<Petitoya>

Plantilla de plan de copia de seguridad de datos



## Página de control de revisiones

| **Fecha** | **Resumen de los cambios realizados** | **Cambios realizados por (nombre)** |
| --- | --- | --- |
| 2024-09-01 | Actualización de datos de contacto para el tipo de almacenamiento en disco. | Johan Vélez |
| 2024-09-02 | Revisión y ajuste del tamaño estimado de la base de datos de clientes. | Juan Suárez |
| 2024-09-03 | Modificación en la frecuencia de respaldo de la base de datos de roles. | Johan Vélez |
| 2024-09-04 | Actualización de la responsable de la base de datos de pedidos a Pedro López. | Juan Suárez |
| 2024-09-05 | Cambios en el contacto para el almacenamiento en la nube y en NAS. | Johan Vélez |
| 2024-09-06 | Ajuste de los tamaños estimados para las bases de datos de productos y pedido\_producto. | Juan Suárez |
| 2024-09-07 | Revisión de la frecuencia de respaldo de los informes de pedidos y carrito. | Johan Vélez |
| 2024-09-08 | Actualización de la persona responsable de la base de datos de historial de cambios. | Juan Suárez |

**Propósito**

El propósito de este plan de copia de seguridad de datos es garantizar que <Client> pueda realizar copias de seguridad de forma segura de datos, sistemas, bases de datos y otras tecnologías de misión crítica para que estén disponibles en caso de una interrupción que afecte las operaciones comerciales. Se espera que todas las <Client>locationes implementen medidas de copia de seguridad de datos siempre que sea posible para minimizar las interrupciones operativas y recuperarse lo más rápido posible cuando ocurra un incidente.

El plan abarca operaciones de copia de seguridad de <Client>data en todas las ubicaciones.

### Alcance

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

### Objetivos del plan

* Sirve como guía para los equipos de copia de seguridad de datos de <Client>IT
* Referencias y puntos a la(s) ubicación(es) de datos, sistemas, aplicaciones y otros recursos de datos de misión crítica respaldados
* Proporciona los procedimientos y recursos necesarios para realizar una copia de seguridad de los datos, sistemas y otros recursos
* Identifica a los proveedores y clientes que deben ser notificados en caso de una interrupción que pueda requerir la recuperación de datos respaldados y otros recursos
* Minimiza las interrupciones operativas al documentar, probar y revisar los procedimientos de copia de seguridad de datos
* Identifica orígenes alternativos para las actividades de copia de seguridad de datos
* Documentos de almacenamiento de datos, copias de seguridad y procedimientos de recuperación de registros vitales y otros datos relevantes

### Suposiciones

* Los empleados clave de copia de seguridad de datos de TI (por ejemplo, administrador principal de copia de seguridad de datos, líderes de equipo, técnicos y suplentes) estarán disponibles después de undesastre.
* Este plan y los documentos relacionados se almacenan en una ubicación segura fuera del sitio y no solo sobrevivieron al desastre, sino que son accesibles inmediatamente después deldesastre.
* La organización de TI tendrá planes de recuperación ante desastres (DR) de tecnología que se alinean con este plan de copia de seguridad dedatos.

### Definición de desastre

Un desastre es cualquier evento perturbador o catastrófico(por ejemplo, corte de energía, clima, desastre natural, vandalismo) que causa una interrupción en la tecnología relacionada con datos, bases de datos, sistemas, datos archivados y otros recursos proporcionados por las operaciones de <Client>IT.

### Copia de seguridad de datos y equipos relacionados

* Equipo de copia de seguridad de datos
* Equipo de soporte técnico de TI

Consulte el Apéndice A para obtener detalles sobre las funciones y responsabilidades de cada equipo.

