7 pasos para crear un plan de continuidad ante emergencias

GRANICUS

INTRODUCCIÓN

Los daños provocados por fenómenos naturales y creados por el hombre que derivan en desastres o situaciones de crisis en el país, presentan como resultado, una desaceleración para el desarrollo nacional, ello implica altos costos a consecuencia de una abrupta interrupción de operaciones en los distintos sectores económicos.

Para sobrevivir estas situaciones; una organización debe mantener sus procesos críticos en funcionamiento durante una emergencia o desastre, minimizando el tiempo de recuperación y asegurando un constante suministro de servicios de primera necesidad para la población.

Objetivo

Los planes de continuidad ayudan a la organización a mantener la resiliencia para poder responder rápidamente a una interrupción, permitiendo a la organización seguir funcionando al menos a un nivel mínimo durante un evento disruptivo o emergencia.

Aprendamos las siguientes definiciones:

- Plan de continuidad de negocio (BCP) Es un conjunto de recursos, actividades y procedimientos que se crean con el fin de ser utilizados en caso de que ocurra una emergencia o desastre.
- Plan de Recuperación de Desastres (DRP) Proceso estructurado que aplica a los aspectos de una organización que depende de una infraestructura de tecnología de la información TI en funcionamiento. Es parte esencial de un plan de continuidad.

Alimento para el pensamiento

1. 75% de las compañías fallan en lograr sus objetivos dentro de $_3$ años por falta de un plan de continuidad
2. ¿Qué operaciones de su organización se verían afectadas por una interrupción en los servicios?
3. ¿Cuántas de ellas son críticas?
4. ¿Cuál sería el impacto sobre la misión de su organización?

Plan de Continuidad y los beneficios de su implementación

1. Identificar los diversos eventos que podrían impactar la continuidad de operaciones, así como sus repercusiones financieras, humanas, de reputación, entre otras.
2. Reacción efectiva ante situaciones de emergencia, evitando perdidas de recursos y agilizando las labores relacionadas a la continuidad de procesos críticos.
3. Clasificación de recursos para priorizar su protección.
4. Identificación de roles y funciones del personal encargado de los procesos críticos definidos.
5. Reducir el número y magnitud de decisiones durante cualquier periodo de crisis.

ELABORACIÓN DEL PLAN DE CONTINUIDAD

PASO 1: Establecer Gobernanza

- Política (Misión y Visión).
- Respaldo alta jerarquía organizacional (recursos).
- Distribuido al personal correspondiente.
- Adiestramiento.
- Responsabilidades contractuales (debe contener las especificaciones, requerimientos, obligaciones y costos (si aplican) de ambas partes).

PASO 2: Análisis de Riesgo (Identificar amenazas)

Identifica aquellas amenazas a las que la organización es propensa. Identifica eventos que pueden desencadenar un incidente, produciendo daños materiales o pérdidas humanas, así como suspensión de servicios o actividades.

1. Naturales (Huracanes, Sismos, Inundaciones, Tsunamis, Sequías).
2. Creados por el hombre (Terrorismo, Epidemias, Sabotaje, Ataques cibernéticos, Concentración de Masas).
    - Es necesario relacionar la probabilidad de que este ocurra con el impacto que causaría.
    - Responsabilidades contractuales (debe contener las especificaciones, requerimientos, obligaciones y costos (si aplican) de ambas partes).

Ejercicio #1

Crear Análisis de Riesgo (Identificar Amenanzas)

Tabla para analizar riesgos:

Amenaza	Probabilidad	Impacto	Riesgo	Acción Preventiva
1.	ALTO	ALTO	ALTO	1. Desarrollar pasos a seguir en preparación llegada de huracán
	ALTO	MEDIO	MEDIO	
	BAJO	ALTO	MEDIO	1. Plan de comunicación, método de comunicación, cuando se activa el plan, acciones correcpondientes por departamento, lugares alternos, personal clave, equipo necesario.
	MEDIO	MEDIO	MEDIO	
	BAJO	BAJO	BAJO	

PASO 3: Análisis de Impacto en el negocio (BIA):

Facilita la identificación de los Procesos Críticos y analiza el nivel de impacto en caso de interrupción. Establece prioridades y objetivos de tiempo de recuperación.

Personal: Impactos que afecten directamente a la integridad del personal.

Instalaciones: Impactos que disminuyan las capacidades de las instalaciones de la organización o atenten contra su seguridad.

Población: Interrupción en las operaciones que afecta un servicio o producto básico para la población.

