



“Análisis de Arquitectura y Seguridad de Redes Corporativas”





Descripción

La finalidad del presente trabajo, es verificar que la actual topología de Red de comunicaciones y sistemas de su empresa, en cuanto a su diseño y distribución, posea los elementos necesarios que permitan asegurar en buena medida, la seguridad y disponibilidad de la información que por ahí se procesa y transmite. Algunas de las características que deben ser visibles en La Arquitectura de son; alta disponibilidad (enlaces, equipos de comunicaciones, rutas, entre otros) y confidencialidad de la información (segregación de ambientes productivos en forma virtual o física).



A quien esta dirigido ...

- Todos aquellos que necesitan asegurar la confiabilidad y estabilidad de su sistema.
- Aquellos que necesitan identificar las áreas desprotegidas
- Aquellos que buscan evaluar el sistema de Seguridad implementado
- Aquellos que nunca han realizado un penetration Testing



Razones para su Implementación

- Debido a que es un proceso destinado a determinar los niveles de seguridad y estabilidad del actual sistema utilizado dentro de la empresa, frente a ataques y/o intrusiones.



Beneficios

- **Desarrollo de nuevas políticas de Seguridad**
- **Identificación de Áreas desprotegidas**
- **Verificar la Integridad del esquema del sistema de Seguridad**
- **Priorizar Problemas evidenciados**
- **Justificar Presupuesto de Seguridad**



Fases del Análisis

Levantamiento:

El levantamiento contempla la recopilación de la información de la infraestructura tecnológica a nivel físico y lógico, trabajo que otorgará claridad sobre el análisis de la arquitectura.



Evaluación Topológica:

La evaluación topológica contempla una revisión detallada del diseño de la arquitectura en donde se pueda visualizar riesgos inherentes al negocio, su funcionalidad y respuesta esperada a los distintos servicios de redes y sistemas según las necesidades del negocio.



Fases del Análisis

Evaluación de Seguridad:

La evaluación de seguridad contempla una revisión en profundidad de vulnerabilidades en los distintos componentes de sistemas, ya sean, servidores, equipos de comunicación, plataformas PC, accesos a Internet, sistemas de control de virus, cortafuegos, entre otros. Esta parte de la evaluación considera emular ataques externos e internos evidenciando los riesgos en seguridad de acceso a las redes y sistemas ya sea por agentes externos o usuarios internos. La evaluación de seguridad también considera el cumplimiento y revisión de las políticas de seguridad de la información de la empresa y las regulaciones locales vigentes.



Fases del Análisis

Informes y Resultados:

El resultado del Análisis de Arquitectura de Red se traduce en un informe ejecutivo en donde se detallarán las actividades desarrolladas en el proceso, conclusiones y recomendaciones. Además un informe técnico detallando el resultado de cada prueba en donde se argumentarán los puntos eficientes de la plataforma y las vulnerabilidades con sus consiguientes riesgos.



Resultados

En base a un estudio de la arquitectura de red, se pueden identificar a nivel lógico y físico las debilidades del diseño y componentes físicos así como la inexistencia de ciertos equipos, tales como, cortafuegos (firewall), elementos de seguridad (IDS, IPS, entre otros), además de velar por el concepto de defensa en profundidad, alta disponibilidad y segmentación de acuerdo al nivel de criticidad de servicios que la red debiese tener.