desastres, ser objeto de errores humanos en su manipulación (caídas, contacto con el agua u otros líquidos, etc.) o simplemente caer en la obsolescencia. Por ello se recomienda desarrollar planes de actualización de los medios de almacenamiento que resguarden la información, considerando el tiempo de conservación definido en la normatividad y/o en el área universitaria (por ejemplo, información histórica que deba mantenerse perpetua).

Es conveniente realizar un mantenimiento periódico al hardware de los dispositivos de almacenamiento para prevenir posibles fallos mecánicos. También es pertinente actualizar oportunamente el software para reducir el riesgo de posibles vulnerabilidades, infecciones e intrusiones.

Dentro de las consideraciones para actualizar los respaldos de la información a nuevos formatos, medios de almacenamiento o aplicaciones están la obsolescencia del formato, del software o del hardware para reproducirlo.

Se recomienda crear un registro sobre la vida útil de los soportes físicos de respaldo para tomar las decisiones pertinentes que contribuyan a proteger la integridad de los datos. Por ejemplo: los CD-R y CD-RW sin usar tienen una vida útil muy corta, de cinco a diez años; los DVD-RW grabados pueden conservarse en buen estado hasta 30 años; las cintas magnéticas hasta 25 años (según la frecuencia de las reproducciones o reescrituras) y los discos duros hasta diez años, entre otros.

En caso de obsolescencia o daño de los medios de almacenamiento se sugiere considerar la destrucción física de soportes no robustos como CD, DVD o papel, para lo cual puede utilizarse una destructora de soportes magnéticos o papel. Cuando se trate de discos duros o cintas, se puede optar por el borrado seguro, la desmagnetización o la destrucción física. También es posible recurrir a empresas especializadas en la destrucción certificada de información, las cuales deben entregar evidencia del proceso realizado.

Acorde con los “Lineamientos generales y políticas sobre el almacenamiento e información compartida entre los sistemas existentes”, los responsables TIC deben establecer un procedimiento para registrar y verificar el borrado seguro; debe quedar definida la responsabilidad de quien lo realiza y de quien verifica. Adicionalmente, se sugiere aplicar el procedimiento establecido en la Sección H De la Baja Documental de los “Lineamientos generales para la organización, administración y conservación de los archivos de la UNAM”.

2.2.3. Sobre copias de un punto en el tiempo (Point-in-Time Copies)

Implica una copia de un volumen de almacenamiento, archivo o base de datos, tal como apareció en un momento dado, la cual se utiliza como método de protección de datos; se le conoce como snapshot. En caso de una falla, los usuarios pueden restaurar sus datos a partir del punto en que se generó el snapshot.

Cuando se maneja un snapshot a nivel de base de datos, se crea una “fotografía” de la base de datos en un punto en el tiempo.

Existen dos métodos principales para mantener actualizados los snapshots de un punto en el tiempo:

- Reasignación de puntero: Se realizan nuevas copias de un snapshot en un momento dado, la copia más reciente mantendrá una asignación a la copia original.

- Copia en escritura: Se realizan cambios en los datos. Solo los datos modificados se copiarán nuevamente, en lugar de hacer otra copia completa del conjunto de datos.

Cuando se usen snapshots como parte del esquema de respaldos, entonces:

a) Deben cumplir con los requisitos del objetivo de punto de recuperación (RPO) de los datos a respaldar. Por ejemplo, si la organización o el estándar de cumplimiento establece no más de cinco minutos de datos perdidos en la recuperación, entonces el intervalo de cada snapshot debe ser de cinco minutos o menos.
b) También deben cumplir con los requerimientos de retención. Por ejemplo, si las copias por hora deben ser al menos de las últimas 48 horas, se deben preservar al menos 48 snapshots que correspondan al período.

Se recomienda que los snapshots obsoletos sean borrados para reducir el posible vector de ataque.

2.2.4. Sobre el espejeo y replicación de la información

Realizar un espejeo consiste en generar una copia exacta de los datos de manera sincronizada en dos medios o dispositivos diferentes. Si uno falla, la información estará disponible a través del otro.

Un método para generar el espejo de la información (*data mirroring*) es el RAID 1 (*redundant array of independent disks*), que consiste en generar una copia exacta de los datos en tiempo real; se utiliza a nivel de la configuración de los discos a través de hardware (tarjeta controladora) o mediante un software. En caso de falla en uno de los discos, mantiene la disponibilidad del servicio del sistema de información y evita la pérdida de los datos.

Por otra parte, se puede realizar el espejeo de los servidores que contienen el Sistema Manejador de Bases de Datos (SMBD) para mantener copias sincronizadas de las mismas, incluyendo las transacciones que se realicen en ellas. En este tipo de configuración, un servidor suele funcionar como primario y otro como espejo. En caso de falla en uno de los servidores, se mantiene la disponibilidad a través del otro servidor.

