ANÁLISIS DE RIESGOS (AR)

Un Análisis de Riesgos (AR) es un proceso de evaluación que permite identificar eventos que podrían afectar negativamente a la organización. Esto incluye la determinación de amenazas, vulnerabilidades y los posibles riesgos, así como el tiempo necesario para recuperar o restaurar las operaciones. Una evaluación de riesgos también ayudará a determinar qué pasos podrían reducir la gravedad de un evento mediante planes de acción, así como las medidas preventivas y controles que pueden mitigar la probabilidad de que ocurra un evento.

La aplicación de una metodología de AR permite la reducción de aquellos riesgos que, en caso de materializarse las amenazas que los originan, puedan representar interrupciones y pérdidas significativas de servicio que impliquen importantes esfuerzos en la reposición de los daños, pérdida de imagen y credibilidad de los usuarios.

FASES DE UN ANÁLISIS DE RIESGO:

- Delimitación del contexto del análisis.
- Evaluación de los riesgos, definición de controles y los riesgos residuales.
- Establecimientos de planes de acción.
- Redacción del informe.

El contexto del riesgo se sustenta en los procesos de negocio donde se desarrollará el AR, estableciendo el inventario de recursos y servicios, derivado a partir de las amenazas y vulnerabilidades asociadas a los riesgos mitigados por un control (riesgo residual). El análisis de riesgo evalúa la probabilidad de que ocurra un evento y define la gravedad de sus consecuencias, en las que la organización puede estar arriesgándo su información o infraestructura al no realizar ciertas actividades. Un ejemplo puede ser un mayor riesgo de virus al no usar el software antivirus más reciente. Se debe recopilar información sobre posibles amenazas para la organización.

UCR

La implementación de controles y planes de acción depende en gran medida de los resultados de la evaluación de riesgos. Después de identificar una amenaza específica y su vulnerabilidad asociada, se planifica la estrategia defensiva más efectiva. Posteriormente, el proceso metodológico continúa con la calificación de los riesgos mediante su impacto para obtener el riesgo absoluto, estableciendo controles para manejar el riesgo (riesgo residual). Los controles y planes de acción necesarios ayudarán a minimizar la materialización del riesgo. De esta forma, con los riesgos residuales de impacto extremo o mayor se definen los planes de acción de mitigación y contingencia.

Los planes de mitigación están diseñados para minimizar la gravedad del evento previo a su ocurrencia. Los ejemplos de medidas de mitigación incluyen supresores de sobretensiones para reducir el impacto de un rayo y sistemas de energía ininterrumpida, para limitar las posibilidades de una detención estricta de los sistemas críticos en caso de un apagón o caída de voltaje. Los planes de contingencia contienen las actividades de recuperación necesarias para restablecer los sistemas y la infraestructura alterados a un nivel que pueda respaldar las operaciones de negocio. Por ejemplo, los datos críticos almacenados fuera del sitio se pueden usar para reiniciar las operaciones en un punto apropiado en el tiempo. Los planes de contingencia deben hacer frente a los efectos, independientemente de las causas.

Los AR buscan que la organización pueda estimar el riesgo potencial al que están sometidos los sistemas e infraestructura de TI, evaluando el impacto asociado con la materialización de un riesgo y definiendo aquellas recomendaciones o controles preventivos que permiten reducir o eliminar el impacto. Los resultados del análisis de riesgos deben resumirse en un informe que contenga las actividades de control y planes de acción recomendadas.

Los análisis de riesgos constituyen un esfuerzo para apalancar la confianza de la organización y su imagen, al demostrar que se toman las medidas preventivas y correctivas para garantizar operaciones con el mejor nivel de continuidad.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de
Informática