POLÍTICA DE RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN

1. INTRODUCCION

La información es un recurso importante del Consejo Nacional para la Igualdad de Género para el cumplimiento de los objetivos estratégicos institucionales, puesto que es un soporte para la toma de decisiones.

Mediante la presente política se establecen lineamientos generales aplicables a la información de la Institución, referente a los procedimientos para el respaldo, resguardo y recuperación de la información, que se debe realizar en el Consejo.

2. MARCO NORMATIVO

a. Acuerdo Ministerial 166, EGSI, y su última modificación del 15 de junio de 2016.
b. NTC ISO 17799: "Seguridad de la Información" Punto 10.5 "Las copias de respaldo de información y software deberían ser realizadas y probadas con regularidad, conforme a la política de seguridad y de continuidad de negocio".
c. NTC ISO 27001 basado en el código de buenas prácticas y objetivos de control el Anexo A, dominio de Control A.12 Seguridad en la Operación - Numeral: A.12.3. Copias de Seguridad, A.12 3.1 Copias de seguridad de la Información, cuyo objetivo es mantener la integridad y disponibilidad de los servicios de tratamiento de información y comunicación.

Ley Orgánica de Transparencia y Acceso a la Información Pública.

3. ANTECEDENTES

El Consejo gestiona información, la cual debe ser manejada y respaldada de forma segura y oportuna. El Esquema Gubernamental de Seguridad de la Información ECSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información.

4. JUSTIFICACION

El establecimiento de políticas de respaldo, resguardo y recuperación es fundamental para garantizar la continuidad de los servicios institucionales. Las políticas de respaldo, resguardo y recuperación de la información, permitirán asegurar la información manejada por la Institución.

El EGSI establece: "Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad,

integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad la requiera".

5. OBJETIVO

Establecer los lineamientos de respaldo para proteger la información, configuraciones y aplicaciones de software en caso de presentarse alguna contingencia y posibilitar la recuperación de la información en el menor tiempo posible garantizando la confidencialidad, integridad y disponibilidad de los datos en el Consejo Nacional para la Igualdad de Género.

6. ALCANCE

Esta política es aplicable a toda la información electrónica contenida en los servidores, estaciones de trabajo y equipos comunicacionales que contengan información, configuraciones, aplicativos y servicios críticos de la Institución.

Esta política se aplica a todo el personal del Consejo, independientemente del tipo de régimen laboral en que se encuentren, y a terceros que presten servicios a la Institución.

Esta política debe ser revisada y/o actualizada anualmente, o cuando se considere necesario por la Unidad de Tecnologías de la Información y Comunicación.

7. RESPONSABILIDADES

La Unidad de Tecnologías de información y Comunicación proporcionará los servicios tecnológicos para el respaldo, pruebas y recuperación de la información.

El Comité de Seguridad de la Información emitirá en coordinación con la Unidad de Tecnologías de la Información y Comunicación los lineamientos sobre el manejo seguro de la información del Consejo. Cada usuario/a tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de controlar el cumplimiento de esta política por parte de los/as usuarios/as bajo su unidad.

8. POLITICAS DE RESPALDO, RESGUARDO Y RECUPERACION DE LA INFORMACION DEL CONSEJO

La Institución, aplicará el EGSI para el manejo, respaldo, restauración y recuperación de activos informáticos de la Institución.

8.1. Definición de Activos Críticos

Los/as Directores/as de área y responsables de Unidad del Consejo, serán los/as encargados/as de identificar la información que necesitan, para mantener operativos sus

procesos, ante posibles eventos de pérdida de información. La Unidad de Tecnologías de la Información y Comunicación, establecerá un esquema de prioridad y periodicidad de respaldo, resguardo y recuperación de los activos informáticos generados u obtenidos, de acuerdo a un procedimiento establecido en el área

El procedimiento debe incluir principalmente:

- Generación de copias de respaldo de la información, aplicaciones, configuraciones, etc.
- Pruebas permanentes de los respaldos realizados, para verificar su integridad.
- Restauración de los respaldos.
- Inventario de los respaldos; y,
- Bitácoras de respaldos.

