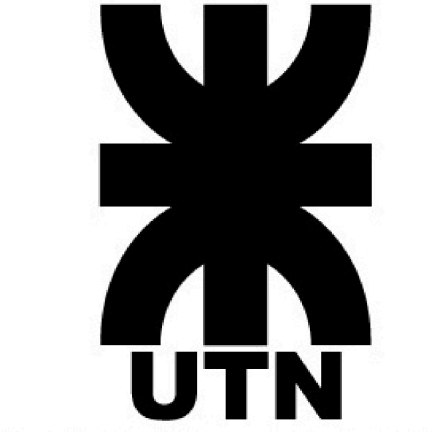
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL RESISTENCIA



Administración de Sistemas de Información
T.P.3.1.: Seguridad de SI

Equipo docente:

- Ing. Soria Ojeda, Claudia
- Ing. Montiel, Raul Alejandro
- Ing. Ramirez, Rosina

Grupo **3** - Integrantes:

- Bianciotto, Joaquín - 27230
- Ferrazzano, Agustín - 27497
- Honnorat, Valentino - 27325
- Kalchichen, Lucas German - 27342
- Lopez Soto, Martin - 27411
- Marain, Yoel Mario - 27314

Año 2025

SUPUESTOS GENERALES:

- *Pensamos que el almacén también es utilizado para la ubicación física de sus servidores.*
- *Pensando que AGUNSA atiende las necesidades de las empresas que buscan el outsourcing de sus procesos de logística, tratamos a los datos de los paquetes como los correspondientes para realizar la distribución (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío), y datos de los clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato) como los correspondientes de las empresas que contratan los servicios de AGUNSA, estas poseen una cuenta corriente y el cobro se realiza a fin de mes, según las entregas que se realizaron.*

Etapa 1: Identificación de riesgos

● Activos Vulnerables

-**Datos e Información del sistema de gestión de almacenes**

- Datos de los Paquetes (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)
- Datos de los Clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato)

-Equipos Informáticos

- Servidores on premise
- Computadora del jefe de almacén.
- Dispositivos de mano (Handheld)

-Software

- Sistema de gestión de almacenes (WMS)

● Vulnerabilidades

- Falta de conocimiento de los empleados sobre posibles ataques informáticos.
- Falta de conocimiento de los empleados sobre manejo de datos.
- Localización física en una ubicación propensa a inundaciones.
- Localización física en una ubicación propensa a hurtos.
- Falta de alarma contra incendios.
- No contar con un antivirus.
- No contar con un mecanismo de seguridad en el almacén.
- No poseer con un suministro de emergencia ante fallos eléctricos.
- No contar con un UPS (estabilizador) en los equipos informáticos.
- Falta de un mecanismo de refrigeración para los equipos.
- Fallos en el diseño de seguridad, errores en el desarrollo de código, configuraciones inseguras y falta de actualizaciones o mantenimiento constante del sistema de gestión de almacenes (WMS).

- Amenazas
    - Incendio en el almacén
    - Inundación en el almacén
    - Sobrecalentamiento de los equipos debido a las altas temperaturas.
    - Baja o alta tensión en la red eléctrica.
    - Corte de suministro en la red eléctrica.
    - Hurto o Robo de equipos informáticos
    - Filtración de datos debido a la apertura de links maliciosos.
    - Borrado accidental de los datos de clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato)
    - Borrado accidental de los datos de paquetes (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)
    - Ataque de Ransomware hacia los datos de los paquetes (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)
    - Ataque de Ransomware hacia los datos de los clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato).
    - Infección de virus en terminales de usuarios
    - Borrado deliberado de los datos de los clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato).
    - Borrado deliberado de los datos de los paquetes(ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)
    - Caída del servidor donde corre el WMS
    - Ataque informático que bloquee el uso del sistema (ransomware)

    - **Clasificación de Amenaza:**

Físicas Accidental	**Físicas Deliberadas**
Incendio en el almacén Inundación en el almacén Sobrecalentamiento de los equipos debido a las altas temperaturas. Baja o alta tensión en la red eléctrica. Corte de suministro en la red eléctrica.	Hurto o Robo de equipos informáticos
Lógicas Accidental	**Lógico Deliberado**
Filtración de datos debido a la apertura de links maliciosos.	Ataque de Ransomware hacia los datos de los paquetes (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)

Borrado accidental de los datos de clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato) Borrado accidental de los datos de paquetes (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío) Caída del servidor donde corre el WMS	Ataque de Ransomware hacia los datos de los clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato) Infección de virus en terminales de usuarios Borrado deliberado de los datos de los clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato). Borrado deliberado de los datos de los paquetes(ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío) Ataque informático que bloquee el uso del sistema (ransomware)

Etapa 2: Análisis del riesgo

Rango de probabilidades elaborado por nosotros	
Baja	0% a 25%
Intermedia	26% a 50%
Alta	51% a 85%
Muy Alta	86% a 100%

Criterio: Probabilidad de agresión se refiere a la probabilidad de que la agresión ocurra en un periodo anual.

Probabilidad de éxito hace referencia a en qué porcentaje afecta la amenaza a mi activo.

Activo: Datos de los paquetes (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)

- El almacén en promedio almacena 500 paquetes
  - El precio promedio es 25.000 usd
- El promedio de precio de los paquetes es 50 USD
- Suponemos que los datos se encuentran impresos en los paquetes.
- Un operario en 8 horas (un día laboral) puede cargar los datos de 17 paquetes almacenados
  - El sueldo del operario es de 250 dólares al mes.
- Se mueve en paquetes 5000 dolares por dia (50 USD x 100 paquetes)
  - 150.000 usd al mes

Amenaza	**Probabilidad de agresión**		**Probabilidad de éxito**		**Frecuencia de pérdida**	**Pérdida Potencial (USD)**	**Pérdida anual esperada (USD)**
Inundación en el almacén	Alta	70%	Muy alta	90%	63%	25000	15750
Incendio en el almacén	Bajo	20%	Muy alta	90%	18%	25000	4500
Ataque de Ransomware hacia los datos de los paquetes	Intermedia	30%	Muy alta	100%	30%	25250	7575

Baja o alta tensión en la red eléctrica.	Muy Alta	100%	Alta	80%	80%	25250	20200
Hurto/Robo de equipos informáticos	Alta	75%	Muy alta	100%	75%	25250	18.937,5
Filtración de datos debido a la apertura de links maliciosos.	Interme dia	50%	Alta	75%	37.5%	540.000	202.500
Borrado deliberado de los datos de los paquetes	Baja	4%	Muy alta	100%	4%	25250	1010
Borrado accidental de los datos de paquetes.	Baja	5%	Muy alta	100%	5%	25250	1.262,5