### Responsabilidades de los miembros del equipo

* Cada miembro del equipo designará unsuplente/respaldo.
* Todos los miembros del equipo deben mantener una lista de llamadas actualizada de los números de teléfono de trabajo, hogar y celular de los miembros del equipo, tanto en casa como en el trabajo.
* Todos los miembros del equipo deben mantener este plan como referencia en casa en caso de que ocurra una interrupción después de las horas normales de trabajo.
* Todos los miembros del equipo deben familiarizarse con el contenido de este plan.

## Política de copia de seguridad

Las copias de seguridad completas e incrementales protegen y preservan la información de la red corporativa y deben realizarse de forma regular para los registros del sistema y los documentos técnicos que no se reemplazan fácilmente, tienen un alto costo de reemplazo o se consideran críticos. Los medios de copia de seguridad deben almacenarse en una ubicación segura y geográficamente separada de la original y aislada de los peligros ambientales. Los componentes de red de respaldo, el cableado y los conectores, las fuentes de alimentación, las piezas de repuesto y la documentación relevante deben almacenarse en un área segura en el sitio, así como en otras ubicaciones corporativas.

Las políticas de retención de datos y documentos se establecen para especificar qué registros deben conservarse y durante cuánto tiempo. Todos los departamentos son responsables de especificar sus requisitos de gestión de datos, retención de datos, destrucción de datos y gestión general de registros.

El soporte técnico de TI sigue estos estándares para la copia de seguridad y el archivado de datos:

## Bases de datos del sistema

* Se debe hacer una copia 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 almacenarsefueradelsitio.
* El administrador de datos principal es responsable de esta actividad.

## Datos de misión crítica

* Los datos y las bases de datos de misión crítica actuales deben respaldarse de acuerdo con los objetivos de puntoderecuperación (RPOs) establecidos, y deben reflejarse o replicarse para proteger las ubicaciones de backup dentro de los marcos de tiempo de RPO.
* Las copias de seguridad deben almacenarsefueradel sitio en una o másubicaciones seguras en la nube o en centros de datos u oficinas de empresas alternativas, o una combinación de estos.
* El administrador de datos principal es responsable de 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 RPOestablecidos, y se pueden duplicar o replicar 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 cambiosrealizados.
* Las copias de seguridad pueden almacenarse enelsitio en instalaciones de almacenamiento seguro, o almacenarse fuera delsitio en una o másubicaciones seguras en la nube o en centros de datos u oficinas de empresas alternativas, o una combinación de estos.
* El equipo de administración de datos es responsable de estaactividad.

Los medios de copia de seguridad se almacenan en ubicaciones seguras, aisladas de los peligros ambientales y geográficamente separadas de los componentes de la red que albergan la ubicación.

## Procedimientos de almacenamiento fuera del sitio

* Las cintas y discos, y otros medios adecuados se almacenan en instalaciones ambientalmenteseguras.
* La rotación de cintas o discos se produce en una programación regular coordinada con el proveedor de almacenamientode información.
* El acceso a las bases de datos de copia de seguridad y otros datos se pruebaanualmente.

## Cintas (si se usan)

* Las cintas de más de tres años de antigüedad se destruyen cada seis meses.
* Las cintas de menos de tres años de antigüedad deben almacenarse localmente fuera delsitio.
* 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 diariamente, semanalmente y mensualmente, dependiendo de la naturaleza de la copia de seguridad. Los administradores de datos deben utilizar la tecnología de copia de seguridad de datos aprobada para preparar, programar, ejecutar y verificar las copias de seguridad. Las copias de seguridad se pueden realizar en recursos de almacenamiento local (por ejemplo, disco, cinta, RAID) localmente o en ubicaciones seguras fuera del sitio (por ejemplo, proveedores de servicios de copia de seguridad de datos en la nube, proveedores de copia de seguridad como servicio) aprobados por la administración de TI.

