Lo que debe y no debe hacer
Un Oficial de Seguridad de la Informacion

Fredda Stanza

Julio 2018

Fredda Stanza

Information Security & Forensics Consulting

5 años de antiguedad y consultores con mas 14 años de experiencia
ofreciendo servicios de:

Information Security

Ethical Hacking
Security Audits
GAP Análisis
Aseguramiento

Forensic / Fraud

Forense Corporativo
Análisis de Fraude Electrónico
Robo información
Reverse Engineering
Code Security Analysis

Risk Management

Risk Assessment
Control Implementation
Control Testing

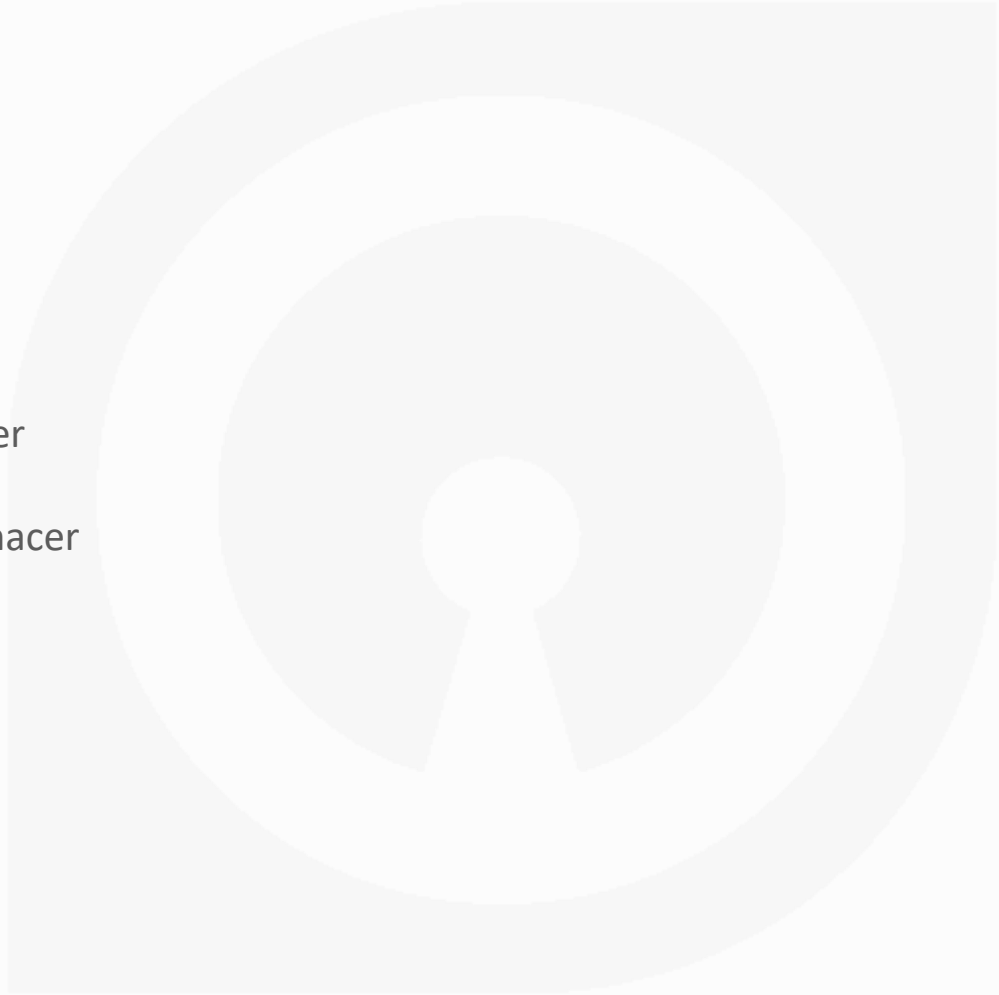
Compliance

ISO 27001
PCI-DSS
Sarbanes Oxley 404 IT
ISO 22301
BCP / DRP

Agenda

Aseguramiento

- Introducción
- Lo que debe hacer
- Lo que no debe hacer



Lo que debe hacer

Conocer el Negocio

Plan estrategico Corporativo

Plan estrategico de TI

Plan estrategico de SI

Lo que debe hacer

Conocer el Negocio

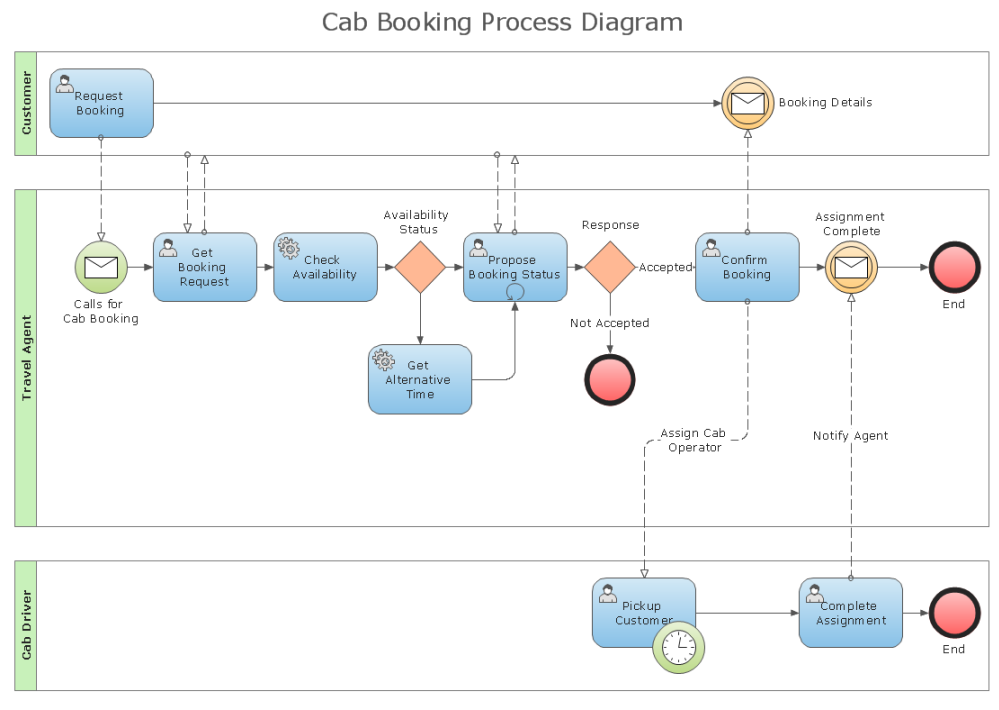
- Prioriza (ejemplo)

Prioridad	Descripción
0	Elaboración del presente Plan Estratégico de Seguridad de la Información
1	Estrategia de la Dirección de seguridad de la información: Incluye las iniciativas que soportan la implementación de la estrategia de la Oficina de seguridad de la información y apalancan su reconocimiento y posicionamiento como un área estratégica y de servicio dentro de la aseguradora.
2	Riesgos Operacionales: Hace referencia a los proyectos y actividades que mitigan los riesgos de seguridad de la información catalogados como relevantes, garantizando salvaguardar la información en su confidencialidad, disponibilidad e integridad.
3	Misional: Identifica aquellos proyectos que favorecen el cumplimiento de la estrategia y metas de la aseguradora y que soportan la gestión o ejecución de las actividades de los procesos misionales de la aseguradora.
4	Desempeño: Soportan el adecuado desempeño de las funciones de la aseguradora. No generan impactos críticos, pero es deseable contar con estas soluciones para mejorar los indicadores de gestión de algunos procesos.

