Importancia de las Consultorías de Seguridad

Facilitador: Carlos Mujica

JULIO 2022

¿En qué consiste la Consultoría de Seguridad?

1.- ¿Qué es Consultoría de Seguridad?

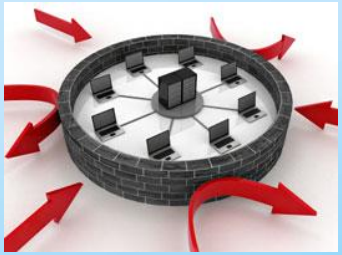
Es el servicio de seguridad a través del cual se pone a disposición el conocimiento, especialización y actualización en materia de seguridad de la información, con el fin de analizar y asesorar los controles y mecanismos de seguridad de la información a implantarse en los requerimientos y proyectos tecnológicos de una empresa.

¿En qué consiste la Consultoría de Seguridad?

Opción 1: Un montón de documentos (Informes de Consultorías de Seguridad) donde se estipulan controles y mecanismos de seguridad que no son implementados en la Plataforma Tecnológica de las empresas y a la final es letra muerta.

Ó

Opción 2: La implementación de los controles y mecanismos de seguridad estipulados en los Informes de Consultorías de Seguridad en la Plataforma Tecnológica de las empresas en pro de disminuir los riesgos ante eventuales ataques de seguridad.



¿*Importancia de una* Consultoría de Seguridad?

❖ Determinar las necesidades de seguridad del proyecto/requerimiento en pro de disminuir los riesgos ante eventuales ataques de seguridad, garantizar la continuidad operacional e implementar nuevos controles de seguridad si fuese necesario, basada en la norma ISO 27001:2013 y la ISO 27002.

¿Por qué contratar a un Consultor de Seguridad?

- **Es un asesor en materia de Seguridad de Información para los nuevos proyectos tecnológicos.**
- **Te realizará un informe que indica los correctos controles y mecanismos de seguridad en base al marco normativo y mejores prácticas en una empresa, basado en la norma internacional ISO 27001 y 27002.**
- **Garantizando que al aplicar estos controles de seguridad minimiza los riesgos tecnológicos en la plataforma.**
- **Apoya en garantizar tu continuidad operacional.**

Valoración del activo de información

Consiste en estimar el valor e importancia que tiene el activo de información para la organización.

Adicional al valor adquisitivo, es la importancia de lo que contiene (en este caso lo que representa el pasajero)

