La Clave para lograr una Estrategia integral de Ciberseg. es basarse en las sig. líneas de acción:

1.- Capacidad de prevención, detección y respuesta ante las ciber-amenazas

a) Incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación ante las ciberamenazas

b) Administración privadas y públicas

c) Infraestructuras críticas

d) Capacidades de seguridad particular, militar y de defensa nacional

e) Otros sistemas de interés particular o nacional

2.- Seguridad de los sistemas de información de las administraciones privadas y públicas

a) Impulsar la implantación de esquemas particulares de seguridad o esquemas nacionales de Seguridad.

b) Reforzar las capacidades de detección

c) Mejorar la defensa de los sistemas clasificados

3.- Seguridad de las redes de datos y los sistemas de información que soportan las infraestructuras críticas

a) Impulsar la implantación de normativas sobre protección de infraestructuras críticas

b) Impulsar la implantación de normativas para la protección de los servicios esenciales

4.- Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia. Potenciar las capacidades para investigar y perseguir los ciberdelitos sobre la base de un marco jurídico y operativo eficaz

5- Seguridad y resilencia en el sector privado o público

Impulsar la seguridad y la resilencia de las infraestructuras, redes, productos y servicios utilizando técnicas de cooperación pública-privada Mediante aspectos políticos, sociales, económicos, Organizacionales, respaldos por una autoridad nacional o internacional efectiva.

Aplicar esquemas mixtos y masivos de colaboración, local, nacional regional y global

6- Conocimientos, competencias

Promover la capacitación de profesionales en ciberseguridad para que se logren soluciones eficaces.

7- Compromiso nacional e internacional

Promover un ciberespacio internacional seguro y confiable, apoyando así intereses nacionales e internacionales

8- Cultura de ciberseguridad:

a) Concientizar a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información

b) Concientizar sobre el uso responsable de las nuevas tecnologías

c) Concientizar sobre los servicios de información

1- Definir y tener claras la visión, misión y objetivos de la organización

2.- Realizar un análisis de la situación informática de la organización (Análisis de riesgos)

- identificar los procesos más críticos o los que pudiera frenar la operación de la empresa
- identificar y documentar los activos más importantes
- identificar las vulnerabilidades
- Clasificar los probables riesgos en orden de importancia o por procesos críticos.

3.- Delimitar el ámbito de aplicación del Programa de Ciberseguridad

4.- Identificar el conjunto de competencias y capacidades necesarias para la aplicación del programa

5.- Definir la estrategia de ciberseguridad

6.- Reclutar y formar el equipo de ciberseguridad

7.- Desarrollar el programa de acuerdo con la estrategia de ciberseguridad

8.- Revisar el estado de ejecución del programa

9.- Aplicar acciones correctivas y de mejoras al programa

- Infraestructura crítica (Europa sí, México No)

aquellas instalaciones, redes y servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las

- administración (servicios básicos, instalaciones, redes de info y principales activos y monumentos del patrimonio nacional)
- Instalaciones del espacio
- Industria Química y Nuclear (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos biológicos, radiológicos, etc.)
- Agua (embalses, almacenamiento, tratamiento y redes)
- Centrales y Redes de energía (producción y distribución)

- Tecnologías de la información y la comunicaciones (TIC)
- Salud (sector e infraestructura sanitaria)
- Transportes (aeropuertos, puertos, instalaciones intermodales ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc)
- Alimentación (producción, almacenamiento y distribución)
- Sistema Financiero y tributario (entidades bancarias, información valores e inversiones

4.2 La protección de la infraestructura crítica también es conocida como la protección de las infraestructuras de energía telecomunicaciones, suministro de agua

Estas infraestructuras críticas necesitan ser protegidas contra eventos accidentales y deliberados que:

a) No les permitirían operar correctamente

b) Impactarían severamente la economía
c) Impactarían severamente al bienestar social de ese país o nación

Las infraestructuras críticas también dependen en mayor o menor medida de las infraestructuras de información (tecnologías de la informarión y de las comunicaciones)

La protecciín de la infraestiuctura crítica es un problema que debe ser resuelto por los gobiernos. Protección compartida
La carencia de una protección de la infraestructura crítica representa un problema para todas
La protección de la infraestructura crítica es una responsabilidad nacional, y puede ser manejada principalmente como un asunto de seguridad nacional
La protección de la información de la infraestructura

Algunos países pueden tener infraestructuras que se comparten con otros países
Los gobiernos deben colaborar con los operadores de infraestructuras del sector privado para asegurar la continuida. del servicio al implementar infraestructuras robustas

México: áreas estratégicas → Correos, telégrafos, Generación de energía nuclear, Sistema eléctrico nacional, Explotación de hidrocarburos Comunicaciones y ferrocarriles

Ley General de Protección Civil: Las infraestructuras estratégicas Son aquellas

Retos que enfrenta la protección de infraestructura crítica

a) Magnitud: Definir cuáles son, donde están, que riesgos tienen y cómo pueden protegerse.
Se estima que hoy deben exitir poco más de 3 mil Instalaciones o infraestructuras críticas

b) Mando: No se percibe una línea de mando clara u Organismo rector. No existe una definición de Infraestructura crítica; no se consideran muchas

c) Intercambio de información: Considerarse la homologación y la compatibilidad en glosarios, bases de datos, plataformas de gestión de informarión, plataformas de comunicación y algunos otros dispositivos relacionados a la seguridad y protección para permitir el intercambio

d) Conocimiento: Cada sector tiene experiencias y prácticas

e) Interdependencia: Quien o que dependen de la infraestructura crítica

f) Herramientas Inadecuadas

g) Conflicto Asimétrico: No existe simetría alguna entre el número de infraestructuras, los recursos para protegerlas y los posibles riesgos y amenazas