El espejeo de información se llega a utilizar conjuntamente con la replicación para mejorar la disponibilidad de las bases de datos.

La replicación, por otra parte, es el proceso de copia de datos de un sistema de almacenamiento a otro por bloques y de forma diferencial. Se suele llevar a cabo a nivel de archivo, de directorio o de sistema de archivos.

A nivel de bases de datos, la replicación consiste en duplicar datos y objetos de base de datos almacenados en diferentes ubicaciones. Para ello, las bases de datos se sincronizan ante cualquier cambio del sitio primario a los sitios secundarios en donde se replica la información.

La replicación puede ser síncrona o asíncrona. En la primera no se reconoce la escritura/transacción del almacenamiento principal hasta que se ha replicado el bloque en la sede de destino

(almacenamiento secundario). En la segunda, primero reconoce la escritura/transacción y luego replica el bloque/registro(s) al cabo del tiempo.

Se recomienda, tanto en la replicación síncrona como en la asíncrona, que el mismo nivel de protección de datos (cifrado de datos en reposo, restricciones de acceso, por ejemplo) utilizado en el almacenamiento principal también se transfiera al almacenamiento secundario.

Cuando los arreglos no tienen volúmenes replicados compartidos, se recomienda deshabilitar la relación de confianza de replicación entre ellos. Cuando los arreglos tienen volúmenes replicados compartidos, los privilegios entre sí deben limitarse a los volúmenes que comparten.

La confidencialidad y la integridad de los datos sensibles, en tránsito durante la replicación y el espejeo, deben protegerse mediante el cifrado. Esta recomendación se puede relajar si existen controles de mitigación apropiados: la replicación a corta distancia dentro de la misma área o en el centro de datos, por ejemplo.

Se recomienda que las replicaciones obsoletas sean borradas para reducir la superficie de ataque.

Anexo 1. Elementos de un plan de recuperación de desastres

Es un componente del plan de continuidad que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operatividad mínima, luego de una contingencia en la que se ven afectados los procesos y recursos informáticos que sostienen a la organización.

En un plan de recuperación de desastres (Disaster Recovery Plan, DRP) se deben contemplar los siguientes puntos:

- Determinación del escenario considerado
  - Condiciones físicas del entorno
  - Servicios y aplicaciones existentes
  - Infraestructura involucrada
- Definición de los tipos de operación en una contingencia
  - Operación inicial (normal)
  - Operación alternativa
  - Operación normal alterna
  - Operación normal restablecida
- Identificar todos los activos implicados en los procesos críticos de la organización
  - Verificar procesos críticos de la organización
  - Verificar el catálogo de servicios
  - Verificar el nivel de criticidad: equipos, servicios y aplicaciones
  - Verificar los acuerdos de niveles de servicio y de operación
- Establecimiento de los servicios mínimos críticos para la operación
- Análisis de los riesgos
  - Identificación de riesgos
  - Matriz de riesgos (probabilidad - impacto)
  - Reporte de evaluación de riesgos
  - Determinación de niveles de desastre
- Estrategia de recuperación
  - Presentación de las distintas estrategias posibles de recuperación
  - Valoración y selección de la estrategia de recuperación
  - Elaboración de la estrategia de recuperación:
    - Plan de tratamiento de riesgos
    - Mitigación de riesgos (medidas preventivas)
    - Descripción de la estrategia
    - Establecimiento del Equipo de Recuperación del Entorno de Desastres
  - Requerimientos para llevar a cabo el plan
  - Establecimiento de los procedimientos:
    - Declaración de la emergencia
    - Recuperación de los servicios
    - Restablecimiento de las condiciones normales de operación
- Establecimiento de un Plan de Pruebas del DRP
- Lineamientos para el seguimiento y mantenimiento del DRP

