vorofx

Plan de Recuperación de Desastres y Continuidad del Negocio

Índice

1. Introducción.

1.1. El Plan de Recuperación de Desastres y Continuidad del Negocio, en adelante "el Plan", tiene como objetivo garantizar la seguridad de los empleados, dar continuidad a las operaciones comerciales vitales e intentar proporcionar un servicio continuo a nuestros Clientes, todo ello tras incidentes no planificados como desastres naturales, cortes de energía, ciberataques y cualquier otro evento perturbador.

El plan incluye:

- Un personal de recuperación de desastres que será responsable de asegurar las operaciones continuas en caso de una interrupción mayor; Archivado de todos los documentos originales;
- La copia de seguridad de los servidores se realiza a través de SQL a una instancia en la máquina de Amazon Web Services (“AWS”). La copia de seguridad se realiza para cada operación comercial. Una copia de seguridad general se realiza desde el servidor principal y de respaldo una vez al día; y
- Servidores críticos replicados en Amazon Web Services en una dirección IP diferente utilizada de servidores de respaldo; y la plataforma de correo electrónico reside en ambas instancias de Amazon Web Services.

2. Alcance del Plan.

2.1. El propósito de este Plan es restaurar las funciones críticas del negocio y los sistemas esenciales y necesarios lo más rápido posible, basándose en la prioridad.

2.2. Muchas de las aplicaciones que son críticas para mantener las funciones del negocio de nuestra empresa no están alojadas en nuestras instalaciones, sino que están hospedadas por socios comerciales. En esos casos, nuestras responsabilidades de continuidad del negocio y recuperación de desastres consisten en asegurar que tenemos conectividad con estas partes y que las aplicaciones requeridas están disponibles.

2.3. Revisaremos los Planes de Continuidad del Negocio y Recuperación de Desastres de nuestros socios y proveedores clave y participaremos en sus ejercicios de Recuperación de Desastres para asegurar operaciones ininterrumpidas si uno de ellos necesita declarar un evento de Recuperación de Desastres.

3. Estrategia de continuidad del negocio.

3.1. Contamos con una arquitectura tecnológica "siempre activa" que proporciona continuidad en caso de una variedad de escenarios de fallo. Este enfoque en la continuidad permite que el negocio permanezca inafectado por la gran mayoría de los eventos localizados potencialmente catastróficos, como un incendio en un edificio de oficinas o centro de datos.

3.2. Para mantener la continuidad de nuestra infraestructura física y arquitectura de software, mantenemos múltiples centros de datos que están ubicados en áreas geográficas separadas de nuestras principales instalaciones comerciales para proteger contra los efectos de un evento a nivel regional. Si ocurre un evento que amenaza la continuidad del negocio de la empresa, cualquier centro de datos puede asumir todas las funciones críticas y son altamente tolerantes a fallos en caso de que un evento de continuidad del negocio afecte la disponibilidad de un servicio crítico de TI, la empresa seguirá la estrategia de recuperación de desastres para restaurar los servicios afectados.

4. Estrategia de recuperación de desastres.

4.1. En caso de tormenta, incendio, huracán, pandemia o cualquier otro desastre, nuestra preocupación inmediata es la seguridad de nuestros empleados. Revisamos y tomamos en consideración los planes emitidos por las autoridades de protección civil y de salud que describen cómo recuperarse de un desastre natural o una ola pandémica. Una vez que tomamos medidas para proteger a nuestros empleados, identificaremos el alcance del incidente. Si la emergencia parece afectar a un centro de datos importante o servicio crítico, o si el acceso a una instalación crítica de la Empresa está prohibido, un Funcionario de la Empresa declarará un desastre, iniciando los procedimientos de recuperación. Una vez que se permita el acceso a la instalación, se realizará una evaluación de daños para determinar la duración estimada del corte. Si se previene el acceso a la instalación, entonces la estimación debe incluir el tiempo hasta que se pueda evaluar el efecto del desastre en la instalación.

5. Comunicación alternativa.

5.1. Podemos usar una amplia gama de sistemas de comunicación para comunicarnos con nuestros Clientes, empleados, contrapartes y reguladores, incluyendo, pero no limitado a: teléfono, correo postal, correo electrónico, publicar un mensaje en nuestro sitio web, mensajería instantánea, nuestro sitio web y reuniones personales. En un escenario de desastre donde uno de nuestros centros de datos no esté disponible, los sistemas de comunicación de centro de datos alternativos están en su lugar.

6. Ubicación operativa temporal.

6.1. Nuestros empleados están equipados para trabajar desde casa en caso de que una instalación dañada no pueda ser ingresada. En todo momento mantendremos oficinas en un sitio distinto a la oficina principal, a la cual podremos reubicar temporalmente a nuestros empleados.

7. Evaluaciones financieras y operativas.

7.1. Hemos establecido procedimientos ante la exposición al riesgo operativo, financiero y de crédito en caso de una interrupción significativa del negocio; los procedimientos son los siguientes:

- Riesgo operativo: En caso de una interrupción significativa del negocio, realizaremos una evaluación de la situación y estableceremos qué sistema de comunicación será más efectivo para comunicarnos con nuestros Clientes y componentes críticos del negocio.

- Riesgo financiero y de crédito: En caso de una interrupción significativa del negocio, realizaremos una evaluación de nuestra condición financiera para determinar las medidas apropiadas. La determinación se basará en:

  - Impacto de la interrupción en la conducción del negocio.
  - Estado actual del capital y la capacidad para cumplir con los requisitos del negocio.
  - Capacidad para saldar responsabilidades con nuestras contrapartes.
  - Contactar a bancos y otras contrapartes para asegurar financiamiento si es necesario.

7.2. Una interrupción que afecte la capacidad para conducir el negocio puede ocurrir en nuestra empresa o en un tercero. Un tercero crítico puede ser un miembro comercial, un banco y/o una contraparte. Antes de entrar en una relación comercial con cualquier tercero, nos aseguraremos de que tal parte tenga un plan de continuidad del negocio.

8. Acceso a fondos y valores.

8.1. En caso de que el acceso del Cliente a fondos y valores se vea afectado por una interrupción significativa del negocio, los Clientes serán notificados por cualquier medio disponible.

9. Regulación.

9.1. Si hay una interrupción significativa del negocio que afecte a las oficinas de reporte y reportes regulatorios, la empresa contactará a los reguladores para discutir alternativas de presentación disponibles para cumplir con los requisitos de reporte.

10. Actualización y revisión anual.

10.1. La Empresa actualizará este Plan siempre que haya un cambio material en las operaciones, negocio o ubicación o contrapartes de servicios críticos. Además, la empresa actualizará el Plan, al menos anualmente (si se requiere), para asegurar que el plan se mantenga consistente con sus operaciones generales de negocio.