**Proyecto SIMP**

**Plan de Respaldo de datos**

**Página de control de revisiones**

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Resumen de cambios realizados** | **Cambios realizados por (Nombres y Apellidos)** |
| 02/03/2024 | Creación y modificación inicial y básica del plan de respaldo de S.I.M.P. | Juan Carlos Mican Muñoz |
| 03/03/2024 | Desarrollo del plan | Jhorman Alexander Culma Hermosa |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Tabla de contenidos**

[Propósito 3](#_Toc1072728356)

[Alcance 4](#_Toc1643019439)

[Objetivos del plan 4](#_Toc1364279321)

[Supuestos 4](#_Toc895977561)

[Definición de desastre 4](#_Toc717717196)

[Responsabilidades de los miembros del equipo 5](#_Toc2009126534)

[Política de respaldo 5](#_Toc973911330)

[Bases de datos del sistema 5](#_Toc198714420)

[Datos de misión crítica 5](#_Toc1682539288)

[Datos que no son de misión crítica 6](#_Toc1649695944)

[Procedimientos de almacenamiento fuera del sitio 6](#_Toc1859605127)

[Cintas (si se usan) 6](#_Toc1707619563)

[Realización de copias de seguridad de datos 6](#_Toc845591020)

[Actividades de la copia de seguridad de datos 6](#_Toc860084957)

[Recuperación de datos 7](#_Toc1715088333)

[Revisión y mantenimiento del plan 7](#_Toc1886069021)

[Apéndices 8](#_Toc397776090)

[Apéndice A: Equipos 9](#_Toc531007586)

[Equipo de respaldo de datos 9](#_Toc1715311973)

[Actividades de apoyo 9](#_Toc278725838)

[Equipo de soporte técnico de TI (ITS) 9](#_Toc196554338)

[Actividades de apoyo 9](#_Toc697779939)

[Apéndice B: Listas de contactos del equipo de respaldo de datos 9](#_Toc1625331136)

[Apéndice C: Lista de contactos de proveedores aprobados 10](#_Toc235782124)

[Apéndice D: Ubicaciones de respaldo de datos 11](#_Toc777987149)

[Apéndice E: Inventario de recursos de datos, bases de datos para respaldar 11](#_Toc1262413887)

[Apéndice F: Inventario de hardware y software para realizar copias de seguridad 12](#_Toc741169100)

[Apéndice G: Inventario de equipos y servicios de red para respaldar 12](#_Toc666612405)

# Propósito

El propósito de este plan de respaldo de datos es garantizar que Pizzería ANGUIE pueda respaldar de manera segura datos, sistemas, bases de datos y otra tecnología de misión crítica para que estén disponibles en caso de una interrupción que afecte las operaciones comerciales. Se espera que todas las ubicaciones del Cliente implementen medidas de respaldo de datos siempre que sea posible para minimizar las interrupciones operativas y recuperarse lo más rápido posible cuando ocurre un incidente.

# Alcance

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

# Objetivos del plan

• Sirve como guía para los equipos de respaldo de datos de TI de la Pizzería Anguie.

• Referencias y puntos a la ubicación de los datos, sistemas, aplicaciones y otros recursos de datos de misión crítica respaldados.

• Proporciona procedimientos y recursos necesarios para realizar copias de seguridad de datos, sistemas y otros recursos.

• Identificar 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 respaldo de datos.

• Identifica fuentes alternativas para actividades de respaldo de datos

• Documenta el almacenamiento de datos, las copias de seguridad y los procedimientos de recuperación de registros vitales y otros datos relevantes.

• Minimizar el tiempo de inactividad del sistema Simp en caso de un desastre.

• Asegurar la integridad y disponibilidad de los datos del inventario de materia prima.

• Proteger la inversión realizada en el desarrollo e implementación del sistema Simp.

• Minimizar el riesgo de pérdida de datos debido a desastres o fallos técnicos.

# Supuestos

• Los empleados clave de respaldo de datos de TI (por ejemplo, administrador principal de respaldo de datos, líderes de equipo, técnicos y suplentes) estarán disponibles luego de un desastre.

• Este plan y los documentos relacionados se almacenan en un lugar seguro fuera del sitio y no solo sobrevivieron al desastre, sino que son accesibles inmediatamente después del desastre.

• El equipo de soporte técnico de TI tiene la capacidad y el conocimiento para realizar las tareas de respaldo y recuperación.

• Se cuenta con la infraestructura y recursos necesarios para almacenar las copias de seguridad.

• Los usuarios del sistema Simp comprenden la importancia de la seguridad de los datos y siguen las políticas de respaldo establecidas.

• Acceso a recursos tecnológicos adecuados.

•Disponibilidad de personal capacitado para llevar a cabo las actividades de respaldo.

• Compromiso de cumplir con los estándares y políticas establecidos.

# Definición de desastre

Un desastre es cualquier evento catastrófico o disruptivo (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 TI de Pizzería Anguie.

