Administración de Recursos
Glosario de Conceptos de IT

Plan de Contingencia

Dentro de la seguridad informática se denomina **plan de contingencia** (también de recuperación de desastres o de continuación de negocios), a la definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización. Es decir, es la determinación precisa del quién, qué, cómo, cuándo y dónde realizar acciones en caso de producirse una anomalía en el sistema de información.

El plan de contingencia debe considerar todos los componentes del sistema: Datos críticos, equipo lógico de base, aplicaciones, equipos físicos y de comunicaciones, documentación y personal. Además, debe contemplar también todos los recursos auxiliares, sin los cuales el funcionamiento de los sistemas podría verse seriamente comprometido: suministro de potencia; sistemas de climatización; instalaciones; etc. Finalmente, debe prever también la carencia de personal cualificado (por ejemplo, por una huelga que impida el acceso del mismo) para el correcto funcionamiento del sistema. Se debe destacar, que previo al comienzo del trabajo, se debe obtener el pleno compromiso de los máximos responsables de la organización. Sin su apoyo decidido y constante, el fracaso del plan está garantizado.

El plan de contingencias debe ser comprobado de forma periódica para detectar y eliminar problemas. La manera más efectiva de comprobar si funciona correctamente, es programar simulaciones de desastres. Los resultados obtenidos deben ser cuidadosamente revisados, y son la clave para identificar posibles defectos en el plan de contingencia. Además el plan de contingencia debe contemplar los planes de emergencia, resguardo, recuperación, comprobación mediante simulaciones y mantenimiento del mismo.

Un plan de contingencia adecuado debe ayudar a las empresas a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio, minimizando el impacto o pérdida a causa del incidente.

El plan de contingencias comprende tres subplanes. Cada plan determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza:

- El **plan de prevención**. Contempla las contramedidas preventivas **antes** de que se materialice una amenaza. Su finalidad es contar con las medidas necesarias para que en caso de materialización del riesgo se pueda restituir el servicio. Ej: contar con repuestos, equipos sustitutos, datos de resguardo.
- El **plan de emergencia**.[1] Contempla las contramedidas necesarias **durante** la materialización de una amenaza, o inmediatamente después. Su finalidad es **paliar** los efectos adversos de la amenaza.
- El **plan de recuperación**. Contempla las medidas necesarias **después** de materializada y controlada la amenaza. Su finalidad es **restaurar** el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Por otra parte, el plan de contingencias no debe limitarse a estas medidas organizativas. También debe expresar claramente:

- Qué recursos materiales son necesarios.
- Qué personas están implicadas en el cumplimiento del plan.
- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.
- Qué protocolos de actuación deben seguir y cómo son.

Fuentes:

https://www.ecured.cu/Plan_de_contingencia_en_seguridad_Inform%C3%A1tica

https://es.wikipedia.org/wiki/Plan_de_contingencias

http://www.forodeseguridad.com/artic/discipl/4132.htm