Financiero / Económico: Interrupciones que afecten los objetivos financieros provoquen pérdidas mayores.

Legal: Impactos que incurran en faltas a la ley y provoquen amonestaciones para la organización.

Operacional: afectan la ejecución de los procesos que se llevan a cabo y tengan impacto en los objetivos estratégicos organizacionales.

Prestigio / Reputación: repercuten a nivel reputacional por no brindar un servicio, producto o info. Suelen repercutir en notas negativas de la prensa.

Ejercicio #2

Crear Análisis de Impacto en el negocio (BIA)

Formato para evaluar el análisis de impacto:

Proceso	(RTO) Tiempo de recuperación	Actividad Principal	Frecuencia	Responsable	Análisis de Impacto
1. Abrir compuertas represa Carraízo	24 horas	Medir nivel del embalse Notificar medida a Director de represa Activar alarma población Abrir compuertas	Antes de alcanzar nivel máximo	Primario- Supervisor de represa.	**Instalaciones:** La interrupción de este proceso prococaría una disminución en las capacidades de las instalaciones **Población:** atenten contra de la seguridad poblacional. **Legal** Prestigio / Reputación

PASO 4: Desarrollo del plan de manejo de incidentes

1. Medidas de Preparación (antes, durante, después del incidente). https://www.ready.gov/plan.

2. Cree estructura de comunicación – ¿Cuándo se activa el plan? Vigilancia, ¿Aviso?, Manejo de Emergencias, ¿Qué método?, Actualizar los teléfonos de contacto de sus empleados, supervisores y compañeros de trabajo.

3. Establezca lugar de encuentro primario y secundario.

4. Equipo de Emergencia (Primera necesidad, seguridad, hardware/software)

    - En el caso de las aplicaciones tecnológicas, identifique las plataformas le por división.

    - Contacte al equipo de atención al cliente y oriéntese sobre el plan de emergencias de los sistemas de información.

    - Garantice la continuidad de los mismos para evitar cualquier interrupción de servicio esencial, como, por ejemplo: Compruebe los sistemas financieros, nómina, manejo de asistencia, recursos humanos, servicios al ciudadano. Al los sistemas estar en la nube Microsoft Azure, le garantiza la seguridad del resguardo de datos, y una vez con acceso a Internet podrán reanudar funciones desde el centro de operaciones de emergencias (COE).

5. Establezca compromisos contractuales con terceros (cadena de suplido).

6. Cree equipos de trabajo y establezca roles y responsabilidades (Equipo de Continuidad, Líder de Continuidad, equipo de evaluación de daños y recuperación).

7. Procedimiento para regresar a facilidades primarias.

PASO 5: Plan de recuperación ante desastres de TI (DRP)

1. Medidas de preparación (antes, durante, después del incidente). https://www.ready.gov/plan

2. Inventario de hardware/software (servidores, computadoras y dispositivos inalámbricos, aplicaciones, datos).

    - Identifique las aplicaciones que pueden apoyarle a servir y capturar información de los servicios inmediatos que necesitan sus ciudadanos

    - (Insertar OneView) Portal de auto-servicio o aplicación móvil OneLink parar recibir solicitudes de servicio, ver historial de solicitudes, crear informes de incidencias referentes al desastre natural.

3. Desarrollar estrategias de recuperación para sistemas, aplicaciones y datos. Plan de Resguardo de Archivos y Formas (copias digitales y físicas).

4. Priorizar la restauración de hardware y software.

5. Establezca lugares alternos de computación “hot sites”.

6. Cree equipos de trabajo y establezca roles y responsabilidades.

PASO 6: Capacite al personal

- Adiestre al personal en cuanto a roles y responsabilidades.
- Procedimientos específicos de recuperación y continuidad.

PASO 7: Conduzca ejercicios

- Realice pruebas y ejercicios (Ejercicios de Mesa).
- Simulaciones (Impacto Huracán, recuperación de data, corte de energía, pérdida/ violación de datos).

CONCLUSIÓN

Existen múltiples recomendaciones para mantener a su organización preparada ante cualquier emergencia, pero es esencial que pueda identificar las necesidades particulares de su entidad para poder trabajar un plan adaptado a su organización. Recuerde que estos planes lo ayudan a detener y prevenir potenciales riesgos. SE recomiendan revisar periódicamente y realizar los ajustes necesarios si existen situaciones de emergencia, o cambios físicos, técnicos o de personal en su organización.