Copia de seguridad de datos y equipos relacionados

• Equipo de respaldo de datos:

• Responsable de TI: Lidera la implementación y gestión del plan de respaldo.

• Técnico de TI: Realiza las tareas de copia de seguridad y recuperación de datos.

• Usuario Final: Es responsable de realizar copias de seguridad de sus propios archivos de trabajo.

• Equipo de soporte técnico de TI:

• **Soporte de Hardware:** Brinda asistencia en caso de fallos del hardware del servidor.

• **Soporte de Software:** Brinda asistencia en caso de fallos del software del sistema Simp.

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 un suplente.

• Todos los miembros del equipo deben mantener una lista de contactos actualizada de los números de teléfono del trabajo, del hogar y del celular de los miembros del equipo, tanto en el hogar 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 del horario normal de trabajo.

• Todos los miembros del equipo deben familiarizarse con el contenido de este plan.

**• Responsable de TI:**

-Desarrollar y mantener el plan de respaldo.

Coordinar las actividades de respaldo y recuperación.

Informar al equipo sobre las actualizaciones del plan.

**• Técnico de TI:**

-Realizar las copias de seguridad programadas.

-Verificar la integridad de las copias de seguridad.

-Restaurar los datos en caso de un desastre.

**• Usuario Final:**

-Realizar copias de seguridad de sus archivos de trabajo.

-Notificar al equipo de TI sobre cualquier problema con el sistema Simp.

# Política de respaldo

Las copias de seguridad completas e incrementales protegen y preservan la información del cliente y deben realizarse con regularidad 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 respaldo deben almacenarse en un lugar seguro, geográficamente separado del original y aislado de los peligros ambientales.

Las políticas de retención de datos y documentos se establecen para especificar qué registros deben conservarse y durante cuánto tiempo.

Detallar los procedimientos y estándares para la realización de copias de seguridad, incluyendo frecuencia, tipos de datos a respaldar y procedimientos de almacenamiento fuera del sitio.

• Frecuencia: Se realizarán copias de seguridad completas del sistema Simp diariamente.

• Ubicación: Las copias de seguridad se almacenarán en dos ubicaciones diferentes: una local y otra remota.

• Retención: Las copias de seguridad se conservarán durante un período mínimo de 3 meses.

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

# Bases de datos del sistema

• Se debe realizar una copia de las bases de datos de misión crítica más actualizadas al menos 4 veces al mes, o según la frecuencia de los cambios realizados.

• Las copias de seguridad deben almacenarse fuera del sitio.

• El administrador de datos principal es responsable de 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 (RPO) establecidos, y deben reflejarse o replicarse para asegurar ubicaciones de respaldo dentro de los plazos de RPO.

• Las copias de seguridad deben almacenarse fuera del sitio en una o más ubicaciones seguras en la nube o en oficinas o centros de datos alternativos de la empresa, o una combinación de estos.

• El administrador de datos principal es responsable de esta actividad.

# Datos que no son de misión crítica

• Los datos y bases de datos actuales que no son de misión crítica deben respaldarse de acuerdo con los RPO establecidos, y pueden duplicarse o replicarse en ubicaciones seguras de respaldo dentro de los plazos de RPO.

• Alternativamente, se deben realizar copias de los datos y bases de datos actuales al menos dos veces por semana, o según las métricas de RPO o la frecuencia de los cambios realizados.

• Las copias de seguridad se pueden almacenar en el sitio en instalaciones de almacenamiento seguras, o se pueden almacenar fuera del sitio en una o más ubicaciones seguras en la nube o en centros de datos u oficinas alternativos de la empresa, o una combinación de estos.

• El equipo de administración de datos es el responsable de esta actividad.

Los medios de respaldo se almacenan en ubicaciones que son seguras, aisladas de los peligros ambientales y geográficamente separados de la ubicación que alberga los componentes de la red.

# Procedimientos de almacenamiento fuera del sitio

• Las copias de seguridad se transferirán a un dispositivo de almacenamiento externo (por ejemplo, cinta o disco duro) y se almacenarán en una ubicación segura fuera del sitio.

• El dispositivo de almacenamiento externo se mantendrá en un lugar seguro y protegido contra el acceso no autorizado.

# Realización de copias de seguridad de datos

• Bases de datos del sistema.

• Datos de misión crítica.

• Datos que no son de misión crítica.

• Se utilizará una herramienta de software de copia de seguridad para realizar las copias de seguridad del sistema Simp.

• La herramienta de copia de seguridad se configurará para realizar copias de seguridad completas del sistema y de los datos de los usuarios.

• Se verificará la integridad de las copias de seguridad después de cada ejecución.