## Actividades de copia de seguridad de datos

En la tabla siguiente se presentanlas actividades de copia de seguridad de datos que deben realizarse 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 seguridad de datos, Jefe de Operaciones de TI |
| 2. | Identificar y categorizar los datos de los que se realizará una copia de seguridad | Administrador principal de copias de seguridad; equipo de copia de seguridad |
| 3. | Identificar y categorizar los sistemas de los que se realizará una copia de seguridad | Administrador principal de copias de seguridad; equipo de copia de seguridad |
| 4. | Identificar y categorizar otros recursos para realizar una copia de seguridad | Administrador principal de copias de seguridad; equipo de copia de seguridad |
| 5. | Programe actividades de copia de seguridad, por | Administrador principal de copias de |

|  | ejemplo, fecha, hora, frecuencia, tipo de recurso del  que realizar la copia de seguridad, destino de las copias de seguridad | seguridad; equipo de copia de seguridad |
| --- | --- | --- |
| 6. | Programe sistemas y recursos de respaldo de acuerdo con 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 otros recursos | 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 completaron y 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 los recursos de copia de seguridad | Administrador principal de copias de seguridad; equipo de copia de seguridad |
| 14. | Actualice los sistemas y tecnologías de copia de seguridad según sea necesario | Administrador principal de copias de seguridad; equipo de copia de seguridad |
|  |  |  |

***Recuperación de datos***

Se establecerán, documentarán yprobarán periódicamente para recuperar datos, bases de datos, sistemas, aplicaciones y otros activos de información si ocurre un evento disruptivo que requiera la recuperación de esos activos y recursos.

# Revisión y mantenimiento del plan

Este plan de copia de seguridad de datos debe revisarse periódicamente y los procedimientos deben validarse (y actualizarse según sea necesario) para garantizar que las copias de seguridad se realicen según sea necesario y cuando sea necesario. Como parte de esta actividad,es aconsejable revisar la lista de personal del equipo de copia de seguridad de datos, proveedoresde servicios de copia de seguridad de datos y proveedores de copia de seguridad de datos en la nube, y actualizar los detalles de contacto según sea necesario.

La versión impresadel plan de copia de seguridad de datos se almacenará en una ubicación común donde podrá ser vista por el personal de TI, como los administradoresdedatos. Las versiones electrónicas estarán disponibles en el Soporte Técnico de TI.

**Apéndices**

# Apéndice A: Equipos

## Equipo de copia de seguridad de datos

Responsable de la planificación, administración y ejecución general de las actividades de copia de seguridad de datos y de proporcionar informes periódicos a la administración de TI sobre el rendimiento de la copia de seguridad de acuerdo con métricas específicas de copia de seguridad de datos.

## Actividades de apoyo

* Analiza el rendimiento de la copia de seguridadde datos en términos específicos
* Establece prioridades de copia deseguridadbasadas en la colaboración con el soporte técnico de TI

y los departamentos de usuario

* Proporciona a la administración de TI datos continuos de estado y rendimiento
* Trabajar con proveedores y soporte técnico de TI para garantizar el funcionamiento continuo de los backups

**Equipo de soporte técnico de TI (ITS)**

Admite el rendimiento de la copia de seguridad de datos y las actividades de almacenamiento de datos relacionadas

## Actividades de apoyo

* Ayudar con las actividades de copia de seguridad de datos según sea necesario
* Orientación sobreequipos, sistemas y otros servicios, según sea necesario
* Coordinar las pruebas de las operacionesde copia de seguridad de datos para garantizar que lasy funcionen normalmente

# 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** |
| --- | --- | --- | --- |
| Juan David Suarez Zapata | Cra 36c # 93 a 20 | Casa | 3114443434 |
|  |  |  |  |

**Equipo de Soporte Técnico de TI (ITS)**

| **Nombre** | **Dirección** | **Hogar** | **Teléfono móvil/celular** |
| --- | --- | --- | --- |
| Johan Sebastian Velez Ortiz | Cr 34a # 93 a 50 | Casa | 3214140079 |
|  |  |  |  |

