1. RESUMEN

El Plan de Recuperación de Desastres asegura que la organización pueda mitigar, responder y recuperarse eficientemente ante incidentes, garantizando la integridad y disponibilidad de sus sistemas tecnológicos.

2. OBJETIVO

El objetivo de este plan es garantizar la recuperación eficiente de los sistemas tecnológicos y datos críticos de la empresa tras un desastre, asegurando la continuidad de las operaciones.

3. ALCANCE

El ámbito de aplicación de las disposiciones contenidas en el presente plan comprende a toda la estructura la organización, es decir que todos los empleados, colaboradores, contratistas, consultores, temporales y demás trabajadores de la organización son responsables de hacer un uso adecuado de este documento, en cumplimiento con las políticas, leyes y regulaciones locales y las directrices establecidas por la organización.

4. PLAN

A continuación, se definen las fases de este plan de recuperación de desastres con el propósito de garantizar la recuperación y continuidad de procesos críticos, minimizando los impactos de interrupciones en los servicios, protegiendo sus activos de información, asegurando la confianza de sus clientes y cumpliendo con las normativas aplicables.

FASE 1: PREPARACIÓN Y PREVENCIÓN

Objetivo: Minimizar la probabilidad de desastres y establecer una base sólida para la recuperación.

Roles:

- **Gerente de TI:** Supervisa la preparación y define políticas de respaldo.
- **Analista de Riesgos:** Evalúa amenazas y prioriza recursos críticos.
- **Administrador de Infraestructura:** Implementa redundancias y medidas preventivas.

Actividades:

1. **Identificación de Sistemas y Datos Críticos**
   - Clasificar los activos de TI según su criticidad y dependencia operativa.
   - RTO (Recovery Time Objective): 4 horas para servicios críticos, 12 horas para sistemas secundarios.
   - RPO (Recovery Point Objective): 30 minutos para información crítica, 2 horas para información secundaria.
2. **Evaluación de Riesgos y Vulnerabilidades**
   - Identificar amenazas potenciales (fallas técnicas, ciberataques, desastres naturales).
3. **Implementación de Medidas Preventivas**
   - Configuración de respaldos automáticos.
   - Replicación de datos en un Data Center alterno.
4. **Capacitación y Simulacros**
   - Entrenamiento continuo del personal en el DRP.
   - Realización de simulacros para validar el plan.

FASE 2: RESPUESTA INMEDIATA

Objetivo: Contener el impacto inicial del desastre y activar el plan de recuperación.

Roles:

- **Coordinador de Respuesta:** Lidera las acciones inmediatas.
- **Especialista en Seguridad:** Contiene amenazas tecnológicas y asegura perímetros.
- **Equipo de Monitoreo:** Identifica anomalías y comunica incidentes.

Actividades:

1. **Detección y Evaluación del Incidente**
   - Monitorear alertas de seguridad y sistemas.
   - Determinar la naturaleza y alcance del incidente.
2. **Activación del DRP**
   - Notificar al equipo de respuesta.
   - Establecer un punto de comando central.
3. **Contención del Daño**
   - Aislar sistemas comprometidos para evitar propagación.
   - Implementar soluciones temporales.

FASE 3: RECUPERACIÓN INICIAL

Objetivo: Restaurar los sistemas críticos en el menor tiempo posible para reanudar operaciones esenciales.

Roles:

- **Gerente de Recuperación:** Decide prioridades y supervisa restauración.
- **Especialista en Backup:** Restaura los datos críticos.

- **Ingeniero de Redes:** Garantiza la conectividad en la infraestructura restaurada.

Actividades:

1. **Evaluación del Daño**
   - Identificar sistemas y datos afectados.
   - Establecer prioridades de recuperación.
2. **Recuperación de Datos**
   - Restaurar datos desde respaldos recientes (RPO: 30 minutos).
   - Verificar integridad y consistencia de los datos.
3. **Reactivación de Servicios Esenciales**
   - Reiniciar servidores y aplicaciones críticas.
   - Validar la conectividad y funcionamiento básico.

FASE 4: RECUPERACIÓN COMPLETA

Objetivo: Restaurar completamente las operaciones tecnológicas y estabilizar los sistemas.

Roles:

- **Director de TI:** Aprueba el restablecimiento total de operaciones.
- **Equipo de QA:** Realiza pruebas funcionales y de calidad en sistemas restaurados.
- **Coordinador Operativo:** Supervisa la transición hacia operaciones normales.

Actividades:

1. **Recuperación de Sistemas Secundarios**
   - Restaurar servicios y aplicaciones no esenciales.
   - Reintegrar todas las dependencias operativas.
2. **Validación Total**

- Realizar pruebas de funcionalidad y seguridad en todos los sistemas.
- Confirmar consistencia y completitud de los datos.

3. **Reintegro Total de Operaciones**
    - Desactivar soluciones temporales implementadas.
    - Comunicar el retorno a la normalidad.

FASE 5: REVISIÓN Y MEJORA CONTINUA

Objetivo: Evaluar la respuesta al desastre y fortalecer el DRP.

Roles:

- **Auditor Interno:** Revisa y valida la efectividad del DRP.
- **Responsable del DRP:** Coordina actualizaciones y mejoras.
- **Encargado de Capacitación:** Organiza entrenamientos y simulacros.

Actividades:

1. **Análisis Post-Incidente**
    - Documentar el desempeño del DRP.
    - Identificar áreas de mejora y lecciones aprendidas.
2. **Actualización del DRP**
    - Incorporar mejoras basadas en los resultados del análisis.
    - Revisar y actualizar roles, procedimientos y tecnologías.
3. **Entrenamiento y Simulacros**
    - Capacitar al personal en las mejoras implementadas.
    - Realizar simulacros regulares para validar la efectividad del plan.

5. CUMPLIMIENTO

5.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de este plan mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video
- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario del plan y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: