

Fases para lograr un alto nivel de seguridad

-3 fases para que una organización logre un alto nivel de seg.

1: Fase técnica : La organización debe asegurarse de que sus infraestructuras IT críticas cuenten con elementos técnicos que impiden accesos no autorizados, pérdidas de info o caídas del servicio

- a) Evaluar el estado de la protección de los archivos mediante técnicas como auditorias de seguridad y pruebas de penetración
- b) Realizar modificaciones en las políticas de protección de seguridad tras los resultados de la evaluación.
- c) Mejorar la arquitectura para lograr un mejor control frente a cualquier incremento de los riesgos
- d) Monitorear constantemente las circunstancias, riesgos y medidas tomadas ante cualquier ataque presentado o que se pueda presentar

2: Fase Legal : La organización debe asegurarse de que el marco jurídico y contractual que rige tales infraestructuras IT críticas establece mecanismos legales para prevenir incidentes de ciberseguridad y mitigar o eliminar daños que la empresa pueda sufrir

- a) Identificar los activos intangibles estratégicos e infraestructuras TIC críticas de la org.
- b) Determinar el marco regulador (contratos con clientes, proveedores y empleados, leyes, códigos de autorregulación, políticas internas) de las infraestructuras TIC críticas.

- c) Identificar vulnerabilidades y plan o programa de acciones.
- d) Solucionar las vulnerabilidades y ejecutar un plan o programa de acciones que cree un escudo de defensa

3.- Fase cobertura: La organización debe contar con una adecuada política de transferencia del riesgo asociado al incidente de ciberseguridad y con pólizas de seguro correctamente diseñadas para dar cobertura a este tipo de siniestros tan particulares.

- a) Analizar qué amenazas tienen mayor probabilidad de materializarse y cuál puede ser el impacto económico
- b) Determinar una política de transferencia de estos riesgos (seguro)

→ Consideraciones para realizar una estrategia integral

- Es un plan de acción o ataque, que comprende todas las opciones y ángulos posibles. Se le llama integral precisamente porque abarca un rango muy amplio, global o total

Matriz FODA pieza clave en el diseño de la estrategia integral

También llamada Matriz de Análisis DAFO o SWOT Matrix en inglés

- g) FODA: Fortalezas, Oportunidades, Debilidades, Amenazas

El análisis FODA es una herramienta que permite conformar un cuadro de la situación actual del objeto de estudio permitiendo de esta manera obtener un diagnóstico preciso para tomar decisiones acordes con los objetivos y políticas formulados

- **Fortalezas:** Capacidades especiales con que cuenta la empresa y que le permite tener una posición privilegiada frente a la competencia. Recursos que se controlan, capacidades y habilidades que se poseen, actividades que se desarrollan positivamente
- **Oportunidades:** Son aquellos factores que resultan positivos favorables, explotables, que se deben descubrir en el entorno en el que actúa la empresa, y que permiten obtener ventajas competitivas
- **Debilidades:** Aquellos factores que provocan una posición desfavorable frente a la competencia, recurso de los que se carece, habilidades que no se poseen, actividades que no se desarrollan positivamente
- **Amenazas:** Aquellas situaciones que provienen del entorno y que pueden llegar a atentar incluso contra la permanencia de la organización.

Estrategia integral de ciberseguridad

Ciberseguridad conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas

Definir estrategia integral de la ciberseguridad

Definir Estrategia integral de ciberseguridad
Una serie de estándares, reglamentos, capacitación al personal que se adecúa a un parámetro consensuado dirigida a preservar los bienes digitales a través de la tríada de seguridad, incluyendo prevenciones, evaluación de riesgos, monitoreo, detección de amenazas, buenas prácticas, definición de políticas de seguridad, educación sobre esos temas, que fomentan el análisis proactivo de riesgos, a través de un equipo experto en distintas materias con el fin de cohesionar una solución más completa para cubrir las necesidades de seguridad informática, considerando todos los ángulos relacionados posibles.

Debe:

- a) Identificar ¿Qué preocupa? ¿Qué tipo de cibermensajes son las más probables?
- b) Identificar ¿en dónde?
Considerar el ámbito que abarca, éste puede ser particular (organizaciones pequeñas, medianas o grandes) general (estatal, federal - país, confederaciones)
- c) Identificar ¿quién tiene responsabilidades? Delimitando roles y órganos de gestión
- d) Identificar Cómo se responde a esa preocupación?
Con líneas de actuación y medidas concretas que alcancen los objetivos marcados