Bibliografía y referencias electrónicas

- DGTIC (2017). *Circular DGTIC/003/2017 Procedimiento para el borrado información.* Recuperado: 2 de mayo de 2023. URL: https://www.red-tic.unam.mx/recursos/2017/2017_Circular_DGTIC_003_2017.pdf
- Domínguez, Ricardo. (2005). *Tesis de Licenciatura: Técnicas de respaldo y recuperación de bases de datos implementadas con el DBMS Oracle.* FES Acatlán.
- INAI (2016). *Guía para el Borrado Seguro de Datos Personales.* Recuperado: 3 de marzo de 2023. URL: http://transparencia.inaes.gob.mx/doctos/pdf/transparencia/Guias/Gu%EDa_Borrado_Seguro_DatosPersonales.pdf
- Instituto Nacional de Ciberseguridad (2016). *Guía de almacenamiento seguro de la información.* Recuperado: 3 de mayo de 2023. URL: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf
- Instituto Nacional de Ciberseguridad (2022). *Copias de seguridad. Una guía de aproximación para el empresario.* Recuperado: 3 de mayo de 2023. URL: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
- ISO/IEC (2015). *Information technology — Security techniques — Storage security.*
- ISO/IEC (2013). *Tecnología de la Información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información.*
- Nash, T., & Olmsted, A. (2017). *Performance vs. security: Implementing an immutable database in MySQL*. Recuperado: 2 de mayo de 2023. URL: https://www.researchgate.net/publication/325071211_Performance_vs_security_Implementing_an_immutable_database_in_MySQL
- NIST (2020). *Security Guidelines for Storage Infrastructure.* Recuperado: 2 de mayo de 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf
- Gillis, A. (s.f.). *Digital signature.* Recuperado: 4 de mayo de 2023. URL: https://www.techtarget.com/searchsecurity/definition/digital-signature
- Tapia Corona, R., & Garcia Macias, K. C. (2001). *Replicación simétrica, un caso avanzado de las bases de datos Oracle. Un ejemplo de su aplicación.* México.
- TechTarget (2015). *Point-in-time snapshot.* Recuperado: 3 de mayo de 2023. URL: https://www.techtarget.com/searchstorage/definition/point-in-time-snapshot-PIT-snapshot
- UNAM (2016). *Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.* Recuperado: 2 de mayo de 2023. URL: http://www.transparencia.unam.mx/documentos_transparencia/manual-de-normas_2021.pdf

- UNAM (2018). *Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México.* Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/recursos/LineamientosArchivosUNAM.pdf
- UNAM (2020). *Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.* Recuperado: 14 de septiembre de 2022. https://www.red-tic.unam.mx/recursos/2020/2020_Norma_ComiteTransparencia_01.pdf
- UNAM (2021). *Glosario de términos de TIC.* Red-TIC, UNAM. Recuperado: 2 de mayo de 2023. URL: https://www.red-tic.unam.mx/recursos/2022/2022_Glosario_RedTIC_01.pdf
- UNAM (2021). *Recomendaciones para el almacenamiento de información.* Red-TIC, UNAM. Recuperado: 2 de mayo de 2023. URL: https://www.red-tic.unam.mx/recursos/2021/2021_Recomendaciones_RedResponsablesTIC_02.pdf
- UNAM (2022). *Catálogo de disposición documental.* Recuperado: 31 de agosto de 2022. URL: https://www.repositoriotransparencia.unam.mx/DocumentosDigitales/descargar/JO HE_1650676046
- UNAM (2022). *Lineamientos generales y políticas sobre almacenamiento e información compartida entre los sistemas existentes.* Recuperado: 2 de mayo de 2023. URL: https://www.red-tic.unam.mx/recursos/2022/2022_Lineamiento_RedResponsablesTIC_01.pdf
- UNAM (2022). *Lineamientos y recomendaciones para la administración de bases de datos.* Recuperado: 2 de mayo de 2023. URL: https://www.red-tic.unam.mx/recursos/2022/2022_Lineamientos_DGTIC_01.pdf
- UNAM (2022). *Política de uso y Acuerdo del Nivel de Servicio - Bóveda Digital UNAM.* Red-TIC, UNAM. Recuperado: 3 de marzo de 2023. URL: https://www.red-tic.unam.mx/content/politica-acuerdo-nivel-servicio-boveda-digital

Créditos

Rector
Dr. Enrique Luis Graue Wiechers

Secretaria de Desarrollo Institucional
Dra. Patricia Dolores Dávila Aranda

Director General de Cómputo y de Tecnologías de Información y Comunicación
Dr. Héctor Benítez Pérez

Coordinación
Dra. Ana Yuri Ramírez Molina
Mtra. María de Lourdes Velázquez Pastrana

Elaboración
Ing. Pedro Bautista Fernández
Mtro. Jesús Salvador Fernández Rauda
Mtro. Alberto González Guízar

Revisión
Ing. José Othoniel Chamú Arias – DGTIC, UNAM
Lic. José Luis Chávez Sánchez – DGTIC, UNAM
Mtra. Susana Laura Corona Correa - DGTIC, UNAM
Lic. Fernando Israel González Trejo, FES Acatlán, UNAM
Mtro. Fernando Huerta Trejo – DGAE, UNAM
Lic. Juventino Jarquín Berra - DGPr, UNAM
Mtro. Miguel Ángel Jiménez Bernal - DGBSDI, UNAM
Lic. Ángel Martínez Hernández - DGTIC, UNAM
Mtra. Elizabeth Rangel Gutiérrez - DGTIC, UNAM
Mtro. Hugo Alonso Reyes Herrera - DGTIC, UNAM
Mtro. Fernando Zaragoza Hernández - DGAE, UNAM