# Apéndice C: Lista de contactos de proveedores aprobados

| **Nombre** | **Contacto** | **Correo electrónico** | **Teléfono móvil/celular** |
| --- | --- | --- | --- |
| Proveedor de backup 1 | Juan Suarez | heljapi110@gmmail.com | 3114443434 |
| Proveedor de backup 2 | Johan Velez | johansebastanvekezortiz@gmail.com | 3214140079 |
|  |  |  |  |

***Apéndice D: Ubicaciones de copia de seguridad de datos***

## Recurso de copia de seguridad 1: N°001

Principal: Calle Ficticia 123, Edificio A

Cuarto 5 Madrid, Comunidad de Madrid Contacto: Juan Pérez, (+34) 600 123 456

Alternativa:Avenida Inventada 456, Planta Baja

Cuarto 2 Barcelona, Cataluña

Contacto: María Gómez, (+34) 611 987 654

**Instalaciones de almacenamiento de datos (por ejemplo, cinta, disco, nubes, NAS, SAN, RAID)**

| **Nombre de la empresa** | **Contacto** | **Trabajo** | **Teléfono móvil/celular** |
| --- | --- | --- | --- |
| Almacenamiento en Cinta 1 | Johan Vélez | Gerente de Almacenamiento | 3214140079 |
| Almacenamiento en Disco 2 | Juan Suarez | Coordinadora de Backups | 3114443434 |
| Almacenamiento en la Nube 3 | Johan Vélez | Especialista en Cloud | 3214140079 |
| NAS Almacenamiento 4 | Juan Suarez | Jefa de TI | 3114443434 |
| SAN Almacenamiento 5 | Johan Vélez | Ingeniero de Sistemas | 3214140079 |
| RAID Almacenamiento 6 | Juan Suarez | Administradora de Datos | 3114443434 |

# Apéndice E: Inventario de recursos de datos, bases de datos para respaldar

| ***Nombre de la Tabla*** | ***Descripción*** | ***Tipo*** | ***Frecuencia de Respaldos*** | ***Tamaño Aproximado*** | ***Contacto Responsable*** |
| --- | --- | --- | --- | --- | --- |
| ***clientes*** | *Información de clientes, incluyendo datos de contacto y credenciales.* | *Relacional (MySQL)* | *Diario* | *50 GB* | *Johan Vélez* |
| ***roles*** | *Definición de roles y permisos de usuarios.* | *Relacional (MySQL)* | *Mensual* | *1 GB* | *Juan Suárez* |
| ***pedidos*** | *Datos de pedidos, incluyendo estado, fecha y monto total.* | *Relacional (MySQL)* | *Diario* | *80 GB* | *Johan Vélez* |
| ***productos*** | *Información sobre productos, incluyendo descripciones y precios.* | *Relacional (MySQL)* | *Diario* | *70 GB* | *Johan Vélez* |
| ***pedido\_producto*** | *Relación muchos a muchos entre pedidos y productos.* | *Relacional (MySQL)* | *Diario* | *60 GB* | *Johan Vélez* |
| ***historial\_cambios*** | *Registro de cambios y actualizaciones realizados por los clientes.* | *Relacional (MySQL)* | *Semanal* | *20 GB* | *Juan Suárez* |
| ***informe\_pedidos\_auditoria*** | *Informes generados automáticamente sobre pedidos y productos.* | *Relacional (MySQL)* | *Semanal* | *15 GB* | *Juan Suárez* |
| ***carrito*** | *Información sobre carritos de compras en curso.* | *Relacional (MySQL)* | *Diario* | *10 GB* | *Johan Vélez* |

