POLÍTICA DE RESPALDOS Y COPIAS DE SEGURIDAD DE LA INFORMACIÓN

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre y Apellido / Cargo	Firma
Elaborado por:	Ing. Geovanny Meza, Mg. **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: JORGE GEOVANNY MEZA MORALES
	Ing. Darío Braganza **Analista de Tecnologías de la Información 3**	Firmado electrónicamente por: DARIO JAVIER BRAGANZA SUAREZ
Revisado y aprobado por:	Ing. Patricio Padrón **Director de Tecnologías de la Información y Comunicación**	Firmado electrónicamente por: NARDO PATRICIO PADRON CORREA

ÍNDICE

1. Notas de Cambio

Versión	Fecha	Detalle de la modificación
1	16/11/2021	Creación de la política

2. Antecedentes

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece una serie de hitos que contemplan la elaboración, implementación y difusión, de políticas, procedimientos, reglamentos, normas y demás instrumentos técnicos, que garanticen el manejo seguro de la información de las instituciones públicas.

Una de las formas de garantizar la seguridad de la información institucional, es con una adecuada política de respaldos y copias de seguridad, razón por la cual es imperativo contar con dichas políticas que contribuyan a generar una cultura de seguridad y protección de la información.

3. Alcance

Las políticas aquí descritas son de alcance general; es decir, para todos los servidores, funcionarios, instancias, dependencias, procesos y subprocesos del Secap.

4. Propósito

Detallar las políticas de respaldos y copias de seguridad (backup) de la información institucional y el software asociado a la misma, a fin de recuperarla en caso de fallas o imprevistos.

5. Definiciones

- **Aplicaciones de software:** Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
- **Backup:** Respaldo o copia de seguridad.
- **Copia de seguridad:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Internet:** Red mundial de computadores conectadas entre sí que ofrecen acceso y comparten información a través de un lenguaje común.
- **Intranet:** Red informática interna basada en los estándares de internet.

- **Red de computadores:** Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.).
- **Respaldo de información:** Es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Seguridad del sistema:** Conjunto de medidas preventivas y correctivas que permiten resguardar y proteger la información y los sistemas de software que la procesan y almacenan.
- **Servicios:** Conjunto de aplicativos o programas informáticos y de comunicación de datos que apoyan la labor del Secap.
- **Servidor/funcionario:** Persona que presta servicios a la Administración o a nombre y por cuenta de esta, como parte de su organización, en virtud de un acto válido y eficaz de investidura, con entera independencia del carácter imperativo, representativo, remunerado, permanente o público de la actividad respectiva.
- **Sistema de software:** Programas informáticos diseñados con el propósito de facilitar a los usuarios la realización de determinadas tareas.
- **Usuario:** Nombre o identificador compuesto por una cadena de caracteres alfanuméricos, que emplea una persona para identificarse en un sistema, equipo o red, previo a ingresar la contraseña.

6. Políticas

6.1. De los respaldos y copias de seguridad

- La Dirección de Tecnologías de la Información y Comunicación, recibirá periódicamente, por parte de las diferentes áreas del Secap, las necesidades de almacenamiento para determinar la información crítica de la institución que debe ser respaldada y la frecuencia con que se debe realizar.
- La Dirección de Tecnologías de la Información y Comunicación en conjunto con el Oficial de Seguridad de la Información y los propietarios de la información, determinarán los requerimientos para respaldar la información y los datos en función de su criticidad.

