POLITICA DE COPIAS DE SEGURIDAD

La Política de Copias de Seguridad establece los principios, procedimientos y responsabilidades para garantizar la integridad, confidencialidad y disponibilidad de la información crítica de la ESE ISABU – Instituto de Salud de Bucaramanga mediante la implementación de medidas de respaldo adecuadas.

1. OBJETIVO

Establecer las pautas y procedimientos específicos para la realización de copias de seguridad, asegurando la protección, integridad y disponibilidad crítica de la información del ESE ISABU – Instituto de Salud de Bucaramanga, con el propósito de garantizar la continuidad operativa, la confidencialidad de los datos, y la rápida recuperación de la información.

2. ALCANCE

Esta política se aplica a todos los sistemas y datos críticos de la ESE ISABU – Instituto de Salud de Bucaramanga administrados por el proceso de Gestión de las TICS.

3. RESPONSABLE

- Líder de sistemas de información
- Líder de infraestructura
- Oficial de seguridad de la información
- Usuarios finales

4. DEFINICIONES

Acuerdo de nivel de servicio (SLA)(ANS): Service Level Agreement (SLA). Un acuerdo entre un proveedor de servicios de Tecnologías de la Información (TI) y un cliente que en este caso será la Oficina de Tecnología e Informática.
Auditoria: La auditoría se refiere a la evaluación sistemática, independiente y documentada para obtener evidencia objetiva y evaluarla de manera imparcial con el fin de determinar en qué medida se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).
Capacidad: El máximo rendimiento que se puede obtener de un Ítem de configuración o Servicio de TI con el objetivo de cumplir los niveles de servicio acordados.
Ciberseguridad: La ciberseguridad se refiere a la protección de los sistemas y datos informáticos contra el acceso no autorizado, el uso malintencionado, la modificación, el robo o la destrucción. La ciberseguridad incluye medidas técnicas, físicas y administrativas para proteger la información. (ISO/IEC 27001:2022).
Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (mintic, s.f.)
Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (mintic, s.f.)
Incidente de seguridad de la información: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.
Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
Información: Datos relacionados que tienen significado para la entidad1. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. (mintic, s.f.)

Riesgos: Los riesgos se refieren a la posibilidad de que ocurra un evento que pueda tener un impacto negativo en un proyecto, una organización o una persona. Los riesgos pueden ser internos o externos, y pueden ser gestionados mediante la identificación, evaluación y mitigación. (ISO/IEC 27001:2022).
Sistema de Información: Conjunto de aplicaciones, servicios, tecnología de información u otros componentes de manejo de información. (ISO/IEC 27001:2022).
Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. (mintic, s.f.)
Id.: Un Id. de usuario es un identificador único de cliente mediante el cual un anunciante elige identificar a un usuario que visita su sitio web. (Ayuda de Google Ads, s.f.)
TI.: El concepto de tecnología de la información refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. (Pérez Porto, 2014).

5. INFORMACION DE USUARIOS DE LA ENTIDAD

- Los líderes de procesos, jefes de dependencias o dueños de la información, serán responsables de identificar y conservar actualizados los activos de información de acuerdo con el GIF-P-007 PROCEDIMIENTO DE IDENTIFICACION, GESTION Y CLASIFICACION DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRITICA DE TI.
- Es fundamental que los líderes de procesos, jefes de dependencias y responsables de la información asuman la responsabilidad de garantizar que la información institucional, especialmente la catalogada como crítica y aquella esencial para la continuidad de los procesos, sea almacenada de forma segura en el OneDrive corporativo bajo el dominio @isabu.gov.co. En este contexto, es esencial garantizar claves seguras para el acceso al repositorio. Cada usuario debe considerar su contraseña como un activo personal e intransferible, con la prohibición explícita de divulgarla a terceros. La seguridad de la información depende en gran medida de la robustez de las claves utilizadas.
- Se establece la política de doble factor de autenticación (DFA) como requisito obligatorio para todos los usuarios que acceden al office 365. La doble autenticación proporciona una capa adicional de seguridad al requerir que los usuarios presenten dos formas de identificación antes de acceder a sus cuentas. Esta medida tiene como objetivo salvaguardar la integridad y confidencialidad de la información crítica almacenada, minimizando el riesgo de accesos no autorizados.
- Los líderes de procesos, jefes de dependencias y responsables de la información deben asegurar que todos los usuarios asociados con la información crítica implementen y mantengan activa la doble autenticación en sus cuentas. Esta política busca proteger la información almacenada contra posibles amenazas de seguridad.
- La Oficina de Gestión de las TIC proporcionará orientación y apoyo en la implementación del proceso de doble factor de autenticación, garantizando una transición fluida y eficiente para todos los usuarios. Además, cualquier pregunta o inquietud sobre la activación o uso del doble factor de autenticación será atendida por el equipo de soporte técnico correspondiente.
- Por ningún motivo se permite alojar en los medios de almacenamiento corporativos como One drive, NAS servidores, entre otros, información catalogada como personal, música, videos, documentos transitorios, y demás que no sea relevante en el cumplimiento de los objetivos de la Entidad.