Formulación de Riesgos

- El riesgo de que se produzca una inundación, debido a que los equipos informáticos se encuentran localizados en zonas propensas a inundaciones y que esto afecta a los datos de los paquetes es de 63% y se generaría una pérdida anual esperada de $15750.
- El riesgo de que se produzca un incendio, debido a la falta de alarmas contra incendios en el almacén y que esto afecta a los datos de los paquetes, es de 18% y se generaría una pérdida anual esperada de $4500.
- El riesgo de que se produzca un ataque de ransomware, debido a la falta de conocimiento de los empleados y que esto afecta a los datos de los paquetes, es de 30% y se generaría una pérdida anual esperada de $7575.
- El riesgo de que se produzca una baja o alta tensión en la red eléctrica, debido a que los equipos informáticos se encuentran localizados en zonas propensas a disturbios en el suministro eléctrico que afectan a los datos de los paquetes, es de 80% y se generaría una pérdida anual esperada de $20200.
- El riesgo de que se produzca un robo de los equipos, debido a la falta de mecanismos de seguridad en el almacén y que esto afecta a los datos de los paquetes, es de 75% y se generaría una pérdida anual esperada de $18937,5.

- El riesgo de que se produzca una filtración de datos por la apertura de links maliciosos provenientes de correos electrónicos, debido a la falta de conocimiento de los empleados sobre manejo de datos que afecta a los datos de los paquetes, es de 37.5% y se generaría una pérdida anual esperada de $202500
- El riesgo de que se produzca un borrado deliberado de los datos de los paquetes, debido a fallos en el diseño de seguridad y controles de acceso y que esto afecta a los datos de los paquetes, es de 4% y se generaría una pérdida anual esperada de $1010.
- El riesgo de que se produzca un borrado accidental de los datos de los paquetes, debido a la falta de conocimiento de los empleados sobre manejo de datos y que esto afecta a los datos de los paquetes, es de 5% y se generaría una pérdida anual esperada de $1262,5.

Consecuencias por Amenaza:

- Inundación en el almacén
  - Primarias
    - ➢ Interrupción del procesamiento a corto plazo, impidiendo la gestión logística de los envíos.
    - ➢ Corrupción de los registros de datos, lo que lleva a información incorrecta sobre la ubicación, el contenido o el estado del envío.
    - ➢ Desaparición de los datos de los paquetes, perdiendo toda la trazabilidad.
  - Secundarias
    - ➢ Retraso en las entregas a los destinatarios finales.
    - ➢ Pérdida de la confianza del cliente que contrató el servicio.
    - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
    - ➢ Impacto económico debido a los costos de recuperación de la información.
- Incendio en el almacén
  - Primarias
    - ➢ Interrupción del procesamiento a corto plazo, impidiendo la gestión logística de los envíos.
    - ➢ Corrupción de los registros de datos, lo que lleva a información incorrecta sobre la ubicación, el contenido o el estado del envío.
    - ➢ Desaparición de los datos de los paquetes, perdiendo toda la trazabilidad.
  - Secundarias
    - ➢ Retraso en las entregas a los destinatarios finales.
    - ➢ Pérdida de la confianza del cliente que contrató el servicio.
    - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
    - ➢ Impacto económico debido a los costos de recuperación de la información.
- Ataque de Ransomware hacia los datos de los paquetes

        - Primarias
            - ➢ Interrupción del procesamiento a corto plazo, impidiendo la gestión logística de los envíos.
            - ➢ Desaparición de los datos de los paquetes, perdiendo toda la trazabilidad.
            - ➢ Revelación de información confidencial del destinatario (nombre, dirección, teléfono) y del contenido del paquete.
        - Secundarias
            - ➢ Retraso en las entregas a los destinatarios finales.
            - ➢ Pérdida de la confianza del cliente que contrató el servicio.
            - ➢ La sede de Barranqueras de Agunsa genera una ganancia de 1.800.000 dólares brutos al año, suponiendo que una filtración de datos afecta a la ventaja competitiva de la empresa, las ganancias se reducen en un 30%.
            - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
            - ➢ Impacto económico debido a los costos de recuperación de la información.
    - Baja o alta tensión en la red eléctrica.
        - Primarias
            - ➢ Interrupción del procesamiento a corto plazo, impidiendo la gestión logística de los envíos.
            - ➢ Corrupción de los registros de datos, lo que lleva a información incorrecta sobre la ubicación, el contenido o el estado del envío.
        - Secundarias
            - ➢ Retraso en las entregas a los destinatarios finales.
            - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
    - Hurto/Robo de equipos informáticos
        - Primarias
            - ➢ Interrupción del procesamiento a corto plazo, impidiendo la gestión logística de los envíos.
            - ➢ Desaparición de los datos de los paquetes, perdiendo toda la trazabilidad.
            - ➢ Revelación de información confidencial del destinatario (nombre, dirección, teléfono) y del contenido del paquete.
        - Secundarias
            - ➢ Retraso en las entregas a los destinatarios finales.
            - ➢ Pérdida de la confianza del cliente que contrató el servicio.
            - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
            - ➢ Impacto económico debido a los costos de recuperación de la información.
    - Filtración de datos debido a la apertura de links maliciosos.
        - Primarias.

        - ➢ Revelación de información confidencial del destinatario (nombre, dirección, teléfono) y del contenido del paquete.
    - Secundarias
        - ➢ Pérdida de la confianza del cliente que contrató el servicio.
        - ➢ La sede de Barranqueras de Agunsa genera una ganancia de 1.800.000 dólares brutos al año, suponiendo que una filtración de datos afecta a la ventaja competitiva de la empresa, las ganancias se reducen en un 30%.
- Borrado deliberado de los datos de los paquetes
    - Primarias
        - ➢ Corrupción de los registros de datos, lo que lleva a información incorrecta sobre la ubicación, el contenido o el estado del envío.
        - ➢ Desaparición de los datos de los paquetes, perdiendo toda la trazabilidad.
    - Secundarias
        - ➢ Retraso en las entregas a los destinatarios finales.
        - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
        - ➢ Impacto económico debido a los costos de recuperación de la información.
- Borrado accidental de los datos de paquetes.
    - Primarias
        - ➢ Corrupción de los registros de datos, lo que lleva a información incorrecta sobre la ubicación, el contenido o el estado del envío.
        - ➢ Desaparición de los datos de los paquetes, perdiendo toda la trazabilidad.
    - Secundarias
        - ➢ Retraso en las entregas a los destinatarios finales.
        - ➢ Incapacidad para continuar con las funciones del sistema que dependen de estos datos.
        - ➢ Impacto económico debido a los costos de recuperación de la información.

Activo: Datos de los clientes (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato).

- Se mueve en paquetes 5000 dolares por dia (50 USD x 100 paquetes)
    - 150.000 usd al mes
    - Suponiendo que se pierden los datos de una semana (los que no estaban en el backup), en un mes se perdería el 25% de los datos si fuera uniforme. Entonces al no poder cobrar esos paquetes se pierde el 25% de la ganancia mensual 37500 usd.
- Se pierden los datos de estado de deuda de la última semana, por lo que la pérdida potencial de perder estos datos es igual a la cantidad de paquetes que se almacenan en promedio.

Amenaza	Probabilidad de agresión		Probabilidad de éxito		Frecuencia de pérdida	Pérdida Potencial (USD)	Pérdida anual esperada (USD)
Inundación en el almacén	Alta	70%	Muy alta	90%	63%	25000	15750
Incendio en el almacén	Baja	20%	Muy alta	90%	18%	25000	4500
Ataque de Ransomware hacia los datos de los clientes	Baja	10%	Muy alta	100%	10%	37500	3750
Filtración de datos debido a la apertura de links maliciosos.	Intermedia	50%	Alta	75%	37.5%	37500	14062,5
Baja o alta tensión en la red eléctrica.	Muy Alta	100%	Alta	80%	80%	37500	30000
Hurto/Robo de equipos informáticos	Baja	5%	Muy alta	100%	75%	37500	28125
Borrado accidental de los datos de los clientes.	Baja	5%	Muy alta	100%	5%	37500	1875
Borrado deliberado de los datos de los clientes.	Baja	4%	Muy alta	100%	4%	37500	1500

Formulación de Riesgos

- El riesgo de que se produzca una inundación, debido a que los equipos informáticos se encuentran en una localización física propensa a inundaciones y que esto afecta a los datos de los clientes, es de 63% y se generaría una pérdida anual esperada de $15750

- El riesgo de que se produzca un incendio, debido a la falta de una alarma contra incendios en el almacén y que esto afecta a los datos de los clientes, es de 18% y se generaría una pérdida anual esperada de $4500.

- El riesgo de que se produzca un ataque de ransomware, debido a la falta de conocimiento de los empleados sobre ataques informáticos y que esto afecta a los datos de los clientes, es de 10% y se generaría una pérdida anual esperada de $3750.

- El riesgo de que se produzca una filtración de datos por apertura de links maliciosos, debido a la falta de conocimiento de los empleados y que esto afecta a los datos de los clientes, es de 37.5% y se generaría una pérdida anual esperada de $14062,5.

- El riesgo de que se produzca una baja o alta tensión en la red eléctrica, debido a que no se cuenta con un UPS para proteger los equipos que alojan los datos de los clientes, es de 80% y se generaría una pérdida anual esperada de $30000.

- El riesgo de que se produzca un robo de los equipos informáticos, debido a la falta de un mecanismo de seguridad en el almacén y que esto afecta a los datos de los clientes, es de 75% y se generaría una pérdida anual esperada de $28125.

- El riesgo de que se produzca un borrado accidental de datos, debido a la falta de conocimiento de los empleados sobre el manejo de datos y que esto afecta a los datos de los clientes, es de 5% y se generaría una pérdida anual esperada de $1875.

- El riesgo de que se produzca un borrado deliberado de datos, debido a fallos en el diseño de seguridad y controles de acceso y que esto afecta a los datos de los clientes, es de 4% y se generaría una pérdida anual esperada de $1500.

Consecuencias por Amenaza:

- Inundación en el almacén
  - **Consecuencias primarias:**
    - ➢ Pérdida o desaparición de datos críticos: La información de los clientes puede perderse total o parcialmente, afectando registros, historiales y transacciones.
    - ➢ Corrupción de datos: Los datos pueden verse dañados o alterados, afectando su integridad y confiabilidad.
    - ➢ Daño a la integridad y disponibilidad del sistema de gestión de datos: Se puede perder la confianza en la plataforma y en la información almacenada.
  - **Consecuencias secundarias**
    - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.
    - ➢ Pérdida de posición competitiva en el mercado

- Incendio en el almacén

- **Consecuencias primarias:**
  - ➢ Pérdida o desaparición de datos críticos: La información de los clientes puede perderse total o parcialmente, afectando registros, historiales y transacciones.
  - ➢ Corrupción de datos: Los datos pueden verse dañados o alterados, afectando su integridad y confiabilidad.
  - ➢ Daño a la integridad y disponibilidad del sistema de gestión de datos: Se puede perder la confianza en la plataforma y en la información almacenada.
- **Consecuencias secundarias**
  - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.
  - ➢ Pérdida de confianza y reputación ante clientes y socios: La exposición o pérdida de datos puede dañar la imagen y credibilidad de la empresa.
  - ➢ Pérdida de posición competitiva en el mercado

- Ataque de Ransomware hacia los datos de los clientes
  - **Consecuencias primarias:**
    - ➢ Pérdida o desaparición de datos críticos: La información de los clientes puede perderse total o parcialmente, afectando registros, historiales y transacciones.
    - ➢ Filtración o exposición de información sensible: La información confidencial puede ser divulgada, afectando la privacidad y cumplimiento normativo.
    - ➢ Daño a la integridad y disponibilidad del sistema de gestión de datos: Se puede perder la confianza en la plataforma y en la información almacenada.
  - **Consecuencias secundarias**
    - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.
    - ➢ Pérdida de confianza y reputación ante clientes y socios: La exposición o pérdida de datos puede dañar la imagen y credibilidad de la empresa.
    - ➢ Sanciones legales y regulatorias: Incumplimiento de normativas de protección de datos.
    - ➢ Pérdida de posición competitiva en el mercado

- Filtración de datos debido a la apertura de links maliciosos.
  - **Consecuencias primarias:**

    - ➢ Filtración o exposición de información sensible: La información confidencial puede ser divulgada, afectando la privacidad y cumplimiento normativo.

  - **Consecuencias secundarias**

        - ➢ Pérdida de confianza y reputación ante clientes y socios: La exposición o pérdida de datos puede dañar la imagen y credibilidad de la empresa.
        - ➢ Sanciones legales y regulatorias: Incumplimiento de normativas de protección de datos.
        - ➢ Pérdida de posición competitiva en el mercado

- Baja o alta tensión en la red eléctrica.
    - **Consecuencias primarias:**
        - ➢ Corrupción de datos: Los datos pueden verse dañados o alterados, afectando su integridad y confiabilidad.
        - ➢ Daño a la integridad y disponibilidad del sistema de gestión de datos: Se puede perder la confianza en la plataforma y en la información almacenada.
    - **Consecuencias secundarias**
        - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.