Tabla 3. Criterios para priorización de proyectos

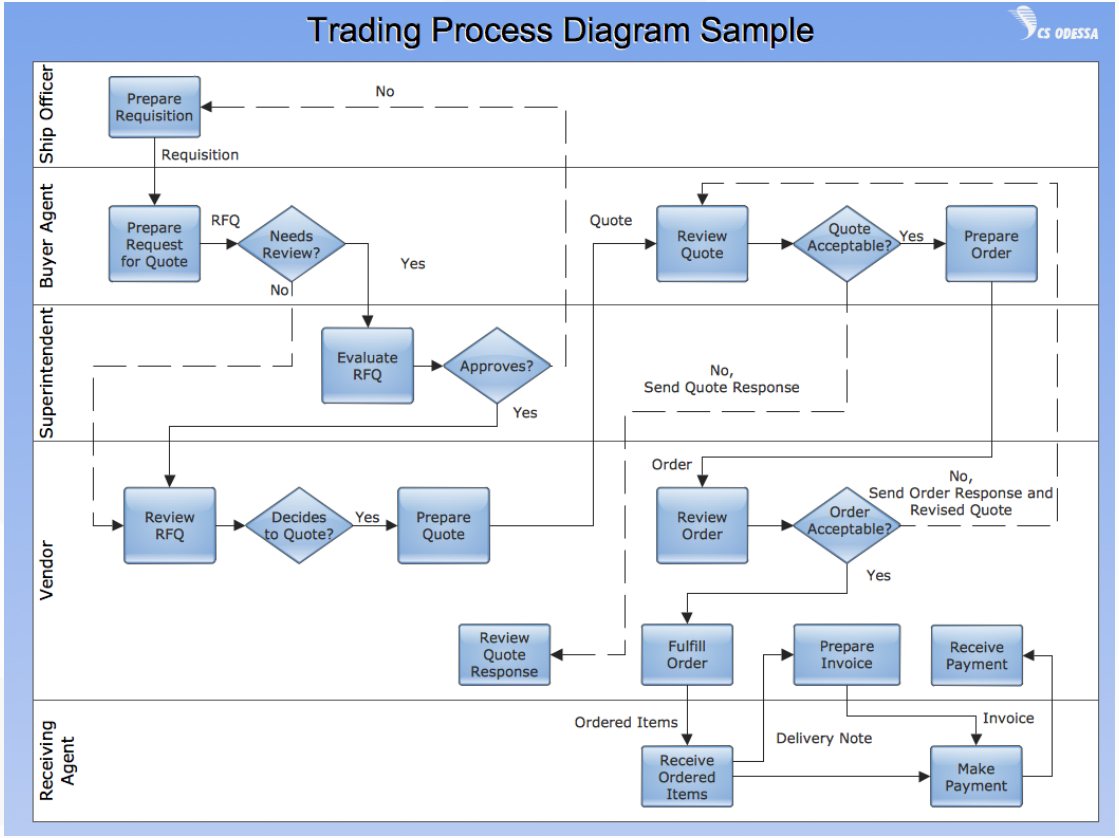
Lo que debe hacer

Conocer el Negocio



Lo que debe hacer

Conocer el Negocio



Lo que debe hacer

Conocer el Negocio

- No todos los activos, necesitan el mismo nivel de protección
- Un excesivo detalle en el analisis de Riesgo, puede no ser finalizado, entendido o percibido, los controles pueden requerir de muchos recursos.
- Con el negocio usa un lenguaje comprensible y no tecnico
- Es preciso (usa metricas de manera estandarizada y responsable)
- Valida el uso adecuado de los activos de informacion
  - Cuantos usan el correo corporativo para temas personales?
  - Se crearon reglas nuevas en el firewall?
  -
- Verifica que se cumplan los SLA y contribuye al establecimiento de estos

Lo que debe hacer

Conocer el Negocio

Entiende que no es un super heroe y transmite al negocio la necesidad de un Area de Seguridad.

Security Analyst

Security Engineer

Security Administrator

Lo que debe hacer

Conocer el Negocio

Entiende que no es un super heroe y transmite al negocio la necesidad de un Area de Seguridad.

Security Software Developer

Cryptographer/Cryptologist

Brand defender

Incident detection innovator

Security strategist

QA / Productivity expert / Process steward

Security PR / Marketing guru / Evangelist

Lo que no debe hacer

-El oficial de seguridad de la información no es un hacker

-El oficial de seguridad de la información no decide, “recomienda”

- Controles
- Tecnologia de seguridad
- Sanciones

Falta de compromiso ético y moral

“Planea” de forma improvisada

No considera la segregacion de funciones

Auditoria depende de TI para sus revisiones?

Seguridad depente de TI?

Lo que no debe hacer

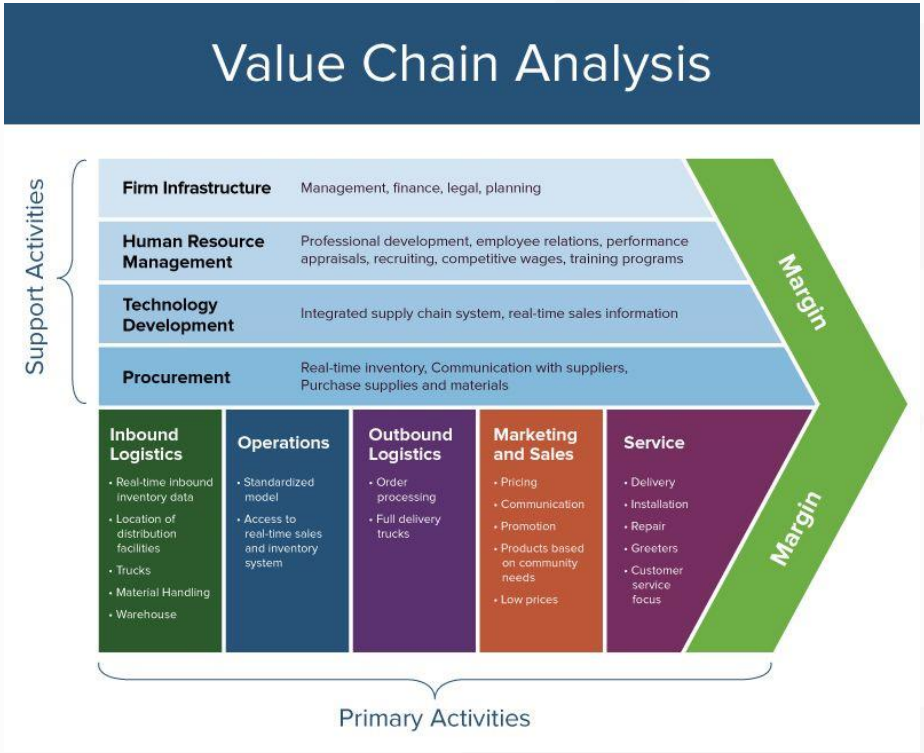
Concentrarse en Exploits (desconoce de procesos de negocio)