- La Dirección de Tecnologías de la Información y Comunicación dispondrá y controlará la ejecución de las copias; así como, las pruebas periódicas de su restauración. Para ello, deberá contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de la institución.
- El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales, teniendo en cuenta los lineamientos de la ley.
- La Dirección de Tecnologías de la Información y Comunicación programará la permanencia de las copias de respaldos, dependiendo de la prioridad de las mismas y de los recursos de almacenamientos que disponga la institución.
- La Dirección de Tecnologías de la Información y Comunicación verificará periódicamente la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.
- La Dirección de Tecnologías de la Información y Comunicación definirá los procedimientos para el respaldo de la información, que incluyan los siguientes parámetros:
  - ✓ Esquema de rotulado de las copias de respaldo, mismo que debe contener toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
  - ✓ Definir un el procedimiento de reemplazo de los medios de almacenamiento discos o cintas de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo a lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.
  - ✓ Almacenar, si los recursos lo permiten, en una ubicación remota o externa, las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.
  - ✓ Para realizar las copias de respaldo en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado por la institución a los que se encuentre sujeta. Se deben asignar los niveles de protección física y

ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

- ✓ Se deben extender los mismos controles de seguridad aplicados a los activos de tecnologías de información en el sitio principal, al sitio alterno.

6.2. Del registro de respaldo de información

- La Dirección de Tecnologías de la Información y Comunicación elaborará un procedimiento formal de administración y control de copias de respaldos, el cual permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.
- La Dirección de Tecnologías de la Información y Comunicación, mediante el Administrador de del Data Center, deberá realizar:
  - ✓ Un registro de los respaldos de información realizada de forma diaria.
  - ✓ Un registro del retiro del respaldo del sitio externo.
  - ✓ Un registro del ingreso del respaldo al sitio externo.
  - ✓ Un inventario de medios magnéticos.
  - ✓ Comprobar de Integridad de la Información
- La Dirección de Tecnologías de la Información y Comunicación probará al menos una vez por año, la información respaldada para asegurar que es confiable, íntegra y que está disponible en el evento que se requiera para su utilización en casos de emergencia.
- La Dirección de Tecnologías de la Información y Comunicación probará al menos una vez al año, los procedimientos de restauración para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.
- La Dirección de Tecnologías de la Información y Comunicación requerirá a las autoridades competentes, los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, para permitir un rápido y eficiente acceso a los medios que contienen la información.
- La Dirección de Tecnologías de la Información y Comunicación, a través del Administrador del Data Center, debe aplicar los siguientes lineamientos:

- ✓ Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los servidores.
- ✓ Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.
- ✓ Validar la integridad y accesibilidad de los medios magnéticos por lo menos cada seis meses.
- ✓ Mantener siempre una copia de la información de los servidores, con una antigüedad no superior a 24 horas.
- ✓ Mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la base de datos, para asegurar la integridad de la información respaldada.
- ✓ Mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad y otros.

6.3. Del respaldo de información para usuarios finales

- Todos los funcionarios y servidores del Secap, son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.
- Toda la información relevante a las funciones del colaborador debe ser almacenada en la aplicación Onedrive, suministrado por la por la institución al momento del ingreso a la misma.
- Los funcionarios y servidores del Secap tienen prohibido realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser considerado como fuga de información.
- Es responsabilidad todos los funcionarios y servidores del Secap que manejan la información crítica asociada con su labor en el servidor de archivos establecido, garantizar que la información está siendo respaldada.

7. Anexos

Controles para revisar el cumplimiento de las políticas de copia de seguridad.

CONTROLES PARA REVISAR EL CUMPLIMIENTO DE LA POLÍTICA DE COPIAS DE SEGURIDAD

Los controles se clasificarán en dos niveles de complejidad:

- Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- DIRECCIONES (DIR): aplica a la dirección o al personal de gestión.
- DIRECCION DE TI (TICS): aplica al personal técnico especializado.
- FUNCIONARIOS (FUN): aplica a todo el personal.