- Hurto/Robo de equipos informáticos
    - **Consecuencias primarias:**
        - ➢ Pérdida o desaparición de datos críticos: La información de los clientes puede perderse total o parcialmente, afectando registros, historiales y transacciones.
        - ➢ Daño a la integridad y disponibilidad del sistema de gestión de datos: Se puede perder la confianza en la plataforma y en la información almacenada.
    - **Consecuencias secundarias**
        - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.

- Borrado accidental de los datos de los clientes.
    - **Consecuencias primarias:**
        - ➢ Pérdida o desaparición de datos críticos: La información de los clientes puede perderse total o parcialmente, afectando registros, historiales y transacciones.
    - **Consecuencias secundarias**
        - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.
        - ➢ Pérdida de confianza y reputación ante clientes y socios: La exposición o pérdida de datos puede dañar la imagen y credibilidad de la empresa.

- Borrado deliberado de los datos de los clientes.

        - **Consecuencias primarias:**

- ➢ Pérdida o desaparición de datos críticos: La información de los clientes puede perderse total o parcialmente, afectando registros, historiales y transacciones.

- **Consecuencias secundarias**
  - ➢ Retraso en las entregas y operaciones: La falta o corrupción de datos genera demoras en la cadena logística y atención al cliente.
  - ➢ Pérdida de confianza y reputación ante clientes y socios: La exposición o pérdida de datos puede dañar la imagen y credibilidad de la empresa.

Activo: Computadora del jefe de almacén.

- El precio de la computadora del jefe es de 2500 usd

Amenaza	**Probabilidad de agresión**		**Probabilidad de éxito**		**Frecuencia de pérdida**	**Pérdida Potencial (USD)**	**Pérdida anual esperada (USD)**
Inundación en el almacén	Intermedia	30%	Muy alta	90%	27%	2500	675
Incendio en el almacén	Baja	20%	Muy alta	90%	18%	2500	450
Sobrecalentamiento de los equipos debido a las altas temperaturas.	Intermedia	50%	Baja	15%	7,5%	500	37
Baja o alta tensión en la red eléctrica.	Muy Alta	100%	Baja	10%	10%	2500	250
Hurto/Robo de equipos informáticos	Baja	5%	Muy alta	100%	5%	2500	125

Formulación de Riesgos

- El riesgo de que se produzca una inundación, debido a que el equipo está en una localización física propensa a inundaciones y que esto afecta a la computadora del jefe de almacén, es de 27% y se generaría una pérdida anual esperada de $675.

- El riesgo de que se produzca un incendio, debido a la falta de alarma contra incendios en la instalación que afecta a la computadora del jefe de almacén, es de 18% y se generaría una pérdida anual esperada de $450.

- El riesgo de que se produzca un sobrecalentamiento, debido a la falta de un mecanismo de refrigeración y que esto afecta a la computadora del jefe de almacén, es de 7.5% y se generaría una pérdida anual esperada de $37.

- El riesgo de que se produzca una baja o alta tensión en la red eléctrica, debido a la falta de un UPS y que esto afecta a la computadora del jefe de almacén, es de 10% y se generaría una pérdida anual esperada de $250.

- El riesgo de que se produzca un robo del equipo, debido a la falta de un mecanismo de seguridad en el almacén y que esto afecta a la computadora del jefe de almacén, es de 5% y se generaría una pérdida anual esperada de $125.

- **Inundación en el almacén**
    - **Consecuencias primarias**
        - Pérdida o daño del equipo: La computadora puede quedar inutilizable o dañada, afectando la operatividad directa.

    - **Consecuencias secundarias**
        - Retrasos en la gestión y control de inventario: Impacto directo en la operación diaria y en la cadena de suministro.
        - Costos asociados a reparación o reemplazo del equipo: Gastos inesperados por daños o robos.

- **Incendio en el almacén**
    - **Consecuencias primarias**
        - Pérdida o daño del equipo: La computadora puede quedar inutilizable o dañada, afectando la operatividad directa..

    - **Consecuencias secundarias**
        - Retrasos en la gestión y control de inventario: Impacto directo en la operación diaria y en la cadena de suministro.
        - Costos asociados a reparación o reemplazo del equipo: Gastos inesperados por daños o robos.

- **Sobrecalentamiento de los equipos debido a las altas temperaturas.**
    - **Consecuencias primarias**
        - Interrupción del flujo de trabajo: Al no disponer del equipo, se interrumpe la gestión y supervisión del almacén.

    - **Consecuencias secundarias**
        - Pérdida de productividad del jefe de almacén y equipo: Mayor tiempo para tareas administrativas o toma de decisiones.
        - Posible afectación a la toma de decisiones estratégicas del almacén: Al no contar con información oportuna y confiable.

- **Baja o alta tensión en la red eléctrica.**
    - **Consecuencias primarias**
        - Pérdida o daño del equipo: La computadora puede quedar inutilizable o dañada, afectando la operatividad directa.
    - **Consecuencias secundarias**
        - Costos asociados a reparación o reemplazo del equipo: Gastos inesperados por daños o robos.

- **Hurto/Robo de equipos informáticos**

    - **Consecuencias primarias**
        - Pérdida o daño del equipo: La computadora puede quedar inutilizable o dañada, afectando la operatividad directa.
        - Interrupción del flujo de trabajo: Al no disponer del equipo, se interrumpe la gestión y supervisión del almacén.
        - Fallas en la comunicación y acceso a sistemas críticos: Se dificulta la interacción con sistemas de inventario, logística o gestión.

    - **Consecuencias secundarias**
        - Retrasos en la gestión y control de inventario: Impacto directo en la operación diaria y en la cadena de suministro.
        - Pérdida de productividad del jefe de almacén y equipo: Mayor tiempo para tareas administrativas o toma de decisiones.
        - Costos asociados a reparación o reemplazo del equipo: Gastos inesperados por daños o robos.
        - Posible afectación a la toma de decisiones estratégicas del almacén: Al no contar con información oportuna y confiable.

Activo: Servidores on premise

- Cuando las temperaturas del servidor superan cierto umbral se pierde capacidad de procesamiento, incurriendo en una pérdida de 1000 usd
- El precio del servidor es de 10000 usd

Amenaza	**Probabilidad de agresión**		**Probabilidad de éxito**		**Frecuencia de pérdida**	**Pérdida Potencial (USD)**	**Pérdida anual esperada (USD)**
Inundación en el almacén	Intermedia	30%	Muy alta	90%	27%	10800	2916
Incendio en el almacén	Baja	20%	Muy alta	90%	18%	10800	1944
Sobrecalentamiento de los equipos debido	Intermedia	50%	Muy alta	100%	7.5%	1000	75

a las altas temperaturas.							
Baja o alta tensión en la red eléctrica.	Muy Alta	100%	Baja	10%	10%	5500	550
Hurto/Robo de equipos informáticos	Baja	5%	Muy alta	100%	5%	10800	540

Formulación de Riesgos

- El riesgo de que se produzca una inundación, debido a que el equipo está instalado en una localización física propensa a inundaciones y que esto afecta a los servidores on-premise, es de 27% y se generaría una pérdida anual esperada de $2916.