Carro familiar

- **Alarma**
- **Sensor de aproximación**
- **GPS (localizar reactivo)**

Carro de un gobernador

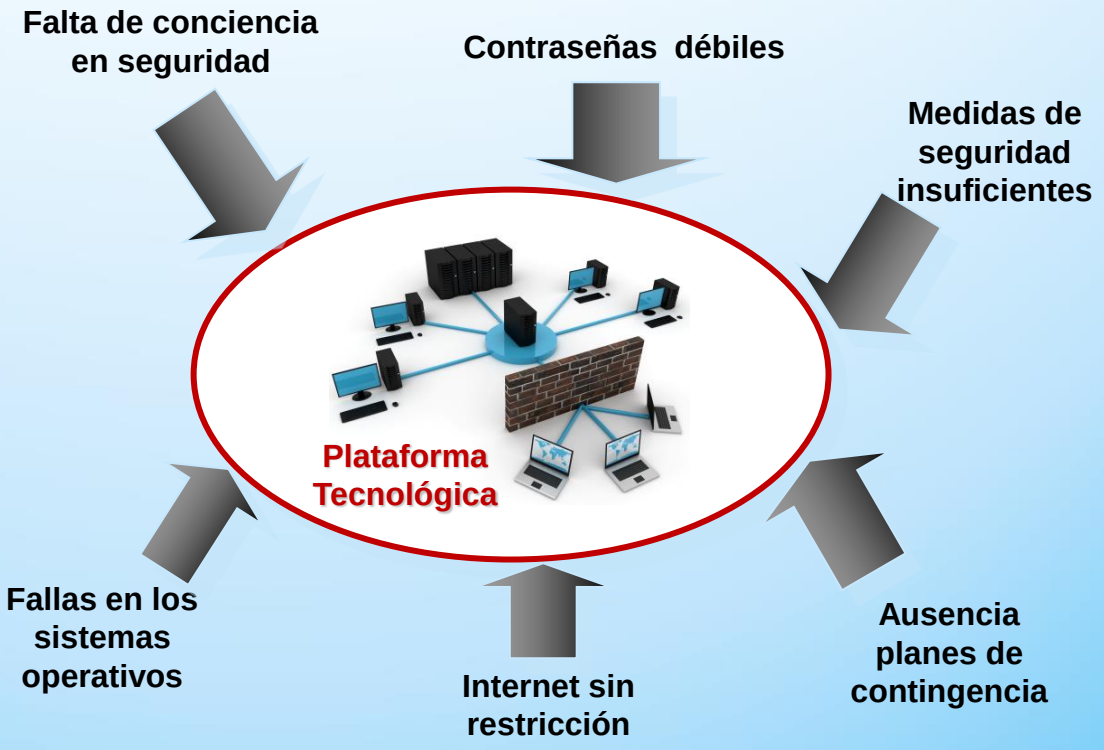
Amenazas

Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Vulnerabilidades

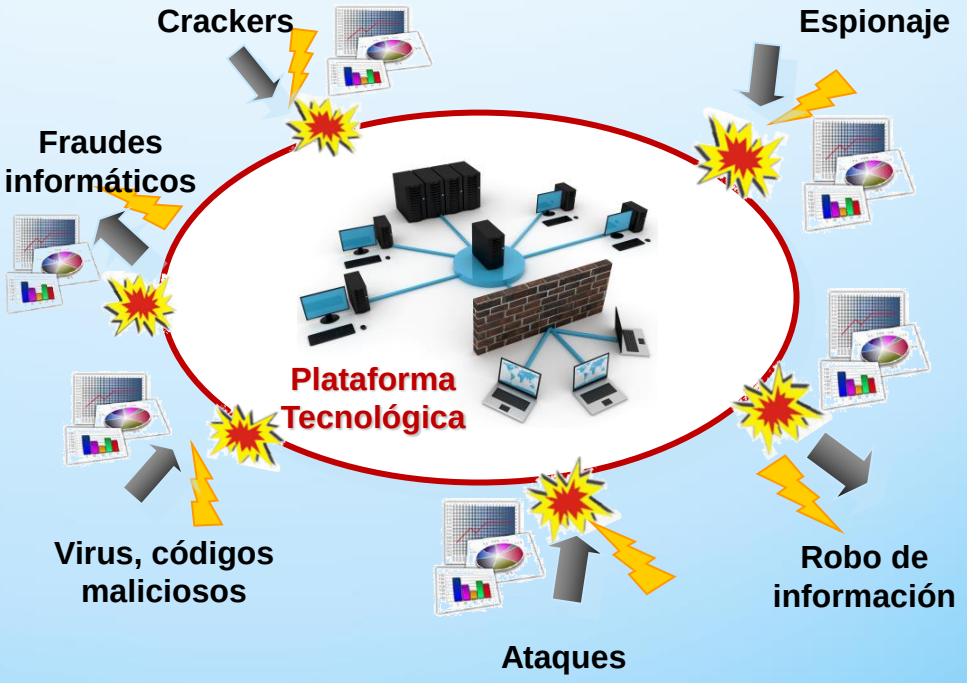
Debilidad de un activo o grupo de activos, que pueden ser aprovechados por una o más amenazas.

Son puntos débiles del activo de información que permiten que un atacante o usuario mal intencionado pueda comprometer la integridad, disponibilidad o confidencialidad del mismo.



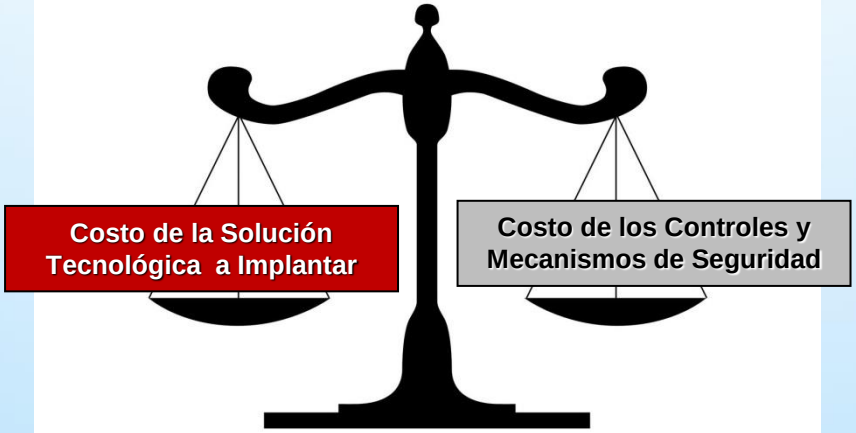
Riesgos

Es la probabilidad que una amenaza dada aproveche una vulnerabilidad para dañar uno o un grupo de activo de información, pudiendo extenderse a toda la organización.



