

Plan de Continuidad de Negocio

Cuando hablamos de Plan de Continuidad de Negocio (PCN), estamos hablando de lo que debemos hacer para asegurar la supervivencia de una empresa o institución en caso de que ésta se viera sometida a una interrupción no deseada de su negocio o funcionamiento.

Para dar una idea de su importancia, citaremos las siguientes cifras del Emergency Management Forum (Estados Unidos): De cada 100 empresas que afrontan un desastre sin contar con un PCN: 43% nunca reabren el negocio, 51% sobrevive, pero están fuera del mercado en 2 años y sólo el 6% logra sobrevivir a largo plazo.

Aún teniendo controles y medidas de salvaguarda implantadas, siempre existe el riesgo de que la continuidad del negocio se interrumpa debido a la materialización de una o varias amenazas, ocasionando pérdidas más o menos nefastas para la empresa o institución.

Cuando se produce esta interrupción la mejor forma de minimizar los efectos dañinos es disponer de un Plan de Continuidad del Negocio y aplicarlo de forma inmediata y controlada. Su implantación nos permite hacer que el negocio siga ofreciendo sus servicios, bien de forma completa o bien con unos mínimos de garantía.

Análisis y Clasificación de los Procesos del Negocio

Lo primero que se debe realizar es un Análisis de Impacto en el Negocio (BIA). Éste es básicamente un informe que nos muestra el coste ocasionado por la interrupción de los procesos de negocio.

Una vez obtenido este informe, la compañía tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial).

Es ese sentido **ESA Security** dispone de una metodología propietaria de recolección de información que permite obtenerla de una forma rápida y eficaz. Gracias a este sistema podemos adaptarnos tanto a grandes compañías como a pymes con una misma metodología.

Plan de Continuidad de Negocio

Un Plan de Continuidad de Negocio (PCN) se puede considerar como un repositorio que recoge toda la gestión necesaria para la ejecución, mantenimiento, pruebas, etc de todas las acciones a tomar para recuperar la continuidad del negocio después de una interrupción.

En este sentido, en un PCN se afrontarán, entre otros, los siguientes aspectos o temas: Los procesos críticos para el

negocio, las personas responsables de los procesos y activos, el personal implicado en el PCN, el proceso de alerta y activación del PCN y los procesos de prueba y mantenimiento.

El objetivo es que los servicios o procesos del negocio vuelvan al estado normal de producción que tenían antes de la interrupción. Estos planes de respuesta y respaldo se gestionan mediante planes de contingencias.

Planes de Contingencia

Un plan de contingencia es la parte práctica del PCN. Consiste en los pasos que el personal debe realizar (de acuerdo con las directrices del PCN) para hacer frente a las situaciones inesperadas que pueden afectar a la continuidad de su negocio. Puesto que el tiempo es un factor crucial en las situaciones de emergencia, se hace necesario disponer de planes de respaldo que permitan una rápida reacción ante cualquier incidencia producida por hackers, virus, desastres naturales, caídas de redes, etc.

En el caso específico de un plan de contingencia, se estudia no sólo los sistemas informáticos, sino también la integración de los mismos con su modelo de negocio y desarrollamos las situaciones hipotéticas que pudieran afectar

a la continuidad del servicio de los sistemas informáticos. También elaboramos planes específicos que permitan una recuperación lo más rápida posible para los escenarios previstos.

Beneficios

- Reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar pérdidas ingentes de capital, bien por facturación fallida, por reposición de los daños causados, por pérdida de oportunidad de negocio, por reclamación de clientes, por sanciones legales, etc.
- Ahorro de tiempo y dinero al afrontar y

corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio.

- Mejora de la imagen y revalorización de la confianza en la empresa de los accionistas, inversores, empleados, proveedores y clientes al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.

Sobre ESA Security

ESA Security es una consultora especializada únicamente en la Seguridad de la Información que ha realizado con éxito la preparación de empresas para que consigan su Certificación ISO 27001,

además de haber obtenido su propia certificación en gestión de Seguridad de la Información.

Sus profesionales están altamente cualificados, incluyendo certificaciones CISA y CISM, y lo más importante: con la experiencia práctica de haber conseguido Certificaciones ISO y haber realizado en múltiples ocasiones Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis y Gestión de Riesgos, Proyectos de Hacking Ético, Formación en Seguridad, Adecuaciones y Auditorías LOPD y servicios relativos a la Seguridad de la Información en general.