

Configure su plan de Recuperación de Desastre en 7 pasos

Configure su plan de Recuperación de Desastre en 7 pasos, es el tema de este post.

Después de una pérdida accidental de datos causada por un desastre , muchas empresas quedan indefensas, sin capacidad de recuperación. Ante esto, cada vez más empresas confían en su plan de recuperación de TI (DRP) para una recuperación rápida en caso de desastre.

¿Cómo planificar esta reanudación de actividad y qué medidas tomar para facilitar la vuelta a la normalidad? ¿Cuáles son las mejores prácticas que se deben adoptar y los obstáculos que se deben evitar para la recuperación segura de datos ? Descubra los secretos de un plan de recuperación de TI eficaz con estos 7 pasos.

Defina el alcance de su proyecto

The background image shows a hand pointing at a target on a desk. The target has concentric circles, with the center being black and the outer rings being white and yellow. A laptop is visible in the background, and the overall scene is dimly lit with a warm, orange-toned light.

Definir el **alcance** de su proyecto

su DRP de TI debe garantizar la seguridad y disponibilidad continuada de los datos.



¿Su empresa necesita un acceso rápido a sus datos para garantizar la continuidad del negocio? ¿O puede permitirse una interrupción sin grandes consecuencias de unas horas o días? En el primer escenario, su DRP de TI debe garantizar la seguridad y disponibilidad continuada de los datos. Incluso en el caso de una posible falla de su equipo en el sitio (falla del equipo, incendio, inundación, etc.) Para lograrlo, es posible recurrir a una solución de almacenamiento fuera del sitio ofrecida por un proveedor de servicios de respaldo subcontratado . Por tanto, sus datos permanecen accesibles en cualquier situación.

Enumere las vulnerabilidades de su organización y realice un análisis de riesgo.

¿Su empresa ha sido blanco de delitos cibernéticos en el pasado? ¿Está ubicado en un área geográfica con riesgos naturales (inundaciones, zona sísmica, etc.) ¿Están sus

empleados al tanto de los problemas relacionados con la delincuencia en línea (ransomware, phishing, etc.) ¿Cuáles son los datos más sensibles a proteger? ¿Quién de sus empleados puede acceder a él?

¿Son sus herramientas de respaldo (discos duros, llaves USB) lo suficientemente confiables o existe riesgo de pérdida? Su plan de recuperación ante desastres debe proteger sus activos tanto como sea posible. Puede ser necesario establecer áreas prioritarias que requieran una atención especial.

Defina sus estrategias de recuperación de datos

El tercer paso es asegurarse de tener una estrategia de recuperación y restauración de datos eficaz. De hecho, no basta con ahorrar y luego esperar un posible desastre. Aún necesita poder restaurar rápidamente sus datos para poder reiniciar su actividad dentro de un período de tiempo aceptable. Los conceptos de [RPO](#) y RT0 entran en juego en este punto del análisis.

El RT0 (objetivo de tiempo de recuperación) designa el tiempo de interrupción máximo aceptable de un recurso informático. Cuanto menor sea el RT0, más corta debe ser la interrupción. El RPO (u objetivo de punto de recuperación) le permite definir la frecuencia de las copias de seguridad. Cuanto más bajo sea, más deberán combinarse las salvaguardias (por ejemplo, sector bancario, telecomunicaciones, etc.)

Cree una versión impresa de su plan de recuperación ante desastres

Su [DRP](#) no debe permanecer en la etapa de post-its esparcidos por todo su departamento de TI. Es necesario reunir todos sus procedimientos en una guía completa que pueda ser entendida

por los empleados involucrados. Esta guía debe guardarse en un lugar de fácil acceso y preferiblemente en papel.

De hecho, sería lamentable sufrir una interrupción en el servicio de TI mientras su plan de recuperación se almacena en estaciones de trabajo inaccesibles. Este plan de recuperación debe haber sido elaborado en colaboración con su equipo, para asegurar que sea lo suficientemente coherente y cercano a la realidad sobre el terreno.

Para comprender todo en el plan de recuperación ante desastres, sus empleados necesitarán capacitación que aclare todos los elementos clave. Como se mencionó en el punto anterior, la redacción del plan de recuperación ante desastres se habrá realizado en colaboración con los miembros de su equipo.

Brinde capacitación a sus empleados

Deberá asegurarse de que todos hayan entendido las medidas que deben tomarse en caso de desastre. Un punto de fricción podría poner en peligro todo el proceso y poner en riesgo a su empresa. Esta formación también permitirá destacar nuevas perspectivas en las que no necesariamente habías pensado, gracias a la retroalimentación de tus empleados.

Prueba tu plan

Un mundo separa la teoría de la práctica. Definir y reunir todas las medidas de DRP es un primer paso esencial, que luego debe completarse con un escenario. ¿Los procedimientos definidos serán lo suficientemente relevantes para minimizar la interrupción del negocio?

Entre las diversas pruebas a realizar, las comprobaciones de las copias de seguridad permiten garantizar que las copias de seguridad no estén dañadas y se puedan utilizar para una

restauración rápida y completa de los datos. La prueba de reinicio de la infraestructura garantizará que todo su sistema (servidores, redes, estaciones de trabajo, etc.) pueda recuperarse después de un bloqueo. Finalmente, también es posible considerar una prueba en un sitio de respaldo, cuando su infraestructura ya no es accesible.

Revise sus procedimientos y actualícelos si es necesario

La evolución tecnológica es constante, el software requiere actualizaciones periódicas y es importante mantenerse informado. Su plan de recuperación ante desastres también debe seguir esta lógica, con revisiones periódicas si es necesario.

Puede integrar nuevos pasos, realizar cambios en otros, simplificar ciertos procedimientos. Tenga en cuenta que estos cambios en su DRP deberán comunicarse a su personal y probarse en una situación de la vida real para validarlos. Los cambios demasiado frecuentes podrían comprometer la confiabilidad general del plan. Así que apégate a los cambios esenciales.

Leer también: [Por qué el plan de recuperación ante desastres ya no debería considerarse una opción para su empresa; Recuperación y protección de datos: ¿su infraestructura crítica es realmente segura?; Servidores alojados, su falta de copias de seguridad y DRP](#)