2.- ¿Qué se persigue con la Consultoría de Seguridad?

❖ Hacer el balance entre el costo de los controles y mecanismos de seguridad y el costo de la solución tecnológica a implantar, a fin de que no sean más caro los controles y mecanismos de seguridad que el valor de la solución.

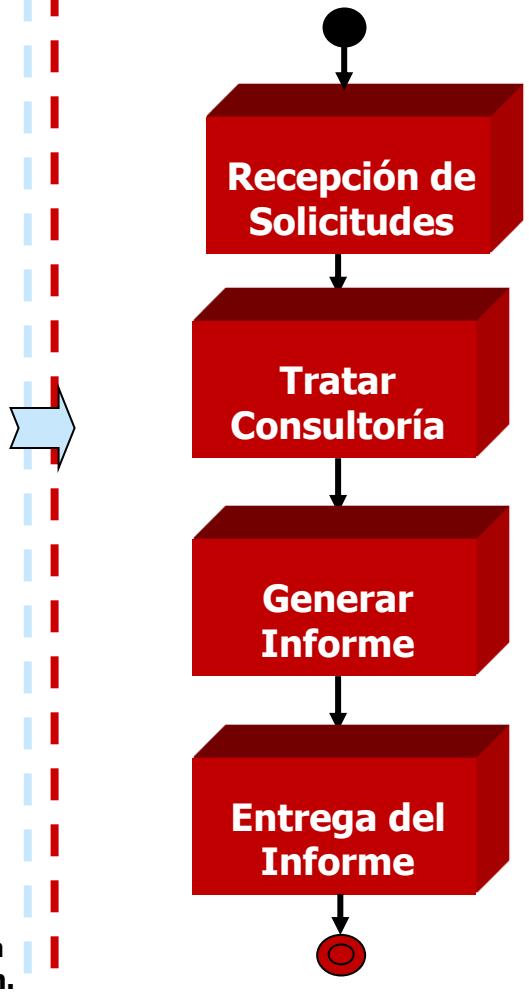


Toda solución tecnológica debe tener los controles y mecanismos de seguridad mínimos para su puesta en producción.

Proceso de Consultoría de Seguridad

ENTRADAS

- Solicitud de Consultoría de Seguridad (Proyectos/Procesos/Actividades que involucren activos de información)
- Cartera de Proyectos TI / Proyectos de Seguridad en Tecnologías de Información
- Norma de Protección de Activos de Información
- Políticas de Seguridad de Información
- Lineamientos de Seguridad
- Procedimientos de Seguridad
- Lista de Chequeos /Boletines de Seguridad
- Marco legal vigente en materia de Tecnológica de Información
- Base de Conocimiento de Consultoría de Seguridad
- Información adicional sobre el proyecto/proceso/actividad (Minuta, Presentaciones, entre otros).
- Mejores Prácticas en materia de Tecnología de Información y Seguridad de Información. (ISO 27002)

