



XITH

CONOCIMIENTO – ESTRATEGIA – CRECIMIENTO

Auditorias de seguridad en TI

Presentación del servicio

Agenda:



1. ¿Qué es una auditoria de Seguridad?
2. Metodología de Implementación
3. Ejemplos de entregables
4. ¿Porqué es necesaria?
5. Beneficios



¿ Qué es una Auditoria de Seguridad ?

¿Qué es una auditoria de Seguridad?

Es una revisión del estado actual de la seguridad de la información en los servicios ofrecidos por el área de tecnologías de la información.

PROCESOS

Políticas de Seguridad



Cumplimiento legal



Análisis de incidentes



Conocimiento del personal



INFRAESTRUCTURA

Accesos



Firewalls



Servidores



Redes



VPNs



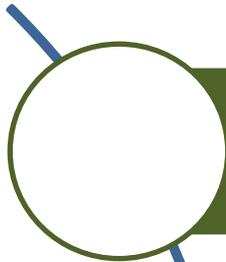
¿Cual es su utilidad?

Sirve para que el área de TI detecte de manera proactiva las siguientes áreas de oportunidad:

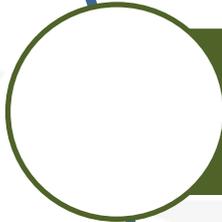


- VULNERABILIDADES QUE FAVORECEN ATAQUES EXTERNOS
- VULNERABILIDADES INTERNAS
- FALLAS DE ADMINISTRACIÓN O INSTALACION DE LOS EQUIPOS DE TI
- FALTA DE ACTUALIZACIONES EN LA INFRAESTRUCTURA TECNOLÓGICA
- CONFIGURACIONES DEFAULT QUE PUEDEN DESENCADENAR VULNERABILIDADES.
- DESALINEACIÓN ENTRE POLITICAS Y LA OPERACIÓN DE LA INFRAESTRUCTURA

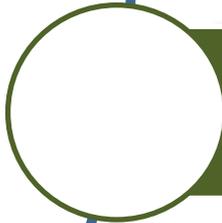
Para quién es recomendable



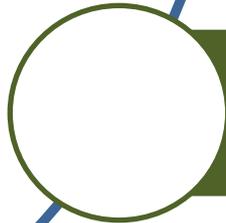
Para empresas que dependen de la tecnología de la información para la operación del negocio



Para empresas que pueden sufrir un alto impacto , económico, legal, de imagen o de producción en caso de la interrupción de su proceso de negocio



Para organizaciones que pueden poner en peligro la vida humana en caso de interrupción en su operación.



Para empresas con una filosofía de administración de riesgos que les permite planear su operación y evitar o reducir los riesgos para lograr sus objetivos



Metodología de ejecución

Procedimiento general



Basado en estándares y certificaciones

OWASP

- Mejores prácticas para aplicaciones web

OSSTMM

- Metodología para pruebas de seguridad

Cisco Safe

- Mejores practicas de seguridad en redes

Fabricantes o req. de cumplimiento

- Recomendaciones de seguridad emitidas por el fabricante (Microsoft, Cisco, IBM, HP, etc) o legales como LFDPPP o CNBV.

ISO 27001

- Sistemas de seguridad de la información

Certificaciones

- Certified Ethical Hacker, Certified Information Security Auditor, ISO 27001/BS 7799-2 Lead Auditor, CRISC, PMP, CCSP

Entregables

DVD con la documentación generada durante el proceso de auditoría

- Presentaciones técnica y ejecutiva
- Documentación de resultados
- Lista de actividades sugeridas para la remediación de las vulnerabilidades
- Evidencia de vulnerabilidades encontradas
- Documentación de mejores prácticas y recomendaciones sobre seguridad de la información
- Herramientas OpenSource utilizadas durante la auditoría.

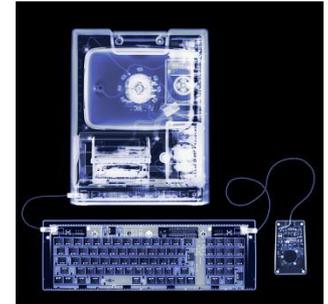
¿Mi empresa requiere una auditoría de seguridad?

Una auditoria es necesaria cuando se detectan las siguientes actividades o problemáticas.

- **Mi sitio web, correo, red o servidor ha sido hackeado o borrado**
- **Existen muchos incidentes de virus, equipos “que no sirven”**
- Hay personal en la organización que conoce información que no debería. (nómina, listados de clientes o proveedores, precios de productos, etc.).
- **Mi empresa cuenta con información altamente confidencial** y seria perjudicial que se conociera fuera de la misma (recetas o instructivos de productos, información de clientes o proveedores, datos financieros, etc.)
- No existen actualmente medidas o personas activas que apoyen para proteger la información de la empresa

Beneficios

- Proporciona una radiografía del contexto actual de la organización, no solo de los aspectos técnicos de la seguridad sino también su relación con las políticas, procedimientos e incidentes de la organización
- Permite detectar acciones que requieren una atención inmediata.
- Contar con un plan de acción priorizado de acuerdo al entorno y necesidades de la organización
- Permite establecer un punto de partida y punto de comparación para proyectos de seguridad de la información.
- El personal que ejecuta la auditoria cuenta con cuando menos estas certificaciones: CEH, CISA, CCSP, PMP, CRISC por lo que los resultados avalan la experiencia del personal con más de 15 años en el área de seguridad de la información.



Gracias, estamos a su servicio..



Contáctenos, podemos aportar beneficios a su organización

CONOCIMIENTO | ESTRATEGIA | CRECIMIENTO
Tel 33-1699-5577 email: contacto@xith.com.mx

www.xith.com.mx