- El riesgo de que se produzca un incendio, debido a la falta de alarma contra incendios en el almacén y que esto afecta a los servidores on-premise, es de 18% y se generaría una pérdida anual esperada de $1944.

- El riesgo de que se produzca un sobrecalentamiento, debido a la falta de un mecanismo de refrigeración adecuado y que esto afecta a los servidores on-premise, es de 7.5% y se generaría una pérdida anual esperada de $75.

- El riesgo de que se produzca una baja o alta tensión en la red eléctrica, debido a la falta de un UPS en los equipos y que esto afecta a los servidores on-premise, es de 10% y se generaría una pérdida anual esperada de $550.

- El riesgo de que se produzca un robo del equipo, debido a la falta de un mecanismo de seguridad física y que esto afecta a los servidores on-premise, es de 5% y se generaría una pérdida anual esperada de $540.

Consecuencias:

- Inundación en el almacén
    - **Consecuencias primarias**
        - Interrupción del servicio y caída del sistema: Detención de operaciones dependientes del servidor.
        - Daño físico a los servidores y hardware asociado: Puede requerir reparaciones o reemplazos costosos.
    - **Consecuencias secundarias**
        - Pérdida de productividad y retrasos operativos: Demoras en procesos internos y atención al cliente.
        - Impacto económico por costos de recuperación, reparación y mitigación: Gastos inesperados para restaurar servicios y equipos.
- Incendio en el almacén
    - **Consecuencias primarias**

        - Interrupción del servicio y caída del sistema: Detención de operaciones dependientes del servidor.
        - Daño físico a los servidores y hardware asociado: Puede requerir reparaciones o reemplazos costosos.
    - **Consecuencias secundarias**
        - Pérdida de productividad y retrasos operativos: Demoras en procesos internos y atención al cliente.
        - Impacto económico por costos de recuperación, reparación y mitigación: Gastos inesperados para restaurar servicios y equipos.
- Sobrecalentamiento de los equipos debido a las altas temperaturas.
    - **Consecuencias primarias**
        - Interrupción del servicio y caída del sistema: Detención de operaciones dependientes del servidor.
        - Daño físico a los servidores y hardware asociado: Puede requerir reparaciones o reemplazos costosos.
    - **Consecuencias secundarias**
        - Pérdida de productividad y retrasos operativos: Demoras en procesos internos y atención al cliente.
        - Impacto económico por costos de recuperación, reparación y mitigación: Gastos inesperados para restaurar servicios y equipos.
- Baja o alta tensión en la red eléctrica.
    - **Consecuencias primarias**
        - Interrupción del servicio y caída del sistema: Detención de operaciones dependientes del servidor.
        - Daño físico a los servidores y hardware asociado: Puede requerir reparaciones o reemplazos costosos.
    - **Consecuencias secundarias**
        - Pérdida de productividad y retrasos operativos: Demoras en procesos internos y atención al cliente.
        - Impacto económico por costos de recuperación, reparación y mitigación: Gastos inesperados para restaurar servicios y equipos..
- Hurto/Robo de equipos informáticos
    - **Consecuencias primarias**
        - Interrupción del servicio y caída del sistema: Detención de operaciones dependientes del servidor.
        - Daño físico a los servidores y hardware asociado: Puede requerir reparaciones o reemplazos costosos.
    - **Consecuencias secundarias**
        - Pérdida de productividad y retrasos operativos: Demoras en procesos internos y atención al cliente.
        - Impacto económico por costos de recuperación, reparación y mitigación: Gastos inesperados para restaurar servicios y equipos.
        - Pérdida de confianza de clientes y socios por fallas en el servicio: Afecta la reputación y relaciones comerciales.

Activo: Dispositivos de mano (Handheld)

- Cada dispositivo vale 100 USD

- Hay 20 dispositivos en el almacén
- *Nota: Al ser hardware la pérdida potencial es la misma para cada amenaza*

Amenaza	**Probabilidad de agresión**		**Probabilidad de éxito**		**Frecuencia de pérdida**	**Pérdida Potencial (USD)**	**Pérdida anual esperada (USD)**
Inundación en el almacén	Intermedia	30%	Baja	5%	1.5%	2000	30
Incendio en el almacén	Baja	20%	muy alta	90%	18%	2000	360
Hurto/Robo de equipos informáticos	Alta	100%	Alta	100%	100%	2000	2000

Formulación de Riesgos

- El riesgo de que se produzca una inundación, debido a que los equipos se guardan en una locación propensa a inundaciones y que esto afecta a los dispositivos de mano, es de 1.5% y se generaría una pérdida anual esperada de $30.

- El riesgo de que se produzca un incendio en el almacén, debido a la ausencia de alarmas contra incendios y que esto afecta a los dispositivos de mano, es de 18% y se generaría una pérdida anual esperada de $360.

- El riesgo de que se produzca un robo, debido a la falta de mecanismos de seguridad física en el almacén y que esto afecta a los dispositivos de mano, es de 100% y se generaría una pérdida anual esperada de $600.

Consecuencias:

- **Inundación en el almacén**
  - **Consecuencias primarias**
    - Daño físico a los dispositivos: Por inundación los dispositivos pueden quedar inutilizables o requerir reparaciones.
    - Interrupción en la operatividad diaria: Sin estos dispositivos, los procesos que dependen de ellos se detienen o ralentizan.
  - **Consecuencias secundarias**
    - Costos adicionales por reparación o reemplazo de equipos: Gastos imprevistos que afectan el presupuesto.

- **Incendio en el almacén**
  - **Consecuencias primarias**
    - Daño físico a los dispositivos: Por incendio, sobrecalentamiento,los dispositivos pueden quedar inutilizables o requerir reparaciones.
    - Pérdida de dispositivos: daños irreparables implican pérdida total del activo.

        - Interrupción en la operatividad diaria: Sin estos dispositivos, los procesos que dependen de ellos se detienen o ralentizan.
    - **Consecuencias secundarias**
        - Retrasos en la gestión y operaciones del almacén: Impacta directamente en la productividad y eficiencia.
        - Costos adicionales por reparación o reemplazo de equipos: Gastos imprevistos que afectan el presupuesto.
        - Riesgo de errores o falta de información actualizada: Al no contar con dispositivos, la captura y actualización de datos puede fallar.
        - Pérdida de confianza interna en los sistemas y procesos: Puede generar frustración y desmotivación en el equipo.