***Apéndice F:Inventario de hardware y software para respaldar***

| ***Tipo*** | ***Nombre/Descripción*** | ***Ubicación*** | ***Tipo de Respaldo*** | ***Frecuencia de Respaldos*** | ***Contacto Responsable*** |
| --- | --- | --- | --- | --- | --- |
| ***Hardware*** | *Servidor Principal* | *Centro de Datos A* | *Completo y Diferencial* | *Diario (completo semanal)* | *Johan Vélez* |
| ***Hardware*** | *Servidor de Respaldo* | *Centro de Datos B* | *Completo y Diferencial* | *Diario (completo semanal)* | *Johan Vélez* |
| ***Hardware*** | *Estación de Trabajo para Administración* | *Oficina Central* | *Incremental* | *Semanal* | *Johan Vélez* |
| ***Hardware*** | *Estación de Trabajo para Desarrollo* | *Oficina de Desarrollo* | *Incremental* | *Semanal* | *Johan Vélez* |
| ***Software*** | *Sistema de Gestión de Base de Datos (MySQL)* | *Servidor Principal* | *Respaldo Automático* | *Diario* | *Juan Suárez* |
| ***Software*** | *Sistema de Administración de Respaldos (e.g., Veeam)* | *Servidor Principal* | *Respaldo Completo* | *Diario* | *Juan Suárez* |
| ***Software*** | *Herramienta de Monitoreo (e.g., Nagios)* | *Servidor Principal* | *Respaldo Configuraciones* | *Mensual* | *Juan Suárez* |
| ***Software*** | *Sistema Operativo del Servidor (Linux)* | *Servidor Principal* | *Respaldo de Configuración* | *Mensual* | *Juan Suárez* |
| ***Software*** | *Herramienta de Desarrollo (IDE, e.g., Visual Studio)* | *Estaciones de Trabajo* | *Manual* | *Según necesidad* | *Johan Vélez* |
| ***Software*** | *Herramienta de Backup en la Nube (e.g., AWS S3)* | *Nube* | *Respaldo Completo* | *Diario* | *Juan Suárez* |

# Apéndice G: Inventario de servicios de red y equipos para respaldar

| ***Tipo*** | ***Nombre/Descripción*** | ***Ubicación*** | ***Tipo de Respaldo*** | ***Frecuencia de Respaldos*** | ***Contacto Responsable*** |
| --- | --- | --- | --- | --- | --- |
| ***Equipo de Red*** | *Router Principal* | *Centro de Datos A* | *Configuración* | *Mensual* | *Juan Suárez* |
| ***Equipo de Red*** | *Switch Principal* | *Centro de Datos A* | *Configuración* | *Mensual* | *Juan Suárez* |
| ***Equipo de Red*** | *Firewall* | *Centro de Datos A* | *Configuración y Logs* | *Semanal* | *Juan Suárez* |
| ***Equipo de Red*** | *Servidor de Backup de Red* | *Centro de Datos B* | *Completo y Diferencial* | *Diario* | *Johan Vélez* |
| ***Equipo de Red*** | *Estación de Trabajo de Administración de Red* | *Oficina Central* | *Configuración* | *Semanal* | *Johan Vélez* |
| ***Equipo de Red*** | *Estación de Trabajo de Soporte Técnico* | *Oficina de Soporte* | *Configuración* | *Semanal* | *Johan Vélez* |
| ***Servicio de Red*** | *Servicio de DNS* | *Servidor Principal* | *Configuración* | *Mensual* | *Juan Suárez* |
| ***Servicio de Red*** | *Servicio de DHCP* | *Servidor Principal* | *Configuración* | *Mensual* | *Juan Suárez* |
| ***Servicio de Red*** | *Servicio de VPN* | *Servidor Principal* | *Configuración y Logs* | *Mensual* | *Juan Suárez* |
| ***Servicio de Red*** | *Servicio de Correo Electrónico* | *Servidor Principal* | *Configuración y Datos* | *Diario* | *Johan Vélez* |
| ***Servicio de Red*** | *Servicio de Monitoreo de Red (e.g., Nagios)* | *Servidor Principal* | *Configuración y Logs* | *Diario* | *Juan Suárez* |