Plan de Recuperación ante Desastres (DRP)

Autor:Santiago Roman

Febrero 2024

1 Introducción

Los desastres son acontecimientos inesperados o repentinos que perturban la sociedad humana, ya sean causados por actividades naturales o humanas. Estos eventos pueden causar daños financieros, económicos, humanos y ambientales. Es bien sabido que la falta de un plan de acción ante desastres naturales o perturbaciones comerciales puede provocar la pérdida total del negocio o un daño grave a su reputación.[1]

Por lo tanto, es esencial crear un Plan de Recuperación de Desastres de Tecnología de la Información (IT DRP) y un Plan de Continuidad del Negocio. El plan evalúa el potencial comercial y establece líneas de base y cronogramas para restaurar la tecnología de la información en el evento. DRP es un proceso detallado y documentado que ayuda a restaurar y proteger la tecnología de una empresa. Está incluido en el Plan de Continuidad del Negocio (BCP), que es un plan para asegurar que la empresa continúe operando.[2]

2 Desarrollo

2.1 Plan de Recuperación ante Desastres (DRP)

Un Plan de Recuperación ante Desastres, también conocido como DRP, es un conjunto escrito de reglas y procedimientos diseñados para guiar a una organización en la implementación de estrategias de recuperación ante desastres. Su objetivo principal es proteger la infraestructura de tecnología de la información de la empresa y facilitar su recuperación oportuna. Para asegurar una respuesta eficaz ante eventos o emergencias que afecten a los sistemas técnicos de la organización, este plan es fundamental.[4]

2.2 Tipos de Plan de Recuperación ante Desastres (DRP)

2.2.1 Plan de Recuperación ante Desastres Virtualizado

Un sistema de recuperación ante desastres utiliza la virtualización para que su implementación sea más fácil y eficiente. Se pueden instalar nuevas máquinas virtuales rápidamente en entornos virtuales, lo que facilita la restauración de aplicaciones gracias a su alta disponibilidad. Aunque las pruebas son sencillas, es importante garantizar que las aplicaciones puedan funcionar en modo de restauración ante desastres y volver al funcionamiento normal dentro del entorno establecido y los objetivos de tiempo de recuperación.[3]

2.2.2 Plan de Recuperación ante Desastres de la Red

El Plan de recuperación de la red menciona que cuanto más compleja sea la red, más difícil será desarrollar un plan de recuperación. Es indispensable definir cuidadosamente el proceso de recuperación, para intentar mantenerlo. Los detalles del proceso se centrarán en otros aspectos de la red, como su trabajo y personal.

2.2.3 Plan de Recuperación ante Desastres en la Cloud

Un plan de recuperación ante desastres en la nube incluye copia de seguridad completa y copia de seguridad de archivos. Aunque requiere espacio, tiempo y dinero, su mantenimiento requiere una gestión cuidadosa. Es responsabilidad del admin conocer la ubicación de los servidores virtuales y físicos, y el sistema debe abordar cualquier problema de seguridad que pueda mitigarse mediante pruebas.

2.2.4 Plan de Recuperación ante Desastres del Centro de Datos

El Plan de Recuperación del Centro de Datos se centra en la infraestructura, así como en una evaluación detallada de los riesgos operativos. Analiza una serie de escenarios posibles mientras evalúa factores importantes como las obras, los sistemas eléctricos, la seguridad y el espacio de oficinas.[3]

2.3 Componentes del Plan de Recuperación ante Desastres (DRP)

- Evaluación de riesgos: Las organizaciones deben evaluar cuidadosamente las posibles amenazas y vulnerabilidades en la seguridad de TI, especialmente en áreas donde las personas son vulnerables a los ciberataques.
- Continuidad del negocio: Incluye la identificación de estrategias y recursos para mantener las empresas operativas en caso de un desastre.
- Copia de seguridad y recuperación: Se centra en documentar e implementar procedimientos y sistemas de copia de seguridad regulares, así como planes detallados para restaurar estos recursos en caso de un ciberataque.

- Respuesta a incidentes: Establecer procesos y procedimientos claros para identificar amenazas y contención, evaluar daños y restaurar los sistemas afectados.
- Comunicación: En caso de un ataque, el plan de recuperación ante desastres debe describir cómo comunicar el incidente a las partes interesadas, como empleados, clientes, medios de comunicación,etc.
- Educación y capacitación: Es esencial establecer un sistema que brinde capacitación efectiva a los empleados sobre buenas estrategias de ciberseguridad y recuperación ante desastres.
- Pruebas y simulación: Los planes de recuperación ante desastres deben realizarse y ejecutarse periódicamente. Esto ayuda al equipo a ganar confianza en sus funciones y responsabilidades, preparándolos para hacer frente a las amenazas cuando surjan.[5]

2.4 Responsables de un equipo de Plan de Recuperación ante Desastres (DRP)

- Director de seguridad de la Información: Responsable de la estrategia global de ciberseguridad en grandes empresas, lidera la recuperación ante desastres y supervisa la seguridad de la información y los datos frente a ciberataques.
- El Equipo de Seguridad TI: Trabaja como soporte técnico especializado bajo la dirección del CISO, monitoreando y protegiendo redes y sistemas, siendo la primera línea de defensa contra ciberataques y respuesta a incidentes.
- Administradores de red: La clave para la ciberseguridad son los profesionales de recuperación de desastres, que son responsables de mantener y proteger redes, servidores y otros equipos, especialmente en pequeñas empresas.
- Servicios TI y Soporte Técnico: Aunque no lideran la seguridad, coordinan las operaciones del día a día de servidores y sistemas, siendo esenciales en los equipos de recuperación ante desastres.
- Especialistas en Gestión de Riesgos: Evalúa y gestiona los riesgos asociados a los ciberataques, identifica amenazas potenciales y propone controles para prevenir amenazas reales.
- Asuntos Legales y Cumplimiento: Garantizar que los procedimientos de gestión de riesgos cumplan con las leyes y regulaciones.
- Comunicaciones de crisis, medios y relaciones públicas: un departamento independiente que ayuda en la recuperación de desastres e informa a los afectados por los eventos.

- Gerente del Plan de Continuidad del Negocio (BCP): Profesional dedicado a desarrollar, mantener e implementar el plan de continuidad del negocio de una organización, asegurando su operación continua y probándolo y actualizándolo periódicamente.[7]

2.5 Pasos para crear un Plan de Recuperación ante Desastres (DRP)

2.5.1 Compromiso Organizacional

Es importante que todos los miembros de la organización participen en el plan de recuperación de desastres (PRD), comenzando por el apoyo y participación activa de la dirección. Se debe iniciar una planificación eficaz al más alto nivel, garantizando la asignación adecuada de recursos al proyecto.

2.5.2 Formación de un Comité de Planificación

Para supervisar el desarrollo y la implementación del DRP, se debe formar un comité multidisciplinario con representantes de todas las áreas funcionales y grupos principales. El comité es responsable de garantizar una representación plena y efectiva durante todo el proceso.

2.5.3 Evaluación de Riesgos y Riesgos del Negocio

ÇPara establecer las bases del plan, el comité DRP debe realizar una evaluación y evaluación del impacto comercial. Este análisis destaca las amenazas y los impactos potenciales en cada parte de la organización.

2.5.4 Planificar opciones de recuperación

Investigar y evaluar posibles opciones para recuperar equipos informáticos perdidos o que funcionan mal. En esta sección se detalla la búsqueda y el mantenimiento de equipos y suministros de emergencia.

2.5.5 Recopilación de datos

la planificación y el diseño exitosos dependen de la recopilación de datos importantes, como registros de respaldo, números críticos y registros de inventario.

2.5.6 Planes y Documentos de Preparación

El plan se define en un documento detallado que incluye los procedimientos para todas las etapas del desastre, organizados en categorías y responsabilidades asignadas.

2.5.7 Plan de pruebas

Las pruebas periódicas, ya sean de simulación o de finalización planificada, son necesarias para determinar el rendimiento del sistema y los cambios necesarios para mejorar su rendimiento en caso de una emergencia.

2.5.8 Aprobación e implementación

Después de redactarse y probarse, el plan debe recibir la aprobación de la gerencia para garantizar que sea coherente con el plan y compatible con los proveedores de servicios y los servicios externos.[6]

3 Conclusiones

- Un plan de recuperación ante desastres es un documento importante para cualquier proyecto de seguridad porque garantiza la continuidad de las empresas, especialmente aquellas con tecnología.
- El Plan de Recuperación ante Desastres (DRP) se muestra como una parte importante de la gestión de seguridad de la empresa, ya que proporciona una forma coordinada de afrontar problemas inesperados y garantizar la seguridad de la organizacion frente a un ciberataque.
- Este plan no solo sirve como marco para ayudar a enfrentar las disrupciones, ademas es reconocido como una herramienta importante para proteger el prestigio, la continuidad del negocio y la confianza de las partes interesadas.Para hacer frente a las amenazas que fluctúan en el entorno empresarial, es fundamental un decuado desarrollo y mantenimiento es esencial.

References

[1] Luis Ignacio Delgado Alvarez. Plan de recuperación ante desastres para la reactivación económica del sector productivo, dec 2018. Disaster Recovery Plan for the economic reactivation of the Productive sector.

[2] BYRBERNY. Introducción al plan de recuperación ante desastres de ti, oct 2020. GESTIÓN DE TI Introducción al Plan de Recuperación ante Desastres de TI “Aquí lo importante es definir las políticas del negocio y establecer lo que el negocio quiere para sus datos y recuperarse en caso de algún evento que ponga en peligro su estabilidad informática”.

[3] Paul Crocetti. Plan de recuperación de desastres o drp, mar 2022. Un plan de recuperación ante desastres (Disaster Recovery Plan o DRP) es un enfoque estructurado y documentado.

[4] EUSKO JAURLARITZA. Plan de recuperación de desastres (drp), jan 2021. El propósito de un plan de recuperación de desastres es explicar de manera integral las acciones consistentes que se deben tomar antes.

[5] Byron Vicente Nieto Muñoz. Análisis y evaluación para el diseño de un plan de recuperación ante desastres (drp) aplicado en un centro de datos para empresas municipales basado en la norma iso/iec 24762: 2008. B.S. thesis, 2015.

[6] Team Ninja. Cómo crear un plan de recuperación ante desastres (drp), feb 2024. En términos de tecnología de la información, una catástrofe es cualquier tipo de evento que interrumpe la red.

[7] Johnny William Santana Sornoza. Drp o plan de recuperación ante desastres, jun 2021. La recuperación ante desastres se define, en términos generales, como la capacidad de una organización para responder y recuperarse de eventos catastróficos que afecten negativamente a sus operaciones o infraestructura.