- **Hurto/Robo de equipos informáticos**
    - **Consecuencias primarias**
        - Pérdida de dispositivos: Robo o daños irreparables implican pérdida total del activo.
        - Interrupción en la operatividad diaria: Sin estos dispositivos, los procesos que dependen de ellos se detienen o ralentizan.
    - **Consecuencias secundarias**
        - Retrasos en la gestión y operaciones del almacén: Impacta directamente en la productividad y eficiencia.
        - Costos adicionales por reparación o reemplazo de equipos: Gastos imprevistos que afectan el presupuesto
        - Riesgo de errores o falta de información actualizada: Al no contar con dispositivos, la captura y actualización de datos puede fallar.
        - Pérdida de confianza interna en los sistemas y procesos: Puede generar frustración y desmotivación en el equipo.

Activo: Sistema de gestión de almacenes (WMS)

- Medio día sin procesamiento debido al virus.
- Se supone que se cae el servidor por 1 día.
- Al ser una empresa con múltiples sucursales, se cuenta con diferentes versiones del sistema, por ello el tiempo que se tarda en realizar la nueva instalación no se podrá operar, suponemos que son 3 días.
- Se supone un corte de energía de medio día.

Amenaza	**Probabilidad de agresión**		**Probabilidad de éxito**		**Frecuencia de pérdida**	**Pérdida Potencial (USD)**	**Pérdida anual esperada (USD)**
Infeccion de virus en terminales de usuarios	Intermedia	30%	Baja	20%	6%	2500	150

Caída del servidor donde corre el WMS	Alta	70%	Muy alta	90%	63%	5000	3150
Ataque informático que bloquee el uso del sistema (ransomware).	Baja	20%	muy alta	100%	20%	15000	3000
Corte de suministro de la energía eléctrica	Muy alta	100%	Muy alta	100%	100%	2500	2500

Formulación de Riesgos

- El riesgo de que se produzca una infección de virus en las terminales de los usuarios, debido a no contar con antivirus en las terminales o al desconocimiento del personal y que esto afecta al sistema de gestión de almacenes (WMS), es de 6% y se generaría una pérdida anual esperada de $150.

- El riesgo de que se produzca una interrupción del servidor, debido a fallas en el mantenimiento del sistema y que esto afecta al sistema de gestión de almacenes (WMS), es de 63% y se generaría una pérdida anual esperada de $3150.

- El riesgo de que se produzca un ataque informático como ransomware, debido a fallos en el diseño de seguridad, errores en el desarrollo de código, configuraciones inseguras y falta de actualizaciones o mantenimiento, y que esto afecta al sistema de gestión de almacenes (WMS), es de 20% y se generaría una pérdida anual esperada de $3000.

- El riesgo de que se produzca un corte de suministro de energía eléctrica, debido a la falta de equipos de respaldo como UPS o generadores y que esto afecta al sistema de gestión de almacenes (WMS), es de 100% y se generaría una pérdida anual esperada de $2500.

Consecuencias:

- **Infeccion de virus en terminales de usuarios**
  - **Consecuencias primarias**
    - Interrupción del funcionamiento del WMS: Paradas o caídas del sistema que impiden la gestión normal del almacén.
    - Pérdida o corrupción de datos críticos: Información de inventarios, pedidos y movimientos puede perderse o dañarse.
    - Impacto en la disponibilidad y confiabilidad del sistema: El sistema deja de estar operativo o presenta errores constantes.
    - Nuevas tareas para el personal, que debe restablecer la aplicación.
  - **Consecuencias secundarias**

        - Retrasos en la preparación, despacho y entrega de pedidos: Se generan demoras que afectan la cadena logística y satisfacción del cliente.
        - Aumento de costos operativos: Por necesidad de trabajos manuales, correcciones y soporte técnico adicional.
        - Pérdida de confianza de clientes y usuarios internos: Se deteriora la percepción de la empresa y de sus procesos tecnológicos.
        - Posibles incumplimientos legales o contractuales: Por fallas en tiempos de entrega o manejo inadecuado de inventarios.

- **Caída del servidor donde corre el WMS**
    - **Consecuencias primarias**
        - Interrupción del funcionamiento del WMS: Paradas o caídas del sistema que impiden la gestión normal del almacén.
        - Nuevas tareas para el personal, que debe restablecer la aplicación.
    - **Consecuencias secundarias**
        - Retrasos en la preparación, despacho y entrega de pedidos: Se generan demoras que afectan la cadena logística y satisfacción del cliente.
        - Aumento de costos operativos: Por necesidad de trabajos manuales, correcciones y soporte técnico adicional.
        - Posibles incumplimientos legales o contractuales: Por fallas en tiempos de entrega o manejo inadecuado de inventarios.

- **Ataque informático que bloquee el uso del sistema**
    - **Consecuencias primarias**
        - Interrupción del funcionamiento del WMS: Paradas o caídas del sistema que impiden la gestión normal del almacén.
        - Impacto en la disponibilidad y confiabilidad del sistema: El sistema deja de estar operativo o presenta errores constantes.
        - Nuevas tareas para el personal, que debe restablecer la aplicación.
    - **Consecuencias secundarias**

        - Retrasos en la preparación, despacho y entrega de pedidos: Se generan demoras que afectan la cadena logística y satisfacción del cliente.
        - Aumento de costos operativos: Por necesidad de trabajos manuales, correcciones y soporte técnico adicional.
        - Pérdida de confianza de clientes y usuarios internos: Se deteriora la percepción de la empresa y de sus procesos tecnológicos.
        - Posibles incumplimientos legales o contractuales: Por fallas en tiempos de entrega o manejo inadecuado de inventarios.

- **Ransomware.**
    - **Consecuencias primarias**
        - Interrupción del funcionamiento del WMS: Paradas o caídas del sistema que impiden la gestión normal del almacén.

        - Pérdida o corrupción de datos críticos: Información de inventarios, pedidos y movimientos puede perderse o dañarse.
        - Impacto en la disponibilidad y confiabilidad del sistema: El sistema deja de estar operativo o presenta errores constantes.
        - Nuevas tareas para el personal, que debe restablecer la aplicación.
    - **Consecuencias secundarias**
        - Retrasos en la preparación, despacho y entrega de pedidos: Se generan demoras que afectan la cadena logística y satisfacción del cliente.
        - Aumento de costos operativos: Por necesidad de trabajos manuales, correcciones y soporte técnico adicional.
        - Pérdida de confianza de clientes y usuarios internos: Se deteriora la percepción de la empresa y de sus procesos tecnológicos.
        - Posibles incumplimientos legales o contractuales: Por fallas en tiempos de entrega o manejo inadecuado de inventarios.