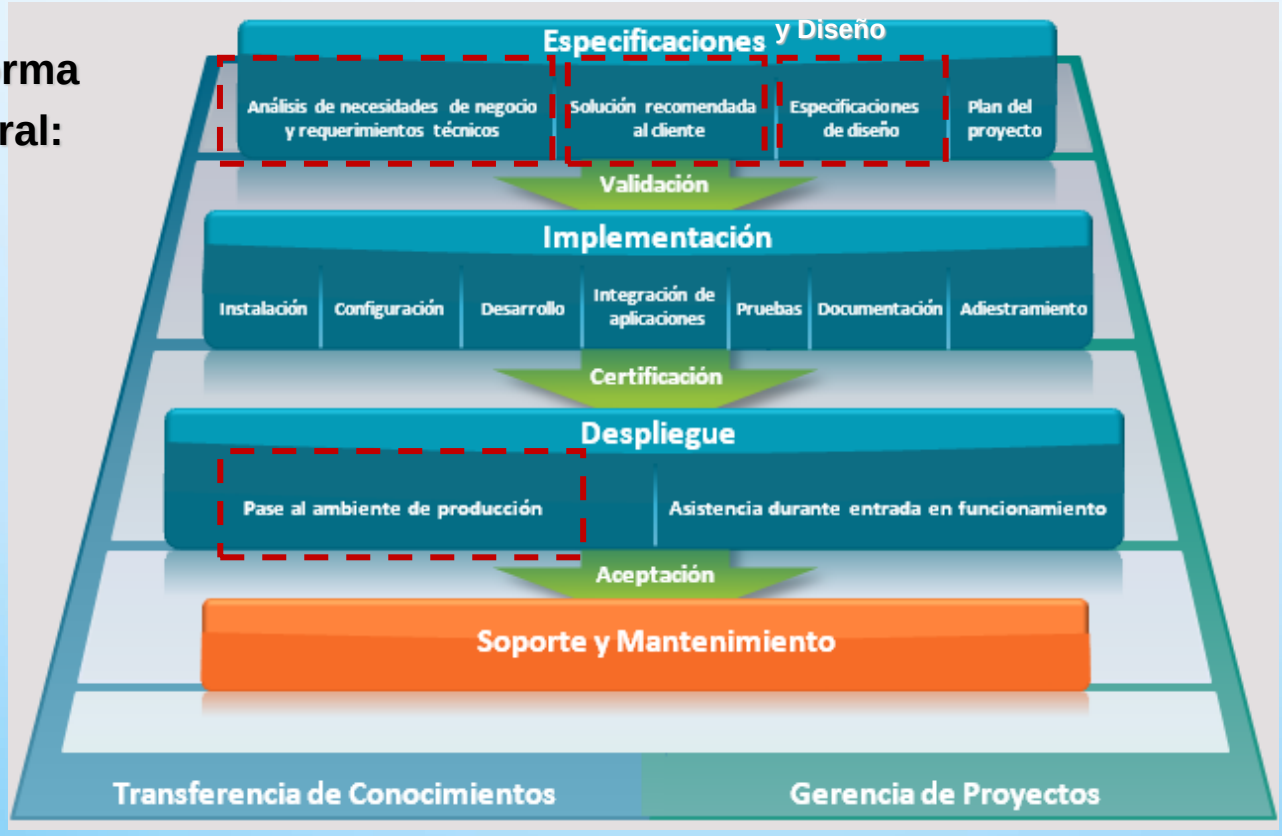


SALIDAS

- Informe de Consultoría de Seguridad
- Solicitud de Actualización/Emisión de Políticas, Normativas y Lineamientos de Seguridad.
- Reporte Mensual de Consultorías de Seguridad realizadas
- Estadísticas/Estrategias
- Alimentación de la Base de Conocimiento de Seguridad
- Solicitud de Estrategia Educativa.
- Solicitud de Adiestramiento en Seguridad para los proyectos que conciernen a la Plataforma Tecnológica
- Solicitud de Cambios/Implantación sobre la Plataforma Tecnológica/Solicitud de implantación de soluciones de Seguridad