5.1. DEFINICIÓN DE COPIAS DE SEGURIDAD DE ACTIVOS CRITICOS DE TI

ACTIVO CRITICO	FRECUENCIA DE COPIAS DE SEGURIDAD	TIPO DE RESPALDO	RESPONSABLE	TIEMPO DE RETENCION	FRECUENCIA DE RESTAURACION	ALMACENAMIENTO	
						Interno	Externo
Base de datos PANACEA	Diaria 12:10 am	Full	Líder de sistemas de información	**Interno** NAS HLN: 4 días **Externo** NAS UIMIST: 8 días	Semanal	NAS HLN	NAS UIMIST CLARO CLOUD BACKUP
Máquina virtual Base de datos PANACEA	Dos veces a la semana (lunes y Miércoles 9:00 pm)	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual Directorio activo principal	Semanal Sábado 4:00 am	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual Directorio activo alterno	Semanal Domingo 1:00 am	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual Citas web	Semanal Jueves 7:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Maquina virtual servidor de programas HLN UIMIS	Semanal viernes 8:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Maquina virtual servidor de programas HLN UIMIS	Semanal Miércoles 6:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Maquina virtual Servidor de programas externos	Semanal domingo 7:00 am	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Maquina virtual Acceso usuario panacea local	Semanal Viernes 8:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual Servidor de programas externos 2	Semanal Jueves 8:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual Servidor de reportes	Semanal Lunes 6:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual Programas appl externo	Semanal Lunes 6:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Máquina virtual interfaz laboratorio	Semanal Domingo 10:00 am	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Owncloud	Semanal Sábado 1:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Gestión documental	Semanal Viernes 11:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Capacitaciones	Semanal Martes 11:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--

ACTIVO CRITICO	FRECUENCIA DE COPIAS DE SEGURIDAD	TIPO DE RESPALDO	RESPONSABLE	TIEMPO DE RETENCION	FRECUENCIA DE RESTAURACION	ALMACENAMIENTO	
						Interno	Externo
GLPI	Semanal Sábado 08:00 a m	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
CNT pacientes	Semanal Jueves 08:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Soporte	Semanal Martes 07:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Base de datos panacea pruebas	Semanal Viernes 01:00 am	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--
Acceso a usuarios panacea local alterno	Semanal Miércoles 6:00 pm	Full	Líder de infraestructura	**Interno** NAS HLN: 3 días	--	NAS HLN	--

5.2. DEFINICIÓN DE SNAPSHOT DEL DISPOSITIVO DE ALMACENAMIENTO NAS

El servidor de almacenamiento NAS QNAP está equipado con una funcionalidad de instantáneas que facilita la creación de copias de seguridad de los propios respaldos. Esta característica posibilita la recuperación de archivos en caso de eliminación o corrupción, al proporcionar la opción de restaurar a una versión anterior mediante esta herramienta. La solución permite retener hasta un máximo de 4 instantáneas, ofreciendo así una flexibilidad efectiva en la gestión de versiones y garantizando la integridad de los datos almacenados.

5.3. DEFINICIÓN DE CLARO CLOUD BACKUP

Se dispone de una herramienta de claro respaldo en la nube para realizar copias de seguridad específicamente relacionadas con la base de datos del sistema de información Panacea. Esta herramienta, con sus 14 instancias de retención busca garantizar la preservación integral de los datos críticos de Panacea. Adicionalmente, como parte de su funcionalidad, la herramienta asegura la copia de los datos en un sitio alterno para mitigar el riesgo de pérdida de información debido a amenazas como el secuestro o la encriptación de datos. Esta medida proactiva busca garantizar la continuidad y seguridad de los datos, respaldando eficazmente contra posibles incidentes de ciberseguridad.

5.4. PROTECCIÓN DE LOS MEDIOS DE RESPALDO

Para garantizar la integridad y confidencialidad de las copias de seguridad y mitigar el riesgo de pérdida de información, se han implementado medidas físicas y lógicas. Los medios de respaldo se almacenarán en lugares seguros, de acceso restringido para proteger la información almacenada.

5.5. PRUEBAS Y VALIDACION DE LOS DATOS

Con el objetivo de garantizar la efectividad de nuestras estrategias de copias de seguridad, se llevarán a cabo pruebas periódicas de restauración de la base de datos del sistema de información PANACEA. Estas pruebas proporcionarán la validación necesaria para asegurar que, en caso de necesidad, las copias de seguridad puedan ser recuperadas de manera rápida y eficiente.

5.6. REVISIONES Y ACTUALIZACIONES

Esta política será objeto de revisiones periódicas para asegurar su relevancia y eficacia. El profesional de seguridad de la información coordinará estas revisiones, realizando ajustes según sea necesario para adaptarse a cambios en la infraestructura tecnológica, regulaciones y mejores prácticas de seguridad de la información.

6. REFERENCIAS

-, M. d.-M. (2022). *NTC ISO/IEC 27001:2022 Anexo A GTC ISO/IEC 27002:2022, CONTROLES TECNOLOGICOS 8.13 COPIAS DE SEGURIDAD DE LA INFORMACIÓN*

7. CONTROL DE MODIFICACIONES

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	26/01/2024	Emisión inicial del documento	Ingeniero de seguridad y privacidad de la información – Proceso de gestión de TI
2	04-02-2025	Cambio en la imagen institucional	Oficina de caldiad