- **Corte de suministro de la energía eléctrica**
    - **Consecuencias primarias**
        - Interrupción del funcionamiento del WMS: Paradas o caídas del sistema que impiden la gestión normal del almacén.
        - Impacto en la disponibilidad y confiabilidad del sistema: El sistema deja de estar operativo o presenta errores constantes.
        - Nuevas tareas para el personal, que debe restablecer la aplicación.
    - **Consecuencias secundarias**
        - Retrasos en la preparación, despacho y entrega de pedidos: Se generan demoras que afectan la cadena logística y satisfacción del cliente.
        - Aumento de costos operativos: Por necesidad de trabajos manuales, correcciones y soporte técnico adicional..
        - Posibles incumplimientos legales o contractuales: Por fallas en tiempos de entrega o manejo inadecuado de inventarios.

Etapa 3: Manejo del riesgo

Activos	Amenazas	Estrategia genérica	Contramedida		
			Prevención	Detección	Recuperación
Equipos Informáticos			- Cerrado hermético de las uniones (PR - RR) - Labores de Mantenimiento	- Sistema de detección de humedad	- Seguros contra inundaciones. - Bomba de Achique.

Datos e Información del sistema de gestión de almacenes	Inundación en el almacén	Transferir el riesgo	(mantener limpio los desagües)		-Restauración desde backup
- Datos e Información del sistema de gestión de almacenes. - Equipos Informáticos	Incendio en el almacén	Transferir el riesgo.		- Detector de Humo -Alarma contra incendios	- Matafuegos - Seguro contra incendios
- Equipos Informáticos	Sobrecalentamiento de los equipos debido a las altas temperaturas.	Asumir el riesgo.			- Contar con repuestos de componentes de computación.
- Datos e información del sistema de gestión de almacenes	Ataque de Ransomware hacia los datos de los paquetes y clientes	Prevenir el riesgo.	-Capacitación en ciberseguridad -Herramientas de seguridad	-Análisis de tráfico inusual	-Restauración desde backups
- Datos e información del sistema de gestión de almacenes	Filtración de datos debido a la apertura de links maliciosos.	Prevenir el riesgo.	-Capacitación en ciberseguridad -Bloqueo de adjuntos sospechoso. -Herramientas de seguridad -Sanciones al empleado		
Equipos informáticos Sistema de gestión de almacenes	Corte de suministro de la energía eléctrica.	Reducir el riesgo.	-Estabilizadores de tensión (UPS) -Monitorización de fuentes de energía.		- Instalación de generadores electricos (RR)
Equipos Informáticos			- Contracción de seguridad privada (PR)	- Sistema de	- Asegurar los elementos afectados (TR)

Datos e Información del sistema de gestión de almacenes	Robo o hurto de los equipos	Prevenir el riesgo.	- Instalar cámaras de seguridad (PR)	alarmas (RR)	-Restauración desde Backup
Equipos Informáticos	Baja o alta tensión en la red eléctrica.	Reducir el riesgo.	-Estabilizadores de tensión (UPS).	-Sistema de medición de niveles de tensión.	
Datos e Información del sistema de gestión de almacenes	Borrado accidental de los datos de paquetes y de los clientes.	Prevenir el riesgo.	-Realizar capacitaciones a los empleados sobre manejo de datos. - Controles de Permisos de Edición -Sanciones económicas a los empleados culpables.	-Gestión de logs de los cambios en la base de datos.	-Restauración desde Backup
Sistema de gestión de almacenes	Infección de virus en terminales de usuarios	Prevenir el riesgo.	- Antivirus. -Herramientas de seguridad	-Análisis y escaneo de virus	-Restauración desde Backup
Datos e Información del sistema de gestión de almacenes	Borrado deliberado de datos de los clientes y paquetes.	Reducir el riesgo	-Controles de Permisos de Edición.	-Gestión de logs de los cambios en la base de datos.	-Restauración desde Backup
Sistema de gestión de almacenes	Ataque informático que bloquee el uso del sistema (ransomware)	Prevenir el riesgo	-Realizar mantenimiento y actualizaciones constantes. -Herramientas de seguridad		
Sistema de gestión de almacenes	Caída del servidor donde corre el WMS	Prevenir el riesgo	-Mantener el hardware y software actualizados	-Controlar el rendimiento del servidor y la utilización de	

				recursos.	

Nota: Dado que los datos están en la misma bbdd las medidas y estrategia elegida es la misma para todos los datos.

Políticas

Políticas Generales (a nivel organización)

- **Permisiva**
    - **Política 1:** Se prohíbe eludir, desactivar o alterar las configuraciones de los controles técnicos de seguridad implementados en los sistemas y redes de la organización.
        - **Línea de actuación:** Gestión de Comunicaciones y Operaciones.
    - **Política 2:** Se prohíbe compartir las credenciales de acceso personales (usuario y contraseña) con cualquier otro individuo, sea interno o externo a la empresa.
        - **Línea de actuación:** Seguridad del Personal.
    - **Política 3:** Se prohíbe el uso de todos los activos de información de la empresa (hardware, software, datos) para otras actividades que no estén relacionadas al cumplimiento de las responsabilidades laborales asignadas, siguiendo los procedimientos establecidos.
        - **Línea de actuación:** Clasificación y control de activos.
    - **Política 4:** Se prohíbe el manejo de información clasificada como "Confidencial" o "Restringida" en equipos personales o en servicios en la nube no autorizados por la organización.
        - **Línea de actuación:** Clasificación y Control de Activos.
- **Prohibitiva**
    - **Política 1:** Se permite acceder a sistemas para los cuales se ha otorgado un permiso explícito y documentado.
        - **Línea de actuación:** Control de Acceso.
    - **Política 2:** Se permite el uso de los dispositivos de mano solo a los operarios
        - Clasificación y control de activos.

Políticas Específicas

- **Permisivas**
    - **Política 1: Se prohíbe estrictamente hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos desconocidos para prevenir infecciones por malware.**
    - **Política 2:** Se prohíbe dejar equipos informáticos móviles desatendidos en áreas de acceso público o no seguras dentro o fuera de las instalaciones.
    - **Política 3:** Se prohíbe realizar modificaciones masivas o eliminaciones de datos en el sistema WMS sin una autorización previa y una copia de seguridad verificada.

    - **Política 4:** Se prohíbe la omisión de los ciclos de mantenimiento preventivo y la no aplicación de parches de seguridad críticos en los servidores y el software del WMS.
- **Prohibitivas**
    - **Política 1:** Se permite solicitar la verificación de un correo electrónico al departamento de TI antes de interactuar con su contenido si existe la más mínima duda sobre su legitimidad.
    - **Política 2:** Se permite el traslado de equipos fuera de las instalaciones para fines laborales, siempre que se cuente con una autorización formal y se utilicen los medios de protección adecuados (fundas, maletines de seguridad).
    - **Política 3:** Se permite que los usuarios autorizados realicen las gestiones de datos necesarias para su rol, exclusivamente a través de la interfaz del WMS que registra todas las transacciones para su posible auditoría o restauración.
    - **Política 4:** Se permite la solicitud de ventanas de mantenimiento extraordinarias si se detecta una falla o vulnerabilidad que ponga en riesgo la estabilidad y seguridad del sistema, previa coordinación con los responsables de la operación

Etapa 4: Recuperación ante el desastre

Plan de contingencias

El siguiente plan de contingencias está orientado a un desastre de **inundación**.