NIVEL		ALCANCE	CONTROL
B	DIR	**INVENTARIO DE ACTIVOS DE INFORMACIÓN** MANTIENES UN INVENTARIO DE ACTIVOS DE INFORMACIÓN (SOFTWARE, DATOS, SOPORTES, RESPONSABLES, UBICACIÓN…) Y LOS CLASIFICAS PARA IDENTIFICAR LOS NECESARIOS (CRÍTICOS) PARA REANUDAR EL NEGOCIO EN CASO DE DESASTRE O INCIDENTE GRAVE.	
B	DIR	**CONTROL DE ACCESO** CONTROLAS EL ACCESO A LAS COPIAS DE SEGURIDAD (SÓLO PERSONAL AUTORIZADO).	
B	DIR/TICS	**COPIAS DE SEGURIDAD DE LA INFORMACIÓN CRÍTICA** HACES COPIAS DE SEGURIDAD DE LA INFORMACIÓN CRÍTICA CORPORATIVA, LA EXIGIDA POR LA LEY Y LA ESTABLECIDA EN LOS CONTRATOS.	
B	DIR/TICS	**PERIODICIDAD DE LAS COPIAS DE SEGURIDAD** LAS COPIAS DE SEGURIDAD SE REALIZAN CADA _____.	
B	DIR/TICS	**TIPO DE COPIA APROPIADA** HACES COPIAS DE SEGURIDAD COMPLETA, INCREMENTAL O DIFERENCIAL (ELEGIR LA ADECUADA PARA TU EMPRESA).	
B	DIR/TICS	**CADUCIDAD DE LAS COPIAS DE SEGURIDAD** CONSERVAS LAS COPIAS DE SEGURIDAD DURANTE _____.	

A	DIR/TICS	**UBICACIÓN DE LAS COPIAS DE SEGURIDAD** GUARDAS AL MENOS UNA COPIA COMPLETA FUERA DE LA ORGANIZACIÓN. GUARDAS LAS COPIAS DE SEGURIDAD EN UNA CAJA IGNÍFUGA Y BAJO LLAVE.	
A	DIR/TICS	**COPIAS EN LA NUBE** TOMAS LAS MEDIDAS DE SEGURIDAD (FIRMAR ANS CON EL PROVEEDOR, CIFRAR LAS COPIAS, COMPROBAR LA CONFIDENCIALIDAD DE LOS CANALES DE TRANSMISIÓN) NECESARIAS SI ALMACENAS TUS COPIAS EN LA NUBE.	
B	DIR/TICS	**PROCEDIMIENTOS DE COPIA Y RESTAURACIÓN** ELABORAS Y APLICAS LOS PROCEDIMIENTOS DE COPIA Y RESTAURACIÓN, REVISÁNDOLOS ANUALMENTE Y CON CADA CAMBIO IMPORTANTE EN LOS ACTIVOS DE INFORMACIÓN.	
B	TICS	**COMPROBAR QUE LAS COPIAS ESTÁN BIEN REALIZADAS Y QUE PUEDEN RESTAURARSE** COMPRUEBAS CADA _____ LA FIABILIDAD DE LAS COPIAS VERIFICANDO QUE PUEDEN RESTAURARSE.	
A	TICS	**SOPORTE DE LAS COPIAS DE SEGURIDAD** ANTES DE HACER LA COPIA REVISAS QUE EL SOPORTE ES EL ADECUADO (TASA DE TRANSFERENCIA, CAPACIDAD, …) Y QUE ESTÁ EN BUEN ESTADO.	
B	TICS	**CONTROL DE LOS SOPORTES DE COPIA** ETIQUETAS LOS SOPORTES PARA REALIZAR LAS COPIAS DE SEGURIDAD Y LLEVAS UN REGISTRO DE LOS SOPORTES SOBRE LOS QUE SE HA REALIZADO ALGUNA COPIA.	
B	TICS	**DESTRUCCIÓN DE SOPORTES DE COPIA** CUANDO SE DESECHAN LOS SOPORTES UTILIZADOS PARA COPIAS DE SEGURIDAD, LOS DESTRUYES DE FORMA SEGURA.	
B	FUN/TICS	**CIFRADO DE LAS COPIAS DE SEGURIDAD** CIFRAS LAS COPIAS DE SEGURIDAD QUE CONTIENEN INFORMACIÓN CONFIDENCIAL Y LA QUE SUBES A LA NUBE.	