Infraestructuras Críticas

Comunicaciones Críticas

Rodriguez Fernando (13094), Santilli Franco (13241), Santiago Marcos (13137), Tagarot Renzo (13138), Zaina Guillermo (13226)

[Ferrodriguez15@gmail.com](mailto:Ferrodriguez15@gmail.com) , [zainaguillermo@gmail.com](mailto:zainaguillermo@gmail.com) , [marcossantiagoh2@gmail.com](mailto:marcossantiagoh2@gmail.com) , [francosantilli47@gmail.com](mailto:francosantilli47@gmail.com) , [renzot0800@gmail.com](mailto:renzot0800@gmail.com) .

**Abstract.** En este documento se desarrollan la fragilidad de las infraestructuras respecto al sector de comunicaciones y sus implicancias.

**Keywords.** Problemáticas Económicas y Sociales. Resiliencia.

1. Introducción

Entendemos como estructura física a todo aquel sistema físico o virtual el cual tiene como principal objetivo facilitar funciones y servicios esenciales en sistemas involucrados a nivel social, económico, medioambiental y político. Estos tienen como característica principal que su interrupción por motivos naturales o humanos trae consigo graves consecuencias.

1. Amenazas de las Infraestructuras

Las infraestructuras críticas son parte muy importante en cualquier estado y estas pueden ser similares en varios países, aparte de estar clasificada en su totalidad como secreta. Por lo que una amenaza a estas puede significar un gran problema, ya que ante un problema no se podrá continuar con normalidad las actividades básicas de la sociedad. Luego el problema empeora cuando una infraestructura depende de otra, así ambas acabarán paralizadas. Por esto es importante que las infraestructuras sean resilientes, es decir, capaz de adaptarse o responder positivamente a nuevas condiciones de manera de poder restaurar, mantener e incluso mejorar sus funciones esenciales

Por ejemplo, podríamos hablar sobre el sistema financiero cuya infraestructura es muy importante para la nación, y se pueden ver grandes riesgos potenciales, como ataques cibernéticos y/o problemas de energía, haciendo mucho hincapié en este último, por lo que funcionarios del gobierno se preocupan en neutralizar las vulnerabilidades que estas infraestructuras padecen. Tales pueden ser:

1. Crimen Organizado: Este puede llegar a desestabilizar de forma muy rápida, el cual apunta a sus propios fines de lucro. Este es manejado principalmente por grupos violentos.
2. Espionaje: Es una gran amenaza llevada a cabo entre países, ya sea por su propia mano como por empresas extranjeras y/o empresas privadas, siendo su objetivo obtener cantidades ingentes de información y datos confidenciales entre los que puedan estar los de infraestructuras críticas.
3. Desastres Naturales: El impacto de las catástrofes perjudica la vida de las personas, así como a los bienes patrimoniales, al medio ambiente y al desarrollo económico. Un ejemplo bastante actual es la pandemia provocada por el COVID-19.
4. Terrorismo: Puede llegar a darse una combinación entre las 3 anteriormente mencionadas, buscando perjudicar a una nación a través de diferentes estrategias y medios

Otro aspecto importante a considerar en la actualidad es la sostenibilidad por lo que es importante tenerlo presente a la hora del diseño de manera que permita un equilibrio entre aspectos sociales, económicos y eficientes, integrar la perspectiva intergeneracional, enfoque de las partes interesadas y por último debe integrar el pensamiento del ciclo de vida.

El modelo actual de desarrollo es insostenible en América latina por lo que requiere de grandes cambios estructurales a fin de cumplir con los objetivos de desarrollo sostenible para 2030.

1. Áreas Estratégicas de las Infraestructuras:

A continuación, mostraremos un listado de las principales áreas de las infraestructuras críticas:

* Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones). Siendo este el principal foco de posibles ataques a las infraestructuras.
* Administración (servicios básicos, instalaciones, redes de información, principales activos y monumentos del patrimonio nacional).
* Agua (embalses, almacenamiento, tratamiento y redes).
* Alimentación (producción, almacenamiento y distribución).
* Centrales y Redes de energía (producción y distribución).
* Instalaciones relacionadas con el Espacio Exterior.
* Centrales nucleares (producción, almacenamiento y transporte de mercancías peligrosas, materiales nucleares, radiológicos, etc.).
* Industria Química (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, etc.).
* Investigación: laboratorios que por su idiosincrasia dispongan o produzcan materiales, sustancias o elementos críticos o peligrosos.
* Salud (sector e infraestructura sanitaria).
* Tecnologías de la Información y las Comunicaciones (TIC, ya sean infraestructuras críticas en sí mismas, como redes de telecomunicaciones, o den servicio de información y comunicaciones a otras infraestructuras críticas)
* Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico).

