Entendiendo el nivel de madurez de su estrategia de continuidad de negocios

Entender el nivel de madurez de sus prácticas de recuperación de desastres exige un proceso honesto de autoevaluación

Usamos el concepto de "niveles de madurez" para tratar de expresar en un lenguaje objetivo, preciso y común el nivel de preparación que tiene una empresa, grupo o aplicación y la capacidad que tiene para recuperarse ante una interrupción de servicio. Esto, por supuesto, puede tener muchas connotaciones: puede tratarse de la pérdida de un solo archivo, la caída de una aplicación o la interrupción completa de un centro de datos. Todos estos elementos pueden afectar de forma negativa la operación de una empresa.

Es posible obtener una comprensión más profunda de esta preparación mediante la evaluación de una serie de factores que nos pueden ayudar a revelar cuál es nuestro nivel de madurez frente a la recuperación de desastres.

A continuación detallamos una serie de preguntas que le permitirán comprender de manera más profunda los criterios para calificar el estado actual de su organización.

Preguntas clave para enmarcar el problema

Para iniciar debemos abordar el ejercicio reflexionando sobre el impacto de la inactividad ante una caída preguntándonos:

¿Qué tan severo es el impacto de una de estas caídas para el negocio?

¿Cuál es el momento exacto en que una organización empezará a sufrir los efectos de esa caída?

En cuanto a:

- Disponibilidad de sistemas vitales
- Bases de datos
- Datos de clientes
- Recursos de red

En este escenario, su compromiso es evaluar de 1 a 5 lo que considere es su nivel de madurez en cada categoría, observando los siguientes criterios:

1 Muy Bajo	**2** Bajo	**3** Moderado	**4** Alto	**5** Muy Alto

Empecemos con la evaluación de nuestras variables independientes:

1. Objetivo de tiempo de recuperación

¿Cuánto tiempo de inactividad puede soportar la empresa? ¿Minutos, horas o días?

Y en caso de ocurrir un incidente: **¿cuánto tiempo sientes que pasaría?** Evalúe esta respuesta siguiendo la escala de arriba, considerando 1 como inaceptable y 5 cómo ideal.

El objetivo de tiempo de recuperación debe identificarse para todos los sistemas, redes, bases de datos y otros recursos de TI de importancia crítica. Estas son una métrica clave al construir planes de recuperación ante desastres.

2. Objetivo de punto de recuperación

¿Cuál es la cantidad de tiempo que los datos pueden "envejecer" antes de que ya no sean útiles para la organización?

¿Cuál estimas es la cantidad de tiempo máxima entre el momento en que ocurre un incidente y tu último backup? Evalúe esta respuesta siguiendo la escala de arriba, considerando 1 como inaceptable y 5 cómo ideal.

Cuanto más corto sea el objetivo de punto de recuperación, más críticos serán los datos. El proceso de copia de seguridad debe ser lo suficientemente robusto como para replicar datos en el menor tiempo posible entre la copia original y la replicada.

3. Arquitectura de protección

¿La solución de protección proporciona recuperación local, recuperación en la nube o ambas?

¿La solución está construida a partir de uno o varios productos?

¿Tiene la infraestructura de red la suficiente capacidad de recuperación para soportar la arquitectura de protección con circuitos de ejecución diversa y suficiente ancho de banda para manejar las demandas de tráfico normal y de emergencia?

¿Es la arquitectura de protección lo suficientemente escalable para soportar una situación anormal en la que se necesitan más recursos de los disponibles?

4. Alcance de la protección

¿Qué activos de TI están siendo protegidos?

- Archivos de usuario
- Bases de datos
- Aplicaciones centrales
- Imágenes de servidor
- Infraestructura de TI

Durante un desastre:

¿Estarán todos los elementos del entorno de TI disponibles y operativos de manera que permita a los empleados conectarse de forma segura y continuar trabajando?

5. Documentación

¿Están todos los procedimientos de recuperación completamente documentados y al día?

¿Existen varias copias de los procedimientos disponibles en papel y en formato electrónico?

¿Cuentan los equipos de emergencia con acceso a copias de planes en espacios alternos como en sus autos o en sus hogares?

¿Estarán los recursos colaborativos - Intranets y repositorios de contenido - disponibles para almacenar copias de planes de forma segura?

¿Tienen los equipos de emergencia copias de los planes de recuperación ante desastres en sus teléfonos móviles?

¿Están en capacidad de acceder de forma remota a sus planes utilizando sus teléfonos móviles?

6. Alcance de pruebas

Las pruebas pueden ser tan simples como una descripción general de un plan. Sin embargo, la cantidad de cobertura al probar y validar los procedimientos de recuperación es importante. Por ejemplo:

¿Se evalúan los archivos al azar y de manera rápida, se tumban los servidores o se verifica la infraestructura secundaria?

Estas pruebas son de vital importancia para garantizar que asuntos más allá de las cuestiones técnicas no se queden por fuera, y que se cuente con los arreglos necesarios, tanto financieros como de suministros, para por ejemplo dotar un nuevo espacio de trabajo en caso de ser necesario.

7. Frecuencia de pruebas

¿Con qué frecuencia se ejecutan procedimientos de recuperación?

La experiencia ha demostrado que un mínimo de una prueba al año es un punto de partida para la mayoría de los sistemas de TI, pero para los sistemas considerados de importancia crítica, es aconsejable realizar pruebas con más frecuencia, especialmente si estos han pasado por una serie de cambios.

Los planes de recuperación ante desastres deben reflejar esos cambios. Aquí es donde muchos de estos planes fallan, al no mantener al día estos cambios dentro del plan de recuperación de desastres.

8. Patrocinio organizacional

¿Es la preparación para la recuperación un proyecto exclusivo de TI o una iniciativa de toda la empresa?

¿Están las directivas de la empresa involucradas en impulsar y respaldar la necesidad de contar con una recuperación ante desastres o únicamente está respaldada por la gestión de TI?

¿Ha aprobado la administración un presupuesto para recuperación ante desastres?

¿El personal de TI ha recibido capacitación en procedimientos de recuperación ante desastres por parte de proveedores de equipos y proveedores de servicios de red?

Idealmente, la recuperación ante desastres se configura como una función específica: con un presupuesto, personal y cronograma de actividades continuo y dedicado que incluye revisiones del plan, ejercicios y formación del personal.

Analizando los resultados

Tras responder internamente a las preguntas anteriores y asignar un valor a cada punto clave, obtendremos un resultado claro de acuerdo a la siguiente tabla que mapea los niveles de apoyo y compromiso con los cinco niveles de nuestro propio modelo de madurez:

NIVEL	PUNTAJE
1 - Ad Hoc	**8**
2 - Reactivo	**9 a 15**
3 - Preparado	**16 a 22**
4 - Proactivo	**23 a 27**
5 - Resiliente	**28 a 35**

Alcanzar el Nivel 3 (Preparado) es un objetivo ideal para la mayoría de las organizaciones porque demuestra un conocimiento y un compromiso con las métricas clave de DR, incluidos RTO / RPO, documentación, pruebas y patrocinio.

Alcanzar el Nivel 4 (Proactivo) se puede lograr aprovechando los servicios únicos de los proveedores basados en la nube.

Después de completar el ejercicio, ¿cómo ha salido rankeada su organización?

Una preparación adecuada ante situaciones adversas e imprevistas es de vital importancia para todas las organizaciones. Contar con el aliado adecuado puede ayudarle a elevar su nivel de preparación contra un desastre.

Para más información visita: LIBERTYNET.COM