8.2. Etiquetado

Todas las copias de respaldo deberán estar claramente identificadas, con etiquetas que contengan la siguiente información:

- Nombre del/a servidor/a, funcionario/a, trabajador/a, practicante, cualquier persona que brinde servicio a la Institución
- Identificación (Nombre que identifique lo que contiene)
- Tipo de respaldo (completo, parcial, por período)
- Frecuencia: (anual, mensual, semanal, diario)
- Fecha de respaldo
- Nombre del responsable que realizó el respaldo

8.3. Registros de Auditoría

Toda ejecución de respaldo ya sea de forma manual o automática, debe generar un registro (logs) en el equipo, que permita la revisión del resultado de la ejecución.

8.4. Frecuencia y Tipo de Respaldos

La unidad de Tecnologías de la Información y Comunicación es la responsable de establecer el Plan de Respaldos, determinar los procedimientos de respaldo, resguardo y recuperación de los activos informáticos, su implementación y actualización. Se deberá contemplar de manera obligatoria, respaldos de bases de datos, logs, aplicaciones y configuraciones.

Las direcciones y unidades poseedoras de la información deberán planificar la obtención o ejecución de los respaldos, de tal manera que no afecte la disponibilidad de los servicios de la Institución.

Tipos de respaldos:

i. Respaldo completo o Total: Considera toda la información comprendida en el servidor, equipo fijo o móvil
ii. Respaldo Incremental: Se respaldarán los archivos creados a diario.
iii. Respaldo Diferencial: Se respaldarán todos los archivos modificados y creados en la semana.

8.5. Vigencia y permanencia de los datos

Las unidades poseedoras de la información, deben definir los periodos de permanencia de la información en función de su naturaleza con el fin de garantizar la consulta histórica de la misma considerando lo establecido en el Reglamento de Archivos de Contraloría General del Estado, Art. 10.- Conservación de documentación, que dice: "La documentación sujeta a control y seguimiento institucional, deben ser conservada durante 7 años, contados a partir de la fecha de emisión de la misma, sea formato físico o digital".

Es responsabilidad de las unidades poseedoras de la información, constatar de forma periódica, el valor y la utilidad de la información almacenada; con la finalidad de contar con espacio suficiente para poder respaldar otros archivos que sean de mayor utilidad.

8.6. Respaldos de Estaciones de Trabajo

Es responsabilidad de cada servidor/a, funcionario/a, trabajador/a, practicante y cualquier persona de la Institución, el debido respaldo de la información contenida en el computador asignado (estaciones de trabajo o portátiles), para lo cual la unidad de Tecnologías de la Información y Comunicación asignará una carpeta o recurso compartido para cada usuario, con un límite de cuota en el servidor de repositorio de datos.

Cualquier necesidad de respaldo urgente, debe ser solicitada formalmente por el/a jefe/a de la Dirección o unidad administrativa.

8.7. Manejo y Seguridad de Medios de Almacenamiento

Los medios de almacenamiento de la información o copias de respaldo, deben ser manipulados, custodiados única y exclusivamente por la Unidad de Tecnologías de la Información.

Los sitios donde se almacenan las copias de respaldo deben ser físicamente seguros, con los controles físicos y ambientales según normas y estándares

8.8. Pruebas de Restauración

Se deben efectuar pruebas planificadas de recuperación o restauración de las copias de respaldo por parte de la Unidad de Tecnologías de la Información, con el objetivo de garantizar que la información almacenada y protegida, se pueda extraer de forma confiable de los diferentes medios de almacenamiento en caso de una eventual restauración.

Las pruebas de recuperación se deben registrar en una bitácora, en la que se evidencie los resultados alcanzados.

9. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCION

El personal de la Institución acepta esta Política de Respaldo, Resguardo y Recuperación con la finalidad de garantizar la seguridad de la información del Consejo y se compromete a:

- La promoción activa de una cultura de seguridad
- Facilitar la socialización de este documento a todos/as los/as funcionarios/as de la Institución.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de Respaldo, Resguardo y Recuperación de la Información de la Institución.
- La verificación del cumplimiento de las políticas.

10. IDENTIFICACION DE RIESGOS

En cumplimiento al Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la información - EGSI, en el Artículo 7 "Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos, en base a la norma INEC ISO/IEC: 27005 "Gestión del Riesgo en la Seguridad de la Información". El Consejo procederá con la respectiva edificación de riesgos a los que puede estar expuesta la institución.

Elaborado Por
Rocío Balarezo B.
Responsable de Planificación y GE
junio 2020