EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.

MANUAL DE COPIAS DE SEGURIDAD Y RECUPERACION

HENRY LISCANO PARRA
GERENTE

NOVIEMBRE 2023

TABLA DE CONTENIDO

1. INTRODUCCION

La empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, dentro de sus lineamientos de Sistemas de Información es primordial tener asegurados todos sus datos tanto correspondientes a bases de datos del sistema de información institucional como también tener lineamiento claros acerca de la información operativa de cada usuario o que este pueda tener en sus equipos de trabajo, para así ante cualquier eventualidad se puedan tener respaldos que nos generen el mínimo de inconvenientes operativos ante una restauración.

Una copia de seguridad, copia de respaldo o Backup en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque informático; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.

2. JUSTIFICACION

El componente de copias de seguridad y restauración del motor de base de datos SQL Server ofrece una protección esencial para los datos críticos almacenados en las bases de datos de SQL Server. Para minimizar el riesgo de pérdida de datos catastrófica, debe realizar copias de seguridad de las bases de datos para conservar las modificaciones en los datos de forma periódica. Una estrategia de copias de seguridad y restauración correctamente planeada contribuye a la protección de las bases de datos de la pérdida de datos derivada de daños causados por diferentes errores.

EMPITALITO ESP, dentro de sus lineamientos de Sistemas de Información es primordial tener asegurados todos sus datos tanto correspondientes a bases de datos del sistema de información institucional como también tener lineamientos claros acerca de la información operativa de cada usuario o que este pueda tener en sus equipos de trabajo, para así ante cualquier eventualidad se puedan tener respaldos que nos generen el mínimo de inconvenientes operativos ante una restauración.

3. OBJETIVO

3.1. Objetivo General

Proteger la información crítica de la entidad almacenada en los servidores de: Bases de datos, Archivos, Códigos fuente de las aplicaciones, Configuración de equipos activos y Administración de infraestructura, con el fin que se conserven respaldos que nos permitan asegurar el principio de disponibilidad de la información en la entidad.

3.2. Objetivos Específicos

- Definir las actividades para implementar la estrategia de divulgación y sensibilización en seguridad y privacidad de la información.

- Socializar a todos los usuarios de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP los conceptos en seguridad y privacidad de la información con el fin que sean apropiados por estos, de tal manera que se mitigue la materialización de incidentes de seguridad de la información.

- Establecer lineamientos para el desarrollo del plan de comunicación en seguridad y privacidad de la información.

- Minimizar por medio de respaldos o copias de seguridad de las bases de datos la perdida de información en caso de presentarse algún inconveniente ya sea de tipo catástrofe informática, natural o ataque a estas por personas o software malicioso.

- Establecer el proceso de copias de seguridad de la información, archivos y documentos de cada usuario periódicamente, para su conservación y uso ante cualquier eventualidad que se presente en la institución y/o su equipo de cómputo de trabajo.

- Establecer indicadores para realizar seguimiento y control al proceso de copias de seguridad de las bases de datos de los sistemas de información institucional HAS SQL, Software Comercial 5IINCO, Sistema Gestión Documental ORFEO, Sistema HELP DESK GLPI, entre otros.

4. DEFINICIONES

✓ **Backup (Copia de Respaldo o Seguridad):** Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos extraíbles) con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto. Es conveniente realizar copias de seguridad y verificación de las mismas a intervalos temporales

fijos (diario o semanal, por ejemplo), en función del trabajo y de la importancia de los datos manejados.

Completa	Es la copia completa o "Full copy" que realiza una copia directa de los archivos y directorios. Este proceso puede durar horas dependiendo del tamaño de los archivos o directorios a copiar, por lo que este proceso normalmente se ejecuta la primera vez o cada cierto tiempo. La ventaja derivada de este tipo de copia es que se tiene la seguridad de obtener una imagen completa de los datos.
Incremental	La copia incremental (o diferencial incremental) es la más avanzada al respecto, ya que únicamente copia los ficheros creados o modificados desde el último backup realizado, ya sea de una copia completa o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso de backup. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema. Normalmente las copias diferenciales ocupan más espacio que las incrementales debido a que parten de la base de un único punto fijo en el tiempo (la copia completa inicial).
Diferencial o parcial	La copia diferencial únicamente copia los archivos y directorios que han sido creados y/o modificados desde la última copia completa. Se ejecutará con mayor o menor rapidez en función de la frecuencia con que se realice. La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

- ✓ **Dispositivo de copia de seguridad:** Disco o dispositivo de cinta en el que se escriben las copias de seguridad de SQL Server del que se pueden restaurar.
- ✓ **Base de Datos:** Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.
- ✓ **Hosting:** Alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web.

