Análisis de Riesgos

Evaluación y Tratamiento de Riesgos

El servicio de Análisis de Riesgos (RA) permite a las organizaciones identificar los eventos y las situaciones que pueden afectar de manera adversa a las áreas de negocio y sus procesos. Es por ello que evaluar la probabilidad de ocurrencia y el impacto (consecuencias) de estos eventos en la organización, es de suma importancia, ya que con ello se pueden identificar controles aplicables que permitan minimizar la probabilidad de ocurrencia, mitigando de esta manera el riesgo existente a un nivel aceptable.

Objetivos del Servicio

Realizar una evaluación de riesgos sobre activos de información asociados con el alcance del proyecto, con el fin de identificar sus amenazas y vulnerabilidades a las cuales se ven afectados, para luego verificar la existencia de controles y su nivel de efectividad para mitigar eventuales riesgos. Para aquellos activos que poseen un nivel de riesgo por sobre el aceptable, se propone un Plan de Tratamiento de Riesgos, el cual propone la mejora o adición de controles que permitan reducir dicho riesgo a un nivel aceptable. Para ello se utilizarán los controles establecidos por las siguientes normas internacionales:

- **ISO/IEC 27002:2013**, Information technology, Security techniques, Code of practice for information security controls
- **CCM V3.0.1**, Cloud Security Alliance, Cloud Controls Matrix.
- **AS-8001:2008**, Australian Standard, Fraud and Corruption Control.

La metodología utilizada para el análisis y evaluación de riesgos está definida por las normas internacionales especializadas para tal fin, las cuales nos entregan las directrices necesarias para enfrentar el proceso de consultoría en la organización:

- **ISO 31000:2009,** Risk management, Principles and guidelines.
- **ISO/IEC 27005:2008,** Information technology, Security techniques, Information security risk management.

Descripción del Servicio

El Análisis de Riesgos es fundamental para identificar los controles existentes y las brechas de seguridad con las cuales cuenta la organización, pero adicionalmente nos entrega información estratégica de importancia para la toma de decisiones de la alta dirección:

- Valorización e identificación de los activos de información en relación con su importancia para los procesos de negocio de la organización.
- Poseer un Plan de Tratamiento de Riesgos (PTR) que contenga una estructura y resultados adecuados que permitan cumplir con los requisitos establecidos por distintos Sistemas de Gestión (ISO 27001, ISO 20000, ISO 22301, etc.).
- Identificar las distintas amenazas y vulnerabilidades de los activos críticos de la organización que pueden implicar un impacto considerable si los riesgos que les afectan se materializan, para lo cual es necesario aplicar controles que permitan mitigarlos.

Proceso de Consultoría

Planificación: Se conforma el Comité de Seguimiento del proyecto y se levanta la documentación e información (activos, manuales, normativas, procedimientos, etc.) necesaria para realizar los análisis correspondientes.

Levantamiento de Procesos: Se realiza un levantamiento y análisis de los procesos y subprocesos que componen las áreas de negocio asociadas con el alcance del proyecto, con el fin de identificar los activos involucrados y su importancia.

Evaluación de Riesgos: Se realiza un análisis de las distintas amenazas y vulnerabilidades que afectan a los activos identificados, así como también se evalúan los controles actuales existentes en la organización, con el fin de determinar el nivel de riesgo actual de dichos activos.

Propuesta del Plan de Tratamiento de Riesgos: Se realiza un plan que propone controles adicionales o la modificación de los existentes, con el fin de mitigar los riesgos que fueron identificados durante las fases de análisis.

contacto@forensiccorp.cl
www.forensiccorp.cl