1. Sector de Comunicaciones:

Es importante destacar que el sector de comunicaciones es fundamental ya que es el medio encargado de permitir las operaciones de todas las empresas y el gobierno ya que para el funciona-miento de una gran parte de equipos y procesos que son utiliza-das en otras instalaciones críticas, dependiendo estos de los ser-vicios que son justamente ofrecidos por las empresas de telecomunicaciones. Entre estos se encuentran:

* Servicios de voz.
* Servicios de Internet.
* Servicios de datos.
* Servicios VoIP.
* Servicios de SMS.
* Cloud computing. Para los servicios de computación a través de Internet.
* Routing manager. Permite actualizar la configuración del servicio a tiempo real y de forma automática.
* Call conference. Facilita la realización de audioconferencias o reuniones virtuales.
* Grabación de voz.
* Contact center virtual.
* Numeración para la recepción masiva de llamadas.
* Servicio de GPS.
* Servicio de streaming.

El sector de comunicaciones actualmente se encuentra interconectado donde se utilizan distintos tipos de transmisión: terrestre, satelital e inalámbrica. Los proveedores de estos a su vez dependen uno de otros para el transporte de la información. Las empresas poseen los requerimientos necesarios para garantizar la interoperabilidad.

1. Medidas de Seguridad:

Para garantizar la continuidad de las operaciones los concesionarios de redes públicas o privadas de telecomunicaciones están obligados a contar con un plan de acciones para así evitar la interrupción de los servicios y proporcionar servicios de emergencia en casos de extrema necesidad.

La importancia de la pronta recuperación de los servicios esenciales en casos extremos permite evitar la pérdida de transferencia de información, la cual puede ser de gran ayuda en casos de desastres y así poder evitar la mayor cantidad de pérdidas y accidentes que la falta de estos ocasionaría en nuestra sociedad actual.

Las medidas de prevención se deben implementar para reducir los riesgos que pueden producir amenazas en este tipo de infraestructuras, las cuales pueden ser tanto físicas como lógicas. Para evitar que estas amenazas se materialicen, se necesita reducir al máximo las debilidades de los activos y de los procesos críticos, los sistemas y las redes, y así de esta forma disminuir de forma considerable su impacto.

El esquema de seguridad integral debe contar con medidas preventivas que introduzcan la recuperación inmediata de los servicios esenciales los cuales esté a cargo la institución o empresa.

Este listado contempla las principales medidas que se pueden aplicar para evitar, controlar o reducir las consecuencias a amenazas:

* Implementar y mantener una cultura de seguridad en todo el personal que conforma la empresa, incluido, desde luego, el cuerpo directivo.
* Analizar los riesgos mediante una evaluación periódica que nos ayude a determinar el porcentaje de probabilidad de que una amenaza, tanto física como lógica, se materialice en los diferentes activos de la organización: personas, instalaciones, sistemas informáticos, redes de comunicaciones, etc.
* Tomar como base normas o estándares de seguridad como los que tiene ASIS International o bien los ISO 27000, ISO 27002, ISO 27005, ISO 31000, etc.
* Implementar medidas de seguridad física como las que a continuación se enuncian:
  + Estricto control de accesos de personas y materiales.
  + Instalación de cerraduras electrónicas mancomunadas en áreas críticas.
  + Contar con diferentes tipos de detectores y equipo de alarmas conectados a una central externa y centro de monitoreo propio.
  + Contar con equipo de videovigilancia distribuido de manera estratégica en zonas vulnerables o críticas.
  + Contar con software analítico de vídeo que coadyuve en la detección preventiva de irregularidades en los protocolos de seguridad establecidos por la empresa.
  + Complementar con personal de seguridad debidamente capacitado y entrenado.
  + Desarrollar normas, políticas y procedimientos de seguridad específicos para este tipo de industria.
  + Contar con un centro de monitoreo propio que valide de manera permanente la aplicación de los protocolos de seguridad de todas las personas que ingresan a las instalaciones y que además coordine acciones en caso de emergencia.
  + Evaluar periódicamente los sistemas y procesos de seguridad mediante la ejecución de simulacros y auditorías.
  + Establecer un esquema de denuncia confidencial para que el personal pueda reportar cualquier tipo de irregularidades que detecte.

1. Conclusión:

Tal como se ha podido comprobar estas infraestructuras críticas son un pilar fundamental de cualquier país y cualquier interrupción a las mismas traería grandes consecuencias al país

Si bien todas son de vital importancia, se pudo notar que la infraestructura de comunicaciones es de gran interés debido a la cantidad de distintas áreas que abarca por lo que es muy importante contar con todas las herramientas y normas de seguridad para así prevenir o evitar posibles amenazas que atenten contra la integridad del sector.

1. Cibergrafía:

* <https://isbl.eu/2020/03/que-son-las-infraestructuras-criticas/#:~:text=Las%20infraestructuras%20cr%C3%ADticas%20son%20todos,%2C%20econ%C3%B3micos%2C%20medioambiental%20y%20pol%C3%ADtico>.
* <https://drive.google.com/drive/folders/1DuPIxot6LUGts2lELxfbr181ApQnKE_T>
* <https://www.segurilatam.com/seguridad-por-sectores/infraestructuras-criticas/infraestructura-critica-telecomunicaciones_20190904.html>
* <https://www.cisa.gov/communications-sector>