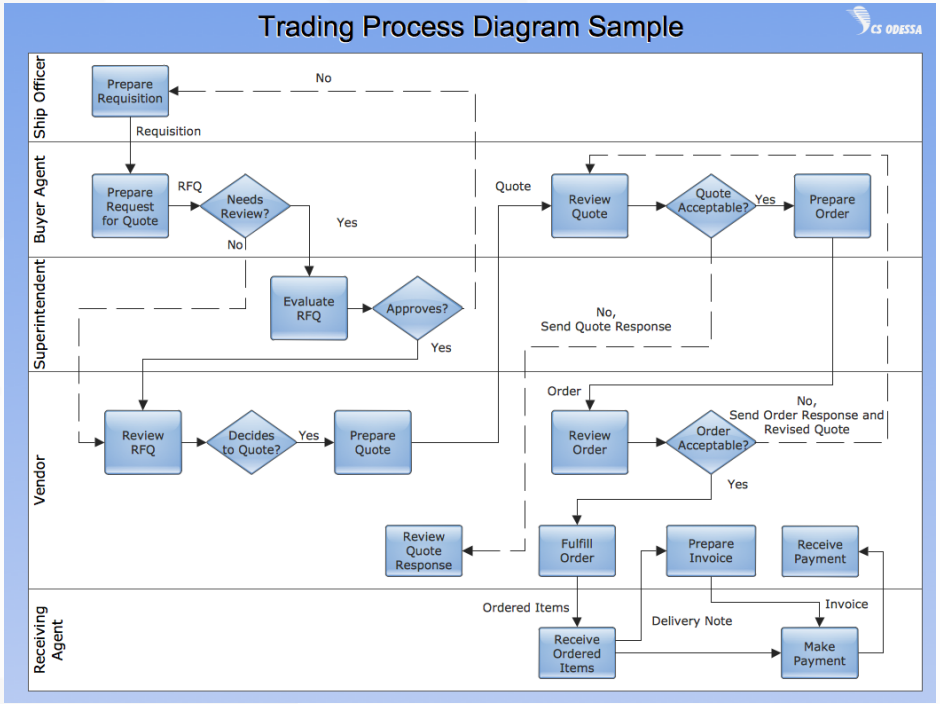
Desconoce el valor de los logs (CLOUD SOC)

Considerar que existe un solo Marco de seguridad, usar mas de un marco de seguridad.

Desconoce la cadena de valor de su empresa

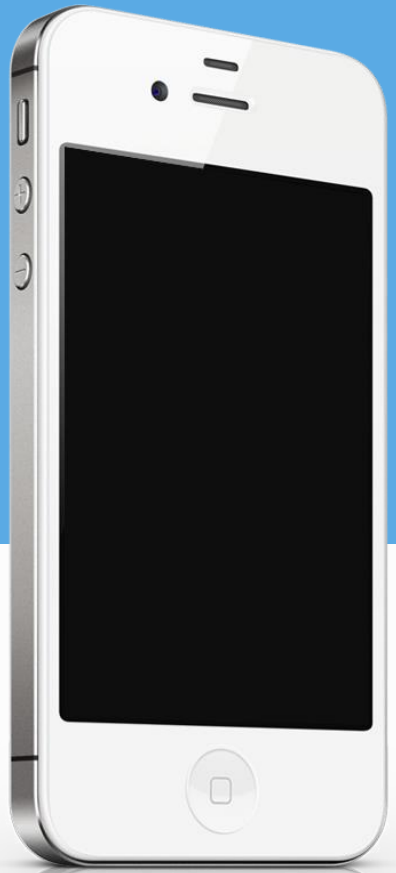
Lo que no debe hacer





Lo que no debe hacer

NO TODO ES TECNOLOGIA!



Informaciones

Info@freddastanza.com

- 14 Años de experiencia en el campo de la seguridad de la información
- Certificaciones Internacionales especializadas en el campo de la seguridad.
- Trabajos realizados en varios países de Centro y Sud América
- Instructor de varios cursos de Seguridad de la Información

Análisis

Experiencia

Certificaciones Internacionales

Coaching

Gracias por su tiempo

Preguntas…?