- ✓ **Log ("registro", en español)**: es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.
- ✓ **Recuperación:** Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.
- ✓ **Repositorio de información:** Un repositorio es un espacio centralizado donde se almacena, organiza, mantiene y difunde información digital, habitualmente archivos informáticos, que pueden contener información importante de una entidad.
- ✓ **Respaldo:** Es la copia de información a un medio del cual se pueda recuperar y restaurar la información original.
- ✓ **Restauración (Restore):** Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otro dispositivo después de un desastre.
- ✓ **Servidor:** Se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.
- ✓ **Sistemas de Información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

5. ALCANCE

El presente documento pretende determinar la manera en que se llevara a cabo el proceso de copias de seguridad de la información de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, tanto para los archivos y documentos de cada usuario como también de las bases de datos de los sistemas de información institucional.

6. DESCRIPCIÓN GENERAL DEL MANUAL

6.1. RESPONSABLES

- **La Oficina TIC:** Como encargados de velar por el cumplimiento de las actividades y normativas del procedimiento.
- **Responsable de la Información**: Verificar la integridad de la información en caso de restauración (Líder de proceso, usuario final, líderes funcionales de los procesos de la entidad).
- Proveedor de servicio contratado por la entidad para el hosting del servicio en la nube.

6.2. GENERALIDADES O POLÍTICAS OPERACIONALES

- ✓ La oficina TIC o de Sistemas de la entidad, debe asegurar la actividad de respaldo de los activos de información mediante la utilización de elementos tecnológicos de almacenamiento externo o interno para la ejecución correcta y segura de las copias de respaldo que sean generadas.

- ✓ Para las solicitudes de copias de respaldo y restauración recibidas por los entes de control, se dará respuesta de este requerimiento a través de los diferentes recursos seguros que permitan compartir la información a restaurar teniendo en cuenta el tamaño de la información.

- ✓ Generar mecanismos para brindar controles de seguridad a la red de EMPITALITO ESP; asi mismo los funcionarios y terceros deben acogerse a los controles de seguridad establecidos para la seguridad de la red.

- ✓ La Oficina TIC definirá los tipos de copia de seguridad que se va a realizar a la información institucional contenida en los servidores de la entidad (recursos compartidos, sistemas de información, bases de datos).

- ✓ Para las solicitudes de copias de respaldo y de restauración de copias debe ser solicitado mediante la herramienta de mesa de servicios GLPI dispuesta para tal fin, indicando solicitud de backup o copia de respaldo.

- ✓ La información que es considerada Pública de acuerdo con la Ley 1712 de 2014 en su artículo 11, cuenta con las medidas de aseguramiento y respaldo de la información que cada funcionario allí deposita, asi como también informes de gestión, evaluación y publicación de datos abiertos entre otros. Por tanto, la Entidad garantiza la disponibilidad de la información allí almacenada publica en su portal web y/o servicio de almacenamiento en nube según sea el caso.

- ✓ En el Servidor de Archivos donde se almacena la información de cada una de las dependencias se tiene control de Modificación/cambios /eliminación.

- ✓ Es deber de los responsables de la información de cada sistema de información verificar la integridad de la información, una vez sea restaurada.

- ✓ Se debe hacer backup de la información contenida en las estaciones de trabajo cuando hay retiro de un funcionario de la Entidad cuando sea necesario, previo a una solicitud generada en la herramienta GLPI por parte del jefe de área al cual corresponde el equipo de cómputo o el que haga de sus veces.

- ✓ Todos los datos almacenados en aquellos equipos de cómputo que sean destinados para baja tecnológica según sea el caso, serán eliminados o borrados de acuerdo con las actividades y herramientas destinadas para tal efecto, donde se asegure los objetivos de seguridad de la información. En este sentido, se deberá tener especial cuidado con respecto a la información almacenada en servidores o estaciones de trabajo, el software licenciado o desarrollado a medida y los elementos que recibirán mantenimiento dentro de la entidad.

- ✓ Para todas las áreas y usuarios internos de EMPITALITO ESP se ha dispuesto un recurso de almacenamiento en red identificado "Backup_(Nombre Usuario)" donde debe reposar toda la información propia de la gestión de cada usuario en la entidad en margen del cumplimiento de sus actividades ejecutadas de conformidad a sus actividades y funciones contratadas.

- ✓ Todos los usuarios deben almacenar la información institucional en la unidad denominada "Backup_(Nombre Usuario)" asociada a la cuenta de usuario del dominio de la Entidad de manera frecuente, a fin de garantizar la salvaguarda de la información institucional que este maneje.

6.3. COPIAS DE SEGURIDAD DE LA INFORMACIÓN

- ➢ **COPIAS DE SEGURIDAD BASES DE DATOS**

La información almacenada en medios magnéticos u ópticos tendrá diversas copias de respaldo en otro medio de que disponga **EMPITALITO ESP**, debido a la importancia de los datos para la toma de decisiones.

