Planes de Contingencia de TI

Asegurar la disponibilidad

www.abast.es

A medida que las organizaciones dependen más y más de la tecnología, que se ha convertido en un componente clave de la mayor parte de los procesos de negocio, la disponibilidad de los servicios de TI es imprescindible para su supervivencia. Esta disponibilidad se consigue mediante la definición e implementación de un Plan de Contingencia cuyo objetivo consiste en garantizar que se puede recuperar la infraestructura de TI que soporta dichos servicios dentro de los plazos y con el nivel de servicio acordado y necesario para el negocio.

Beneficios

1. 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.

2. 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.

3. 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.

Retorno de la inversión

Nuestra metodología tiene como objetivo principal ayudar a la organización a garantizar que se implementan las medidas y estrategias de recuperación que el negocio realmente necesita y puede permitirse.

Es fundamental, por tanto, entender que significa para el negocio la no disponibilidad de sus sistemas y realizar las acciones y planes necesarios para evitar que ocurra. La clave para lograr esta comprensión es la calificación (la validación con el negocio) de lo que significa realmente el tiempo de inactividad y, a continuación, la cuantificación (medición) de las consecuencias para el negocio. Se trata, por tanto, de estimar el coste de mejorar la infraestructura de TI actual frente a las pérdidas por no disponibilidad.

¿Por qué ABAST?

La realización de planes de contingencia necesita, además de un componente metodológico o procedimental, un fuerte componente tecnológico. Cuando un cliente aborda un proyecto de plan de contingencia con nosotros, toda nuestra organización trabaja para usted. Nuestro equipo de consultores coordina el resto de nuestros departamentos técnicos especializados que participarán en el análisis de su infraestructura tecnológica actual.

Nuestros consultores y técnicos están altamente cualificados y certificados en diversas metodologías y productos con el compromiso de ofrecer a sus clientes la máxima calidad en sus proyectos.

Nuestra metodología

1. Análisis de impacto en el negocio. Consiste en identificar los procesos más críticos del negocio, los servicios de TI que los soportan, determinar el impacto si uno o varios de estos servicios de TI se ven afectados total o parcialmente y definir los requerimientos de recuperación establecidos por el negocio (tiempo máximo de interrupción y máxima pérdida de datos permitida).

2. Análisis de riesgos. Consiste en estimar el riesgo potencial al que están sometidos los sistemas de TI, evaluando el impacto asociado a la materialización de una amenaza, y definir aquellas recomendaciones o controles preventivos que permitan reducir o eliminar dicho riesgo.

3. Definición de las estrategias de recuperación. Consiste en establecer los escenarios de recuperación en función de las amenazas determinadas en el análisis de riesgos y los requerimientos de negocio definidos en el análisis de impacto.

   En esta fase se definirá el escenario tecnológico óptimo para soportar los procesos de negocio, atendiendo a las disponibilidades del servicio.

4. Desarrollo e implementación del Plan de Contingencia. Una vez definida la estrategia de recuperación, el plan debe definir y establecer aquellos procedimientos, manuales técnicos y checklists funcionales que permitan restaurar los servicios de TI (sistemas, operaciones y datos) después de una emergencia o afectación total o parcial de estos servicios. La implementación del plan consiste en la ejecución de las recomendaciones establecidas en el análisis de riesgos y el escenario tecnológico definido.

5. Prueba y mantenimiento del plan. Las pruebas del plan son esenciales para identificar las deficiencias de planificación y preparación del personal. Además, el plan debe ser un documento vivo que se actualiza periódicamente para mantenerse al día con los cambios en los sistemas de TI.

CYBALL. Servicios de seguridad global de Abast

ABAST ofrece una amplia oferta de servicios y soluciones para dar respuesta a sus necesidades en ciberseguridad y seguridad del negocio. Las estructuramos en 4 capas:

GOBIERNO: Alineación estratégica seguridad/negocio. Tratamiento del riesgo. Análisis coste/beneficio. Medición madurez de la seguridad.

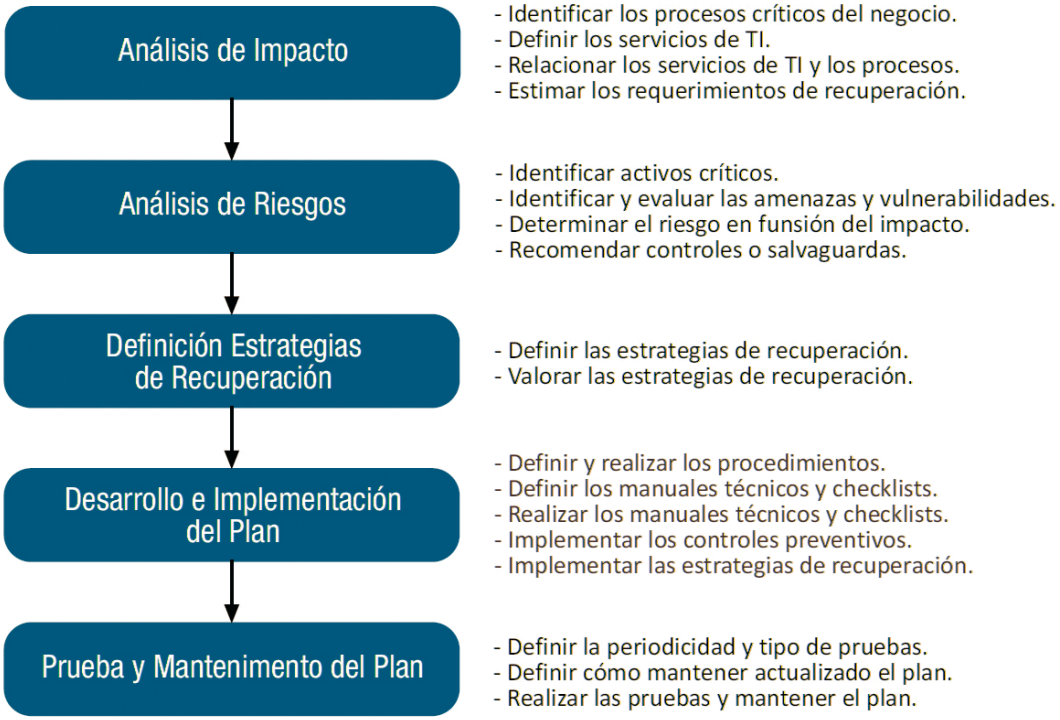
GESTIÓN: Auditorías de Seguridad. Continuidad de negocio. Cumplimiento normativo/legal. Gestión de crisis y de incidencias. Formación y concienciación.

OPERACIONES (SOC/MDR): Monitorización de la Seguridad 24x7. Detección de Amenazas e incidentes. Prevención de brechas. Respuesta a los incidentes.

INFRAESTRUCTURA: Asesoramiento e implantación de infraestructura/soluciones de seguridad TI. Administración de la seguridad TI.

abast cyball 360°

Fases de un plan de contingencia de TI



Para más información:
seguridad@abast.es

abast
www.abast.es · info@abast.es

Tel. 933 666 900
Fax 933 666 910
Carrer Equador 39-45
08029 Barcelona

Tel. 914 061 601
Fax 914 061 604
Calle de la Basílica 19, 9° B
28020 Madrid

Tel. 97 170 68 82
Calle Fluviá 1, Bajos dcha.
Despacho 25 (Son Fuster)
07009 Palma de Mallorca