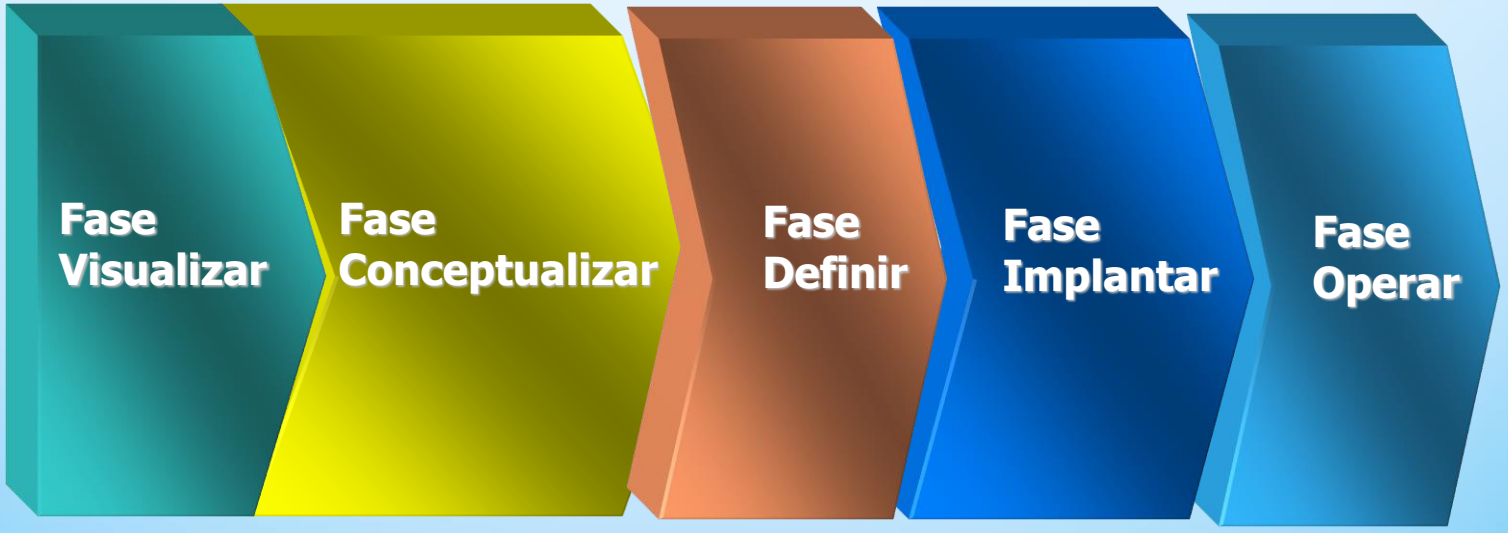
4.- En que fase entra la Consultoría de Seguridad dentro de un proyecto o requerimiento

De forma General:



En que fase entra la Consultoría de Seguridad dentro de un proyecto o requerimiento

- En base al Proyecto GGPIC (Guía de Gerencia para Proyectos de Inversiones del Capital) adaptado a Tecnología:



Controles de la ISO 27001:2013 asociados a la Consultoría de Seguridad.

- Analicemos los controles de la ISO IEC 27001:2013 asociados a la Consultoría de Seguridad.

Controles de la ISO 27001:2013 asociados a la Consultoría de Seguridad.

A.14 Adquisición, desarrollo y mantenimiento de los sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información, a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.		
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	*Control* Los requisitos relacionados con la seguridad de la información se deben incluir en los requisitos para los nuevos sistemas de información o para las mejoras a los sistemas de información existentes.

Controles de la ISO 27001:2013 asociados a la Consultoría de Seguridad.

A.6.1.5	Seguridad de la información en gestión de proyectos * **(VER LA NOTA UNIT 1)**	*Control* La seguridad de la información debe ser abordada en la gestión de proyectos, independientemente del tipo de proyecto.

Norma ISO 27001

Norma ISO 27001

Aspectos Generales:

- ✓ El estándar cuenta con **14 dominios**, **35 objetivos de control** y **114 controles**.
- ✓ Su anexo A es de carácter normativo y referencia a los objetivos de control y controles que luego son ampliados en la Norma ISO 27002.
- ✓ Los requerimientos de evaluación del riesgo consideran la implementación de la ISO 31000 y la ISO 27005.
- ✓ El estándar enfatiza el establecimiento de objetivos, monitoreo del desempeño y métricas ISO 27004.
- ✓ La estructura de la Norma lleva implícito el uso del ciclo de Mejora Continua PHVA.

Norma ISO 27001

Ciclo PHVA y documentación obligatoria

- Alcance.
- Política y Objetivos de seguridad de la información.
- Proceso de evaluación de riesgos.
- Proceso de tratamiento de riesgos
- Declaración de Aplicabilidad
- Evidencia de competencia
- Documentación necesaria para la efectividad del SGSI.

- Documentación necesaria para confiar en que los procesos requeridos para la planificación y el control operativo se han llevado a cabo según lo previsto.
- Resultado de las evaluaciones de riesgos.
- Resultado de tratamiento de riesgos.

- Evidencia de no conformidades y cualquier acción posterior tomada, y los resultados de cualquier acción correctiva.