MEDIOS DE ALMACENAMIENTO DE LOS BACKUP.

- ✓ Carpeta Backup de cada uno de los servidores donde opera los sistemas de informacion.
- ✓ Servidor Synology NAS.
- ✓ Disco Duro Externo destinado para copias de seguridad.
- ✓ Equipo oficina TIC.
- ✓ Servicio de almacenamiento en la nube (Google Drive).

Las copias de respaldo de los datos son esenciales, como principal mecanismo de seguridad de la información, para facilitar las tareas se deben centralizar las copias de seguridad del servidor, mediante unos horarios determinados. El esquema de copias de seguridad para los sistemas de Información de **EMPITAITO ESP** aplicará así:

Base de datos / Aplicativo	Periodicidad	Tipo de Backup	Hora	Tiempo De Retención	Observaciones
HAS SQL	Diaria	Completa	7:00 P.M	Permanente	Copia diaria, copia de seguridad completa de la base de datos de producción.
Sistema de Gestion Documental – ORFEO	Diaria	Completa	11:00 PM	Permanente	Copia diaria, copia de seguridad completa de la base de datos de producción.
Software Comercial 5IINCO	Mensual	Completa	12:00 P.M	Permanente	El software comercial operado en la entidad es contratado con una empresa externa. La empresa externa lleva un estricto registro y control de los Backup y nos comparte una copia completa de manera mensual.
Sistema de mesa de ayuda – GLPI	Semanal	Completa	Cada Viernes 7:00 pm	Un mes	Copia Semanal, se guarda una copia semanal de los días 1, 8, 15, 22 y 30 o 31 de cada mes.

Las fechas y horas definidas, deben de ser de estricto cumplimiento y reforzarse con otras cuando se presentan cambios generados por el sistema administrativo HAS SQL, por cuadres e informes finales del sistema financiero o por manejo interno de la oficina de Sistemas de Información.

EMPITALITO ESP ubicará mensualmente una de las copias de seguridad completas en una caja fuerte, donde se tenga la custodia de las copias, adicionalmente este proceso también podrá realizarse en la nube, buscando mantener almacenadas por lo menos 3 copias de fecha diferente, esto con el fin de protegerse contra los posibles siniestros que puedan suceder en las Instalaciones de la Empresa.

Se tendrá siempre en cuenta en EMPITALITO ESP los siguientes lineamientos:

- La información debe ser verificada íntegramente, tanto el original como las copias y revisar que la información no esté contaminada con virus informáticos.
- El disco duro es un medio de almacenamiento temporal de la información, el cual debe ser depurado permanentemente de los archivos que no volverán a ser utilizados en forma inmediata.
- Sólo el personal encargado de la elaboración y procesamiento del sistema y el usuario responsable del mismo, podrán acceder y usar la información que está almacenada en los medios magnéticos u ópticos.
- Los medios magnéticos u ópticos (cintas, discos), que contienen a los archivos de información, deben tener etiquetas con su respectivo rótulo donde se especifiquen las características de la informacion salvaguardada, además de la fecha de generación de los mismos.

➢ **COPIAS DE SEGURIDAD DE LA INFORMACIÓN, ARCHIVOS Y DOCUMENTOS DE LOS USUARIOS**

En EMPITALITO ESP, los usuarios son los responsables de hacer periódicamente copias de seguridad de su información, archivos y/o documentos, es importante tener en cuenta que estos podrán tener apoyo del área de Sistemas de Información para el proceso de copias de seguridad siempre que lo solicite, tanto para que el usuario pueda guardar registro de sus archivos en medios extraíbles de su propiedad así como también para que el área de Sistemas de la empresa, guarde un respaldo o copia de estos en discos duros externos, en el servidor Backup Synology NAS o en la Nube (Google DRIVE).

Para el caso de los usuarios de nivel Directivo (Gerente, Directores, Asesores), Lideres de Proceso y Coordinadores, adicional a lo anotado anteriormente, contaran con cuentas corporativas de Gmail, las cuales aparte de ser utilizadas para el servicio de correo electrónico tanto interno como externo, poseen la herramienta Google Drive con una capacidad de 15 Gigas que les permitirá a estos usuarios realizar copias de seguridad en la Nube así como también poder acceder a nuestra información almacenada desde cualquier lugar, esto siempre con los niéveles de acceso y seguridad establecidos por Google.

6.4. DEL ALMACENAMIENTO FISICO

- ➢ Los ambientes donde se depositan los medios magnéticos deben contar con adecuadas condiciones de temperatura y no presentar humedad.
- ➢ Los medios magnéticos en los cuales se almacena la información histórica deben ser completamente nuevos (primer uso), verificándose su buen estado operacional.
- ➢ Los medios magnéticos donde está grabada la información deben recibir mantenimiento de limpieza cada dos meses como mínimo.

- Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios magnéticos almacenados.

6.5. ACCESO A LA INFORMACION

Para acceder continuamente a los datos del Sistema de Información de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, se tienen definidos los siguientes lineamientos:

- En los Sistemas Informáticos se tienen programas de cómputo, que cuentan con rutinas de control para el acceso de los usuarios.
- Las rutinas de control, permiten que los usuarios ingresen al Sistema, previa identificación, mediante una palabra clave (password), la cual será única para cada uno de ellos; negando el acceso a las personas que no han sido definidas como usuarios del Sistema.
- Las rutinas de control de acceso identifican a los usuarios autorizados a usar determinados sistemas con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas.
- Es recomendable que existan 4 niveles de acceso a la información:
    - a) Nivel de consulta de la información no restringida o reservada.
    - b) Nivel de mantenimiento de la información no restringida o reservada
    - c) Nivel de consulta de la información incluyendo la restringida o reservada.
    - d) Nivel de mantenimiento de la información incluyendo la restringida o reservada
- Para garantizar estos niveles cada rol o perfil de usuario tendrá asignada uno de estos niveles de acceso.
- Consecuentemente la información que se considere restringida o reservada estará debidamente identificada, así como a los usuarios que la acceden.
- Cada área maneja los 4 niveles de acceso a la información, contando para ello con un Administrador de la Información, quien es responsable de la asignación de las palabras claves, de los niveles de acceso y las fechas de expiración.
- Para la administración de claves se dispondrá de un procedimiento que posibilite que las palabras claves tengan o se generen bajo un período de tiempo prudencial de vigencia.
- El Jefe de cada área es responsable del acceso a la información y será quien proporcione las directivas adecuadas al Administrador de la Información.
- Los operadores de la información restringida o reservada realizarán estrictamente lo indicado en cada procedimiento establecido de procesamiento de la información, para lo cual éstos deberán estar claramente documentados.

- Los operadores de la información deben mantener su clave en estricta reserva, ésta sólo debe ser conocida individualmente por cada uno de los usuarios y máximo por otra persona más de apoyo a cada proceso en cada una de las áreas, diferente al Administrador del Sistema de cómputo general.

6.6. PROTECCION ESPECIAL DE LA INFORMACION

Se recomienda la adquisición de un software que permita encriptar la información con el fin de obtener mayor protección a la información. Garantizando un límite máximo de instalaciones (licencias autorizadas), para uso.

La protección especial de la información incluye establecer procedimientos adecuados para el control y distribución de la información impresa, así como para la grabación de los medios magnéticos u ópticos y su respectivo almacenamiento.

6.7. INDICADORES

Para realizar seguimiento y control al proceso de copias de seguridad de las bases de datos del sistema de información institucional, se tendrá en cuenta el siguiente indicador:

Porcentaje de copias de seguridad realizadas
Número de Copias de Seguridad realizadas en el mes / Número Total de Copias de Seguridad Programadas en el mes
Estándar: 100%

Este indicador será evaluado mensualmente, y para esto se deben tener en cuenta las copias de seguridad realizadas en la frecuencia semanalmente, es decir, los días 1, 8, 15, 22 y 30 o 31 de cada mes.

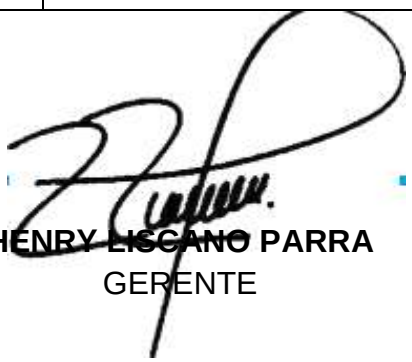
Actividad	Meta	Formula del Indicador	Fuente del indicador	Responsables	Unidad Medida
Realización de las copias de seguridad de las bases de datos de la entidad	100% de las copias de seguridad realizadas	Número de Copias de Seguridad realizadas en el mes / Número Total de Copias de Seguridad Programadas en el mes	Servidores de la entidad	Profesional de Sistemas	Porcentaje

7. CONTROL DE CAMBIOS

VERSIÓN N°.	FECHA DE APROBACIÓN.	DESCRIPCIÓN DEL CAMBIO.
1	30 - 11 - 2023	Se crea el Manual de Copias de Seguridad Y Recuperación

8. APROBACIÓN

	Elaboró	Revisó	Aprobó
Nombre	Jefersson Silva Losada	Mónica Alexandra Lagos	Henry Liscano Parra
Cargo	Profesional de Sistemas	Jefe Oficina de Planeación y Proyectos	Gerente



HENRY LISCANO PARRA
GERENTE