Ciberseguridad

Cada día, gobiernos, empresas y ciudadanos enfrentan las consecuencias de ciberataques que amenazan la seguridad digital. La creciente sofisticación y frecuencia de estas amenazas, que van desde el robo de datos y la interrupción de servicios hasta el espionaje y la manipulación de información, impactan profundamente la estabilidad económica, la reputación institucional y la confianza pública en el entorno digital. Este panorama exige una comprensión profunda y proactiva de los desafíos que plantea la ciberseguridad.

Es por ello que la comprensión de los principios y prácticas de la ciberseguridad se ha vuelto indispensable para todos los sectores de la sociedad. Desde la protección de infraestructuras críticas hasta la salvaguarda de la privacidad individual, la capacidad de identificar, prevenir y responder eficazmente a los incidentes cibernéticos es crucial para mantener la resiliencia y la continuidad de nuestras operaciones cotidianas.

Este documento tiene como objetivo clarificar conceptos clave que a menudo generan confusión en la sociedad, presentándolos de manera estructurada a través de distintos capítulos. Su propósito es educar y capacitar a un público amplio, proporcionando las bases necesarias para fomentar una cultura de ciberseguridad robusta y consciente. Además, se destaca la importancia de la cooperación regional y el desarrollo de estrategias nacionales integradas para abordar esta amenaza global de manera efectiva.

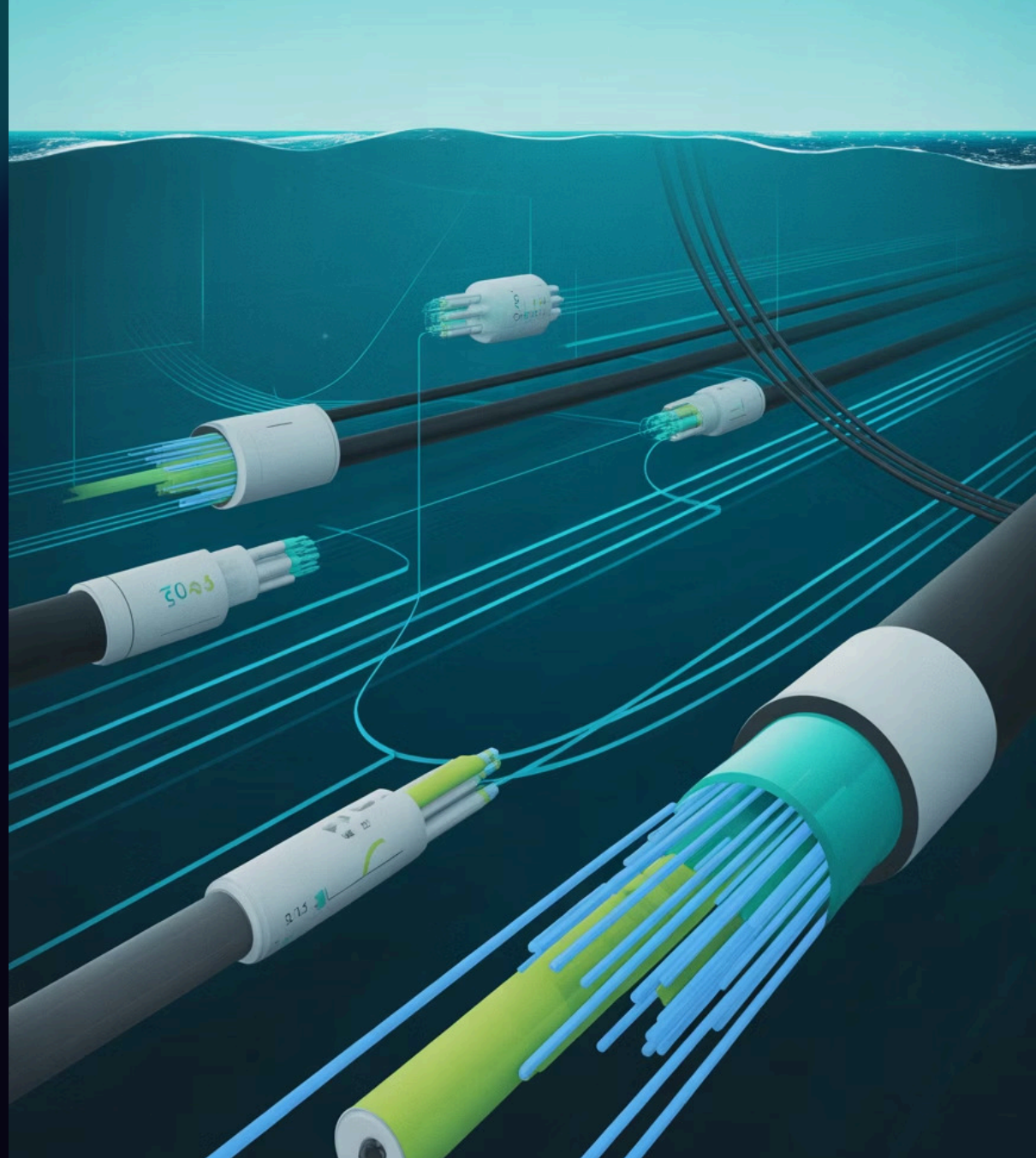
Eduardo Jorge Martino

Índice de Contenidos

Introducción

Cómo Argentina se conecta con el mundo

Eduardo Jorge Martino



Diferencia entre conectividad internacional por fibra óptica y por servicios satelitales

La relación entre el tráfico cursado por fibra óptica submarina y la conectividad vía satélite es complementaria y se basa en las fortalezas y debilidades de cada tecnología. No son competidores directos en la mayoría de los casos, sino que sirven a diferentes propósitos en la red global de Internet. Aquí se detalla la relación entre ambos:

Eduardo Jorge Martino

La Fibra Óptica Submarina como "la columna vertebral"

Capacidad masiva y velocidad

La inmensa mayoría del tráfico de Internet a nivel mundial (se estima que más del 99%) viaja a través de cables de fibra óptica submarinos. Estos cables tienen un ancho de banda y una capacidad de transmisión de datos incomparablemente superiores a los satélites. Un solo cable puede transportar varios terabits de datos por segundo. Esto los convierte en la "columna vertebral" de la conectividad global, permitiendo la comunicación fluida entre continentes.

Baja latencia

La latencia (el tiempo de retardo en la transmisión de datos) es crucial para aplicaciones en tiempo real como videojuegos en línea, transacciones financieras de alta frecuencia y videoconferencias. La fibra óptica, al transmitir datos a la velocidad de la luz a través de un medio físico, ofrece una latencia significativamente más baja que los satélites.

Fiabilidad y costos

Aunque la instalación de los cables es costosa y compleja, una vez operativos, son extremadamente fiables (con las debidas protecciones) y tienen un costo por bit de datos mucho más bajo que la conectividad satelital.

> Las