El plan de contingencias contendrá lo siguiente**:**

- **Definir los responsables y roles que van a tener cada una de las personas ante la situación**

1. Alta Gerencia
    - Responsable: Director General o Junta Directiva.
    - Rol: Autoridad y Aprobación.
    - Responsabilidades:
        - Declarar oficialmente la situación de desastre e iniciar la activación del plan de contingencia.
        - Autorizar la contratación y activación del Hot Site con el proveedor externo, liberando los fondos necesarios.

2. Comité de Recuperación de Desastres
    - Formado por: el Jefe de TI, Gerente de Operaciones, Jefe de Almacén.
    - Rol: Liderazgo y Gestión del Plan. Es el responsable de orquestar toda la operación de recuperación.
    - Responsabilidades:
        - Supervisar la ejecución del plan de recuperación.
        - Coordinar con el proveedor externo del Hot Site para asegurar que las condiciones de activación se cumplan.
        - Declarar la finalización exitosa de la recuperación y el retorno a las operaciones normales.

3. Equipo Técnico
   - Responsable: Personal de Sistemas
   - Rol: Ejecución Técnica. Son los responsables de la restauración de la infraestructura tecnológica.
   - Responsabilidades:
     - Llevar a cabo el plan de recuperación.
     - Informar al Jefe de TI sobre las eventualidades del proceso
     - Declarar la finalización exitosa de cada paso.

4. Personal de Almacén y Operaciones
   - Responsable: Empleados operativos.
   - Rol: Ejecución de Tareas Dirigidas.
   - Responsabilidades:
     - Llevar a cabo el plan de recuperación
     - Reportar cualquier anomalía o error al Jefe de Almacén inmediatamente.
     - Declarar la finalización exitosa de cada paso.

- **Determinación del orden de prioridades en materia de recuperación de aplicaciones, software de base y archivos de datos según el grado de tolerancia con respecto a la interrupción.**

Criterio de Prioridad elaborado por nosotros	
1 - Crítico	Activos cuya pérdida detiene completamente las operaciones. Su ausencia afecta funciones esenciales y no hay métodos alternativos viables.
2 - Vital	Activos importantes que, si bien afectan la operación, pueden ser sostenidos por un corto plazo con soluciones temporales
3 - Sensible	Activos que pueden mantenerse en funcionamiento mediante procedimientos manuales o alternativos, aunque con menor eficiencia.
4- No crítico	Activos cuyo uso puede suspenderse temporalmente sin comprometer la operación. Pueden recuperarse al final del proceso.

Prioridad	Activo	Justificación
1 – Crítico	**Sistema de Gestión de Almacenes (WMS)**	Es el núcleo crítico del negocio logístico. Su caída detiene toda operación de recepción, almacenamiento y despacho. No existe alternativa manual sostenible.
1 - Crítico	**Datos de los Clientes** (identificación de la empresa, deuda, cantidad de paquetes, detalles del contrato)	Afecta gravemente ya que estos datos incluyen el estado de deuda de cada cliente y los paquetes asociados a cada uno.
1 - Crítico	**Servidores on premise**	Infraestructura que soporta el sistema y sus bases de datos. Si no están operativos, el sistema no puede levantarse ni ejecutarse.
2- Vital	**Datos de los Paquetes** (ubicación de los paquetes, contenido del paquete, identificación personal del destinatario, dirección, teléfono, estado del envío)	Afectan la operación, pueden ser sostenidos por un corto plazo con soluciones temporales, a partir de las impresiones en los paquetes.
3- Sensible	**Dispositivos de mano (Handheld)**	Herramientas operativas importantes, pero reemplazables temporalmente por procedimientos manuales impresos.
4- No Crítico	**Computadora del jefe de almacén**	Herramienta de supervisión. Puede reemplazarse temporalmente. Su caída no detiene la operación si el sistema está en marcha.

- **Detalle del orden de procesamiento de tareas que lo requieran.**

1. El Personal de Almacén y Operaciones deberán evacuar a las personas que se encuentren en el almacén
2. El Equipo Técnico deberá cortar el suministro eléctrico de los equipos informáticos (Servidor, Computadora del jefe de almacén)

3. El personal de Almacén y Operaciones deberá prender la bomba de achique para empezar con el desagote del agua.
4. El Personal de Almacén y Operaciones deberá proceder a sacar el agua con los métodos manuales convenientes.
5. El Personal de Almacén y Operaciones deberá levantar los equipos informáticos y salvaguardarlos en la oficina administrativa de la empresa.
6. El Jefe de TI y el equipo técnico deberán activar el Hot Site.
7. El equipo técnico deberá verificar los daños en los equipos informáticos y de ser posible repararlos.
8. El equipo técnico deberá verificar el estado de los datos/información de nuestros paquetes/clientes y de ser necesario intentar recuperarlos a través de un backup.
9. El personal de Almacén y Operaciones una vez desagotada toda el agua deberá volver a llevar los equipos informáticos al almacén.
10. El equipo técnico deberá establecer los equipos y el WMS.

- **Disponibilidad de hardware alternativo:**

Se contará con un Hot Site contratado a proveedor externo, con condiciones de activación en menos de 4 horas. Ideal para proteger un sistema crítico como el WMS, que no puede ser reemplazado manualmente y del que depende toda la operación logística.

- **Disponibilidad de una sede alternativa para el almacenamiento de medios magnéticos (datos de backup) y documentación.**

La centralización de los datos en servidores on premise y la exposición a amenazas físicas (inundaciones, incendios, robos, fallas eléctricas) hace imprescindible que los backups no se encuentren en la misma ubicación que los sistemas originales.

Se recomienda establecer una política de resguardo físico y lógico externo que contemple:

- Backups semanales de los datos del WMS, incluyendo la base de datos operativa y los archivos de configuración del sistema.

- Copia automática y verificada en un repositorio remoto (en el lugar que decida la empresa).

- Resguardo físico semanal en dispositivos externos (discos duros cifrados o cintas LTO), almacenados en una sede alternativa geográficamente separada del almacén principal.

Esta sede puede ser una oficina administrativa secundaria de la empresa o un servicio especializado de custodia de medios. Debe cumplir con condiciones mínimas de seguridad: control de acceso, monitoreo ambiental, protección contra incendios y humedad, y trazabilidad de ingresos y egresos.