- Evidencia de los resultados de monitoreo y medición del desempeño.
- Programa y resultados de las auditorías internas.
- Evidencia de los resultados de las revisiones de gestión.

Norma ISO 27001

***Controles**:*

- ✓ Definición de roles y responsabilidades de seguridad (7.1.2 y A.13.2.4).
- ✓ Inventario de activos (8.1.1).
- ✓ Reglas para el uso aceptable de activos (8.1.3).
- ✓ Esquema de clasificación de información (8.2.1).
- ✓ Política de control de acceso (9.1.1).
- ✓ Procedimientos operativos para la gestión de TI (12.1.1).
- ✓ Registros de actividades de usuarios, excepciones y eventos de la seguridad (12.4.1 y A12.4.3).
- ✓ Principios de ingeniería de sistemas seguros (14.2.5).
- ✓ Política de seguridad del proveedor (15.1.1).
- ✓ Procedimiento de gestión de incidentes (16.1.5).
- ✓ Procedimientos de continuidad comercial u operacional (17.1.2).
- ✓ Requisitos legales, reglamentarios y contractuales (18.1.1).

Dominios de la Norma ISO 27002 y los Niveles Organizacionales

14 dominios

35 dominios de control

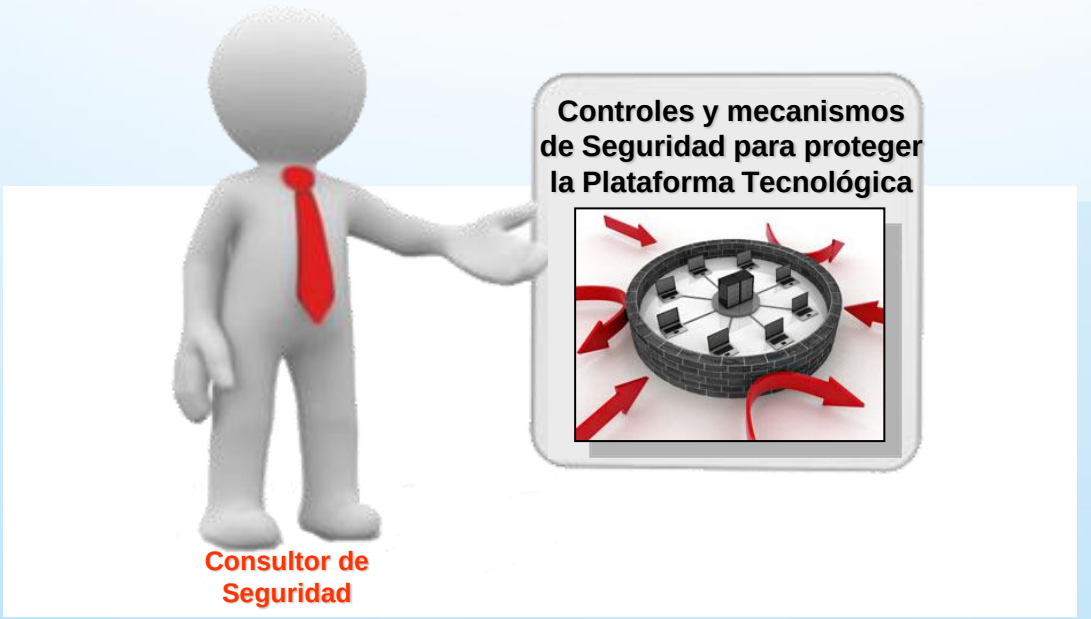
114 controles

- **Seguridad organizativa**
- **Seguridad lógica**
- **Seguridad física**
- **Seguridad legal**

Diferencia de una Diagnóstico de Seguridad versus un sevicio de Pentest

- **Diagnostico de Seguridad**
  - Recolección de datos
  - Identificación de vulnerabilidades
  - Investigación de remediaciones de las vulnerabilidades
- **Pentest (Prueba de Penetración)**
  - Recolección de datos
  - Identificación de vulnerabilidades
  - Investigación de remediaciones de las vulnerabilidades
  - Investigaciones de exploit
  - Fase de ataques a los objetivos
  - Generación de resultados exitoso y remediación de las vulnerabilidades

Fin de la Presentación



Muchas Gracias por su atención

Carlos Mujica

Celular: 0412-901.88.82