Política Específica de Copias de Seguridad

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

Establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo haciendo copias de seguridad, ensayando su oportuna recuperación, registrando eventos o fallos y monitoreando el entorno de los equipos cuando proceda.

Este documento se aplica a todo el alcance del Sistema Integrado de Gestión (SIG); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SIG.

Los usuarios de este documento son todos los colaboradores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, clausula 8.13.

3. POLÍTICA ESPECÍFICA

Todo colaborador de DACTA o tercero para el desempeño de sus funciones como organización, se compromete a lo siguiente:

3.1. INFORMACIÓN DE USUARIOS INTERNOS

- Ningún tipo de información de DACTA puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación del usuario de cada computadora con su jefe inmediato a la cabeza, trasladar toda información valiosa a las carpetas destinadas para este fin dentro de los servidores de DACTA.
- Es responsabilidad de cada usuario, del coordinador de área y del Gerente respectivo mantener organizada, clasificada y depurada la información de las carpetas virtuales asignadas dentro de los servidores de DACTA.
- Es responsabilidad de cada usuario, del coordinador de área y Gerente respectivo solicitar oportunamente al Coordinador de TI la inclusión de nuevas carpetas o bases de datos en la relación de activos a respaldar especificando la frecuencia con la que debe ser respaldada dicha información.
- El Coordinador de TI debe asegurar los respaldos diarios de la información de todos los servidores con información relevante para las operaciones de DACTA.

3.2. RESPALDOS DE BASE DE DATOS

Se definirán procedimientos generales para el resguardo de la información, que deberán considerar los siguientes puntos:

- Las copias de respaldo de bases de datos deben ser almacenadas en un servidor físico distinto al cual pertenece la información respaldada. El lugar, que albergue los dispositivos de almacenamiento donde se guardarán los respaldos, puede ser interno o externo a DACTA. En cualquiera de los casos, este lugar, deberá contar con las condiciones físicas, ambientales y de seguridad adecuadas.
- Deberá evaluarse la opción de almacenar copias recientes de las bases de datos y de toda información crítica gestionada por DACTA en una ubicación remota y a una distancia suficiente como para evitar daños provenientes de un desastre en la sede Central. Los respaldos deben contar con registros específicos y completos de la información respaldada y con los procedimientos documentados para la recuperación.

- Periódicamente, el Coordinador de TI de DACTA, o la persona que éste designe verificará la correcta ejecución de los procesos de backup y actualizará diariamente el inventario de los backups realizados.
- Las copias de respaldo se guardarán con el objetivo de restaurarla para atender los siguientes eventos: Efectos posteriores a un ataque de virus informático, avería en los discos de almacenamiento, problemas de los servidores o computadores, materialización de siniestros, pruebas de calidad y/o por requerimiento legal.
- Los medios o dispositivos de almacenamiento que tengan que ser dados de baja deben pasar por un proceso de borrado seguro y posteriormente deben ser destruidos asegurándose, el Coordinador de TI, que nunca más se pueda recuperar ninguna información.

3.3. RECUPERACIÓN DE LA INFORMACIÓN

El Coordinador de TI determinará los requerimientos para resguardar cada activo de información en función de su criticidad. Según ello, se definirá y documentará un esquema de resguardo de la información. También dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de DACTA. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de contingencia de las actividades de DACTA.

Se definirán procedimientos generales para la restauración de la información abordando los siguientes puntos:

- Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
- Probar periódicamente la recuperación de los servidores de bases de datos como de los servidores de aplicaciones buscando minimizar la pérdida de información, así como el tiempo de restauración del servicio.

En caso de no cumplir con la presente Política Específica de Copias de Seguridad, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Oficial de Seguridad de Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, tomará las medidas disciplinarias necesarias, las cuales están sujetas al Código de ética y conducta de DACTA.

4. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
F-E-SIG-039	Solicitud de respaldo de Información periódica	Coordinador de TI	12 meses
F-E-SIG-008	Inventario de copias de respaldo	Coordinador de TI	12 meses
F-E-SIG-009	Registro de eliminación de datos	Especialista de Seguridad Informática	12 meses

5. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	OSI	Comité SIG	Gerente General
2	22/02/2023	Actualización	OSI	Comité SIG	Gerente General
2	22/02/2024	Revisión	OSI	Comité SIG	Gerente General
Firmas de la versión vigente			 S. Rafaile  A. Morales	 S. Rafaile  A. Morales	 G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022.