# Actividades de la copia de seguridad de datos

La siguiente tabla enumera las actividades de respaldo de datos que se realizarán de manera programada regularmente.

|  |  |  |
| --- | --- | --- |
|  | **Acción** | **Responsable(s)** |
| 1. | Identificar y categorizar los datos que se respaldarán. | Administrador de respaldo principal; equipo de respaldo. |
| 2. | Identificar y categorizar otros recursos para respaldar. | Administrador de respaldo principal; equipo de respaldo. |
| 3. | Creación de cronograma con las fechas, hora y recursos a respaldar, destino para respaldos | Administrador de respaldo principal; equipo de respaldo. |
| 4. | Programe los sistemas y recursos de respaldo de acuerdo con el cronograma y la política. | Administrador de respaldo principal; equipo de respaldo. |
| 5. | Ejecute copias de seguridad de datos, sistemas y otros recursos (según cronograma). | Administrador de respaldo principal; equipo de respaldo. |
| 6. | Verifique que las copias de seguridad se hayan completado y que todos los recursos de la copia de seguridad no hayan cambiado. | Administrador de respaldo principal; equipo de respaldo. |
| 7. | Verificación de integridad de las copias de seguridad. | Administrador de respaldo principal; equipo de respaldo. |
| 8. | Programar y realizar pruebas de copias de seguridad de datos. | Administrador de respaldo principal; equipo de respaldo. |

# Recuperación de datos

Se deben establecer, documentar y probar periódicamente procedimientos 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 recomendable revisar las listas del personal del equipo de respaldo de datos, proveedores de servicios de respaldo de datos y proveedores de respaldo de datos en la nube, y actualizar los datos de contacto según sea necesario.

La versión impresa de este plan de respaldo de datos se almacenará en una ubicación común donde el personal de TI, como los administradores de datos, pueda verlo. Las versiones electrónicas estarán disponibles a través del Soporte técnico de TI.

# Apéndices

## Apéndice A: Equipos

### Equipo de respaldo de datos

Responsable de la planificación, gestión 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

### Actividades de apoyo

• Analiza el rendimiento de la copia de seguridad de datos con métricas específicas.

• Establece prioridades de respaldo basadas en la colaboración con el soporte técnico de TI y los departamentos de usuarios.

• Proporciona a la gestión de TI datos de rendimiento y estado continuos

• Trabaja con proveedores y soporte técnico de TI para garantizar el funcionamiento continuo de las copias de seguridad.

### 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

• Proporcionar orientación sobre equipos, sistemas y otros servicios, según sea necesario.

• Coordinar las pruebas de las operaciones de copia de seguridad de datos para garantizar que funcionen con normalidad.

## Apéndice B: Listas de contactos del equipo de respaldo de datos

**Equipo de respaldo de datos (EBD)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Empresa/Nombres y Apellidos** | **Contacto** | **Dirección Domicilio** | **Numero de Celular/Fijo** |
| Juan Carlos Mican Muñoz | 0000000 | 000000 | 0000000 |
| Julian Dario Triana Mozquera | 0000000 | 000000 | 0000000 |
| Jhorman Alexander Culma Hermosa | 0000000 | 00000 | 000000 |
|  |  |  |  |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Empresa /Nombres y Apellidos** | **Contacto** | **Dirección Domicilio** | **Numero de Celular/Fijo** |
| Juan Carlos Mican Muñoz | 0000000 | 000000 | 0000000 |
| Julian Dario Triana Mozquera | 0000000 | 000000 | 0000000 |
| Jhorman Alexander Culma Hermosa | 0000000 | 00000 | 000000 |
|  |  |  |  |

## Apéndice C: Lista de contactos de proveedores aprobados

|  |  |  |  |
| --- | --- | --- | --- |
| **Empresa** | **Contacto (Nombres y Apellidos)** | **Dirección Domicilio** | **Numero de Celular/Fijo** |
| Proveedor de respaldo 1 |  |  |  |
| Proveedor de respaldo 2 |  |  |  |
| Proveedor de respaldo 3 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 

## Apéndice D: Ubicaciones de respaldo de datos

**Recurso de copia de seguridad 1 – <Nombre de la ubicación>**

Primaria: Dirección

Teléfono

Ciudad, Localidad, Estado, Barrio

Nombres y Apellidos de Contacto

Alternativa Dirección

Teléfono

Ciudad, Localidad, Estado, Barrio

Nombres y Apellidos de Contacto

**Recurso de copia de seguridad 2 – <Nombre de la ubicación>**

Primaria: Dirección

Teléfono

Ciudad, Localidad, Estado, Barrio

Nombres y Apellidos de Contacto

Alternativa Dirección

Teléfono

Ciudad, Localidad, Estado, Barrio

Nombres y Apellidos de Contacto

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre de la Empresa** | **Contacto (Nombres y Apellidos)** | **Dirección Domicilio** | **Numero de Celular/Fijo** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

Base de datos simpUv.sql

## Apéndice F: Inventario de hardware y software para realizar copias de seguridad

**Hardware:**

**-Servidores(físico o virtual)**

**- DAS (Direct Attached Storage)**

**- Dispositivos de red (Routers)**

**- Estaciones de trabajo y portatiles**

**- Dispositivos móviles**

**Software:**

**- Sistema Operativo**

**- Bases de datos**

**- Software de virtualización**

**- Servicio de almacenamiento en la nube**

## 

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