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

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

Contenido

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

Objetivo

Definir los lineamientos, elementos de referencia y buenas prácticas para la protección y resguardo de la información electrónica gestionada por 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 que es responsable de sistemas o fuentes de información electrónica de la universidad, con la finalidad de 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 (información). Elemento de clasificación de los activos de información que permite definir, acorde a su importancia e impacto para una organización, cómo ha de ser tratada y protegida la información.

Copia de seguridad (respaldo). Es la elaboración de una 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 datos o archivos digitales de 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, 6 horas.

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

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

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

Respaldo incremental. Copia de seguridad en la que se resguardan 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 pasar antes de una recuperación completa de los datos, es decir, en cuánto tiempo se recuperará la copia de seguridad de los datos. Por ejemplo: 2 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

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

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

De igual forma, las áreas universitarias deben establecer procedimientos para permitir el acceso y recuperación de los datos (tanto al medio de almacenamiento como a la lectura de los formatos utilizados) a través de todo el período de retención que tenga la información de acuerdo a la normatividad aplicable.

Las áreas universitarias deben establecer procedimientos que permitan la eliminación de la información y/o medios de almacenamiento una vez pasado el período de retención, permitiendo la trazabilidad de los mismos al interior 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 de los servicios de TI que soportan los sistemas de información de un área universitaria.

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 recuperar 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 que 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 todos 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 por mes, debidas a interrupciones no planeadas
- Número de procesos críticos de negocio que dependen de TI, que no están cubiertos por un plan de continuidad.
- % 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 de tiempo. Por ejemplo: 1 respaldo diario, 2 respaldos por semana, 1 snapshot diario (generalmente utilizado para máquinas virtuales o bases de datos).
   ii) Retención. Se refiere al periodo de tiempo para mantener almacenados los datos en los respaldos realizados antes de eliminarlos acorde a la normatividad y utilidad. Por ejemplo: se conservan los respaldos del último mes o los últimos 10 días por 6 meses.

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

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 de tiempo 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 lo que se deben mantener alejados de altas temperaturas, polvo, luz solar y humedad.

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

v) Tipo de protección. Se sugiere para todo respaldo 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, como: tarjetas de memoria, unidades flash, discos duros externos, cintas magnéticas; almacenamiento en red, como: NAS (*Network Attached Storage*), SAN (*Storage Area Network*), nube o bóvedas digitales. Para lo cual se debe considerar aspectos como: la cantidad de información almacenada, la frecuencia con que será accedida, si se requiere tener disponible por cuestiones normativas y el período de retención especificada para el tipo de información.

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

Debido al espacio que implica retener los respaldos de información se debe considerar el mover de un tipo de almacenamiento a otro y el tiempo de retención que se considera en la normatividad para el tipo de información contenida.

Así mismo, dentro del ciclo de vida de la información llegará el momento en que dejará de ser útil o que llegue al final de su período de retención y, por tanto, deberá ser eliminada de manera segura (https://www.seguridad.unam.mx/borrado-seguro-de-informacion).

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

d) Procedimientos de respaldo y restauración de la información. Los procedimientos para el respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea importantes para el área universitaria deben estar documentados.

Si los respaldos se automatizan o se realizan de forma remota, se deberá considerar la supervisión de eventos y capacidad disponible de recursos como memoria, procesador, espacio libre en disco, entre otros, por ejemplo, que el uso del CPU sea menor al 70% para que cualquier falla pueda ser detectada de manera temprana y ser rectificada antes de que cause problemas.

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 creado, por lo que se sugiere priorizar las copias de seguridad que son críticas y verificar dependencias con otras, de manera que permitan recuperar el servicio brindado por el sistema o la totalidad de la información que requiere para la operación del área.

Se aconseja probar periódicamente los respaldos (al menos una vez al mes para datos críticos) para verificar su integridad y su capacidad para restaurarse. Entre las fallas más comunes en los respaldos están:

- Falla física (mecánica, eléctrica, magnética, etc.) en los medios de almacenamiento como: disco, cinta, entre otros.
- Error humano, por ejemplo: definir mal el medio de almacenamiento que contendrá los datos (cinta en lugar de discos), realizar un respaldo incompleto o sobrescribir respaldos accidentalmente.
- Actualizaciones de software que generen incompatibilidades entre el software de respaldos y las nuevas versiones de las aplicaciones o del sistema operativo.
- Ciberataques: ransomware, daño intencionado a los respaldos, etc.
- Falla de infraestructura, por ejemplo: en las unidades o bibliotecas de cintas, arreglos de discos, servidores de respaldo y problemas en la red como alta latencia, etc.

Se recomienda mantener un catálogo de recuperación actualizado para rastrear cada copia (incluida la copia de seguridad, la replicación, las copias de un momento dado, etc.) que registre con qué herramientas antimalware se ha escaneado y cuáles son los resultados, además de documentarse la forma de recuperación de 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 a realizar, 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 al menos tan seguros como el utilizado en su almacenamiento). También se debe considerar la retención de claves de cifrado y la rotación de claves.

   Se deberá considerar cifrar la información sensible o que contenga datos personales a ser respaldada, 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 que se almacenen en la nube pública no deberá ser 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 (ver sección de marco legal).

2.2.1. Sobre el nombre de los archivos

Es recomendable que no se guarden archivos de respaldos con nombres muy largos (más de 64 caracteres), ya que ocasionan problemas al ser interpretados en diferentes sistemas operativos y/o aplicaciones de descompresión.

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

Se sugiere no utilizar espacios en blanco en ninguna parte del nombre y evitar el uso de caracteres especiales como: *#$%&?¡'¿<>:|*/()* o acentos para nombrar archivos y carpetas de los respaldos debido a que algunos sistemas no los permiten o pueden ocasionar problemas en el uso del archivo.

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"*, así como las "*Recomendaciones para el almacenamiento de información en la normateca de la Red de Responsables TIC"* disponibles en (https://www.red-tic.unam.mx/).

El almacenamiento de los respaldos y la documentación relacionada debe realizarse en lugares diferentes de donde reside la información primaria (regla 3-2-1) y protegidos contra modificaciones. De este modo se evita la pérdida si un desastre (terremoto, incendio, inundación, etc.) afecta a todo el edificio o la ubicación de trabajo.

Las condiciones ambientales y seguridad física de los lugares donde se almacenen los soportes físicos deben revisarse periódicamente con la finalidad de verificar que no los afecten de manera adversa, se sugiere hacerlo en un período no superior a los seis meses.

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 la obsolescencia del propio soporte. Por lo que se recomienda desarrollar planes de actualización de los medios de almacenamiento que resguarden la información considerando el tiempo de conservación que tenga definido en la normatividad y/o el área universitaria (por ejemplo, información histórica que deba mantenerse perpetua).

Es aconsejable realizar un mantenimiento periódico del hardware y software de los dispositivos de almacenamiento, con el fin de prevenir los posibles fallos mecánicos del hardware, así como las posibles vulnerabilidades, infecciones e intrusiones que pueden derivar del software sin actualizar.

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 llevar un control de la vida útil de los soportes físicos de respaldo y así evitar que cualquier posible deterioro afecte a la integridad de los datos. Por ejemplo: los CD-R y CD-RW sin usar tienen una vida útil muy corta (de 5 a 10 años), los DVD-RW grabados (hasta 30 años), cintas magnéticas (hasta 25 años, depende de la frecuencia de las reproducciones o reescrituras), discos duros (hasta 10 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, y para discos duros o cintas puede optarse por el borrado seguro, la desmagnetización o la destrucción física. Se puede recurrir a empresas especializadas en la destrucción certificada de información que entreguen evidencia de la destrucción.

Acorde a los "Lineamientos generales y políticas sobre el almacenamiento e información compartida entre los sistemas existentes", los responsables TIC deben establecer un procedimiento donde se registre y verifique el borrado seguro, quede definida la responsabilidad de quien lo realiza y de quien verifica, adicionalmente, se sugiere considerar seguir el procedimiento definido 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 y se utiliza como método de protección de datos, a la cual se le conoce como snapshot. A partir de las cuales los usuarios pueden restaurar sus datos ante una falla a partir del punto en que fue generado el snapshot.

Cuando se maneja un snapshot a nivel de base de datos se crea una "fotografía" de cómo se veía la base de datos fuente en el momento de que se generó.

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

- Reasignación de puntero: Se realizan nuevas copias de un snapshot de 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, estos deben de ser configuradas de acuerdo con:

a) El snapshot debe 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 requiere de no más de cinco minutos de datos perdidos en la recuperación, entonces el intervalo de cada snapshot debe ser de 5 minutos o menos.

b) El snapshot debe cumplir con los requerimientos de retención. Por ejemplo, si las copias por hora deben ser al menos de las últimas 48 horas, se debe asegurar 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/dispositivos diferentes, con el fin de que si uno falla, la información siga estando disponible a través del otro.

Un método para generar un espejo de la información (*data mirroring*) es el RAID 1 (*redundant array of independent disks*), el cual 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. Permite que en caso de la falla de uno de los discos se mantenga la disponibilidad del servicio del sistema de información y no se pierdan 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 la duplicación de datos y objetos de base de datos almacenados en diferentes ubicaciones. Para ello las bases de datos se sincronizan ante cualquier cambio del primario a los 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 que, tanto en la replicación síncrona como en la asíncrona, el mismo nivel de protección de datos (p. ej., cifrado de datos en reposo, restricciones de acceso) que se utiliza en el almacenamiento principal también debe transferirse al almacenamiento secundario.

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

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, sus 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 cuando existen controles de mitigación apropiados (por ejemplo, la replicación a corta distancia dentro de la misma área o Centro de Datos).

Se recomienda que las replicaciones obsoletas sean borradas para reducir la posible 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 debe 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 dentro de la organización
  - Verificar catálogo de servicios
  - Verificar el nivel de criticidad: equipos, servicios, 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 x 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 seguro de información de la UNAM almacenada en medios digitales**. 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**. 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 de la 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

LINEAMIENTOS Y RECOMENDACIONES PARA EL RESGUARDO DE INFORMACIÓN ELECTRÓNICA

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 DGTIC, UNAM
Mtra. María de Lourdes Velázquez Pastrana
Dra. Ana Yuri Ramírez Molina
Mtro. Juan Manuel Castillejos Reyes

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

Revisión técnica
Mtra. Susana Laura Corona Correa – DGTIC, UNAM
Ing. José Othoniel Chamú Arias – 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
Mtro. Hugo Alonso Reyes Herrera – DGTIC, UNAM
Mtro. Fernando Zaragoza Hernández – DGAE, UNAM

Revisión jurídica
Mtra. Elizabeth Rangel Gutiérrez – DGTIC, UNAM
Lic. José Luis Chávez Sánchez – DGTIC, UNAM

Revisión estructural y publicación en NormaTIC
Mtra. Ma. Teresa Ventura Miranda – DGTIC, UNAM
L.A. Heidi Alejandra Pérez Vera – DGTIC, UNAM