Jar ingeniería diseños estructurales

Plan de copia de seguridad de datos

Farleny Serna Yemail
Liliana Sanmartín
Yennifer Barreneche

Página de control de revisiones

Fecha	Resumen de los cambios realizados	Cambios realizados por (nombre)

Propósito

El propósito de este plan de copia de seguridad de datos es garantizar que Jar Ingeniería Diseños Estructurales pueda realizar copias de seguridad seguras de datos, sistemas, bases de datos y otras tecnologías críticas para asegurar su disponibilidad en caso de interrupciones que afecten las operaciones comerciales. Se espera que todas las ubicaciones de Jar Ingeniería Diseños Estructurales implementen medidas de copia de seguridad de datos para minimizar las interrupciones operativas y recuperarse eficientemente en caso de incidentes.

Este plan abarca las operaciones de copia de seguridad de datos en todas las ubicaciones de Jar Ingeniería Diseños Estructurales.

Alcance

El alcance de este plan se limita a las actividades de copia de seguridad de datos y no constituye un documento de procedimientos de resolución de problemas diarios.

Objetivos del Plan

Servir como guía para los equipos de copia de seguridad de datos de Jar Ingeniería Diseños Estructurales.
Proporcionar referencias y puntos de localización de datos, sistemas, aplicaciones y recursos críticos respaldados.
Suministrar procedimientos y recursos necesarios para ejecutar copias de seguridad de datos, sistemas y otros recursos.
Identificar proveedores y clientes que deben ser notificados en caso de interrupciones que requieran recuperación de datos y recursos respaldados.
Minimizar interrupciones operativas mediante documentación, pruebas y revisión de procedimientos de copia de seguridad.
Identificar fuentes alternativas para actividades de copia de seguridad de datos.
Documentar almacenamiento de datos, copias de seguridad y procedimientos de recuperación de registros vitales y otros datos relevantes.

Suposiciones

Empleados clave del equipo de copia de seguridad de datos de TI estarán disponibles después de un desastre.
Este plan y documentos relacionados se almacenarán en un lugar seguro fuera del sitio y serán accesibles inmediatamente después del desastre.
La organización de TI tendrá planes de recuperación ante desastres alineados con este plan de copia de seguridad de datos.

Definición de Desastre

Se considera un desastre cualquier evento perturbador o catastrófico (como corte de energía, clima extremo, desastre natural, vandalismo) que cause una interrupción en la tecnología relacionada con datos, bases de datos, sistemas y recursos proporcionados por las operaciones de TI de Jar Ingeniería Diseños Estructurales.

Copia de Seguridad de Datos y Equipos Relacionados

Equipo de Copia de Seguridad de Datos.
Equipo de Soporte Técnico de TI.

Responsabilidades de los Miembros del Equipo

Cada miembro del equipo designará un suplente/respaldo.
Mantener listas de contactos actualizadas con números de teléfono de trabajo, hogar y celular de los miembros del equipo.
Mantener el plan como referencia en casa en caso de interrupciones después de horas laborales.
Familiarizarse con el contenido del plan.

Política de Copia de Seguridad

Se realizarán copias de seguridad completas e incrementales para proteger y preservar la información corporativa. Los medios de copia de seguridad se almacenarán en ubicaciones seguras y separadas geográficamente de las originales. Las políticas de retención de datos se establecerán para determinar qué registros deben conservarse y por cuánto tiempo.

Bases de Datos del Sistema

Deben realizarse copias de seguridad de las bases de datos de misión crítica más recientes al menos dos veces al mes, o en función de la frecuencia de los cambios realizados.
Las copias de seguridad deben ser almacenadas fuera del sitio.
El administrador de datos principal es responsable de llevar a cabo esta actividad.

Datos de Misión Crítica

Los datos y bases de datos de misión crítica actuales deben respaldarse de acuerdo con los objetivos de Punto de Recuperación (RPOs) establecidos. Deben reflejarse o replicarse para proteger las ubicaciones de backup dentro de los marcos de tiempo de RPO.
Las copias de seguridad deben almacenarse fuera del sitio en una o más ubicaciones seguras, como en la nube o en centros de datos u oficinas de empresas alternativas, o en una combinación de estas opciones.
El administrador de datos principal es responsable de llevar a cabo esta actividad.

Datos No Críticos de Misión

Los datos y bases de datos actuales que no son de misión crítica deben respaldarse de acuerdo con los RPOs establecidos. Pueden duplicarse o replicarse para proteger las ubicaciones de copia de seguridad dentro de los marcos de tiempo de RPO.
Alternativamente, las copias de los datos y bases de datos actuales deben hacerse al menos dos veces por semana, o en función de las métricas de RPO o la frecuencia de los cambios realizados.
Las copias de seguridad pueden almacenarse en el sitio en instalaciones de almacenamiento seguro, o fuera del sitio en una o más ubicaciones seguras, como en la nube o en centros de datos u oficinas de empresas alternativas, o en una combinación de estas opciones.
El equipo de administración de datos es responsable de llevar a cabo esta actividad.
Los medios de copia de seguridad deben almacenarse en ubicaciones seguras, aisladas de los peligros ambientales y geográficamente separadas de los componentes de la red que albergan la ubicación. Esto asegura la integridad y la disponibilidad de los datos respaldados en caso de incidentes o desastres.

Procedimientos de Almacenamiento Fuera del Sitio

Cintas, discos y otros medios adecuados deben ser almacenados en instalaciones ambientalmente seguras.
La rotación de cintas o discos debe realizarse según una programación regular coordinada con el proveedor de almacenamiento de información.
Se debe probar el acceso a las bases de datos de copia de seguridad y otros datos anualmente.

Cintas

Las cintas con más de tres años de antigüedad deben ser destruidas cada seis meses.
Las cintas con menos de tres años de antigüedad deben almacenarse localmente fuera del sitio.
El supervisor del sistema es responsable del ciclo de transición de las cintas.

Realización de Copias de Seguridad de Datos

Las copias de seguridad de datos deben programarse diaria, semanal y mensualmente, según la naturaleza de la copia de seguridad.
Los administradores de datos deben utilizar tecnología de copia de seguridad de datos aprobada para preparar, programar, ejecutar y verificar las copias de seguridad.
Las copias de seguridad pueden realizarse en recursos de almacenamiento local (como disco, cinta, RAID) en las instalaciones o en ubicaciones seguras fuera del sitio (como proveedores de servicios de copia de seguridad en la nube o proveedores de copia de seguridad como servicio) aprobados por la administración de TI.
Estos procedimientos aseguran que los datos sean respaldados de manera efectiva, que se mantengan en ubicaciones seguras y que se mantenga un ciclo de retención adecuado para las copias de seguridad. Además, la programación regular y las pruebas de acceso garantizan la disponibilidad de los datos de respaldo cuando sea necesario.

Actividades de Copia de Seguridad de Datos

A continuación, se presentan algunas de las actividades de copia de seguridad de datos que deben llevarse a cabo de forma regular:

	Acción	Quién actúa
1.	Revisión del programa con la gestión de TI;aprobaciones seguras según sea necesario	Administrador principal de copia de seguridadde datos, Jefe de Operaciones de TI
2.	Identificar y categorizar los datos de los que serealizará una copia de seguridad	Administrador principal de copias de seguridad; equipo de copia de seguridad
3.	Identificar y categorizar los sistemas de los que serealizará una copia de seguridad	Administrador principal de copias de seguridad; equipo de copia de seguridad
4.	Identificar y categorizar otros recursos para realizaruna copia de seguridad	Administrador principal de copias de seguridad; equipo de copia de seguridad
5.	Programar actividades de copia de seguridad, incluyendo fecha, hora, frecuencia, tipos de recursos y destinos de copias. Programar actividades de copia de seguridad, incluyendo fecha, hora, frecuencia, tipos de recursos y destinos de copias.	Administrador principal de copias de seguridad; equipo de copia de seguridad
6.	Programe sistemas y recursos de respaldo de acuerdocon la programación y la política	Administrador principal de copias de seguridad; equipo de copia de seguridad
7.	Programe actividades de rotación y backup en cinta	Administrador principal de copias de seguridad; equipo de copia de seguridad
8.	Ejecutar copias de seguridad de datos, sistemas y otrosrecursos	Administrador principal de copias de seguridad; equipo de copia de seguridad
9.	Asegúrese de que las cintas estén aseguradas para su recogida y estén debidamente etiquetadas; verificar la recogida	Administrador principal de copias de seguridad; equipo de copia de seguridad
10.	Compruebe que las copias de seguridad se completarony que todos los recursos respaldados no han cambiado	Administrador principal de copias de seguridad; equipo de copia de seguridad
11.	Preparar y distribuir informes de copia de seguridad	Administrador principal de copias de seguridad; equipo de copia de seguridad
12.	Programe y realice pruebas de copias de seguridad de datos	Administrador principal de copias de seguridad; equipo de copia de seguridad
13.	Programe y realice la aplicación de parches de losrecursos de copia de seguridad	Administrador principal de copias de seguridad; equipo de copia de seguridad
14.	Actualice los sistemas y tecnologías de copia deseguridad según sea necesario	Administrador principal de copias de seguridad; equipo de copia de seguridad

Recuperación de Datos

Se establecerán, documentarán y probarán procedimientos periódicos para recuperar datos, bases de datos, sistemas, aplicaciones y otros activos de información en caso de eventos disruptivos que requieran la recuperación de estos activos y recursos.

Revisión y Mantenimiento del Plan

Este plan de copia de seguridad de datos debe ser revisado periódicamente, y los procedimientos deben ser validados y actualizados según sea necesario para garantizar que las copias de seguridad se realicen de manera adecuada y en el momento necesario.
Como parte de esta actividad, es recomendable revisar la lista de personal del equipo de copia de seguridad de datos, así como los proveedores de servicios de copia de seguridad y los proveedores de copia de seguridad en la nube, y actualizar los detalles de contacto según sea necesario.

Almacenamiento de la Versión Impresa del Plan

La versión impresa del plan de copia de seguridad de datos se almacenará en una ubicación común donde el personal de TI, incluidos los administradores de datos, pueda acceder a ella.
Las versiones electrónicas del plan estarán disponibles en el Soporte Técnico de TI.
Estos procedimientos aseguran que el plan de copia de seguridad de datos esté actualizado y sea accesible para el personal relevante, lo que contribuye a la efectividad y la disponibilidad de las medidas de copia de seguridad y recuperación en caso de necesidad.

Apéndice B: Listas de contactos del equipo de copia de seguridad de datos

Equipo de copia de seguridad de datos (DBT)

Nombre	Dirección	Hogar	Teléfono móvil/celular
Farleny Serna Yemail.		Medellín	
Liliana Sanmartín.		Medellín	
Yennifer Barreneche.		Bello	

Equipo de Soporte Técnico de TI (ITS)

Nombre	Dirección	Hogar	Teléfono móvil/celular
Farleny Serna Yemail.		Medellín	
Liliana Sanmartín.		Medellín	
Yennifer Barreneche.		Bello	

Apéndice D: Ubicaciones de copia de seguridad de datos:

Disco c:/Backup/HTM

Nombre de la empresa	Contacto	Trabajo	Teléfono móvil/celular
HTM	Farleny Serna		3002433408
HTM	Liliana Sanmartín		
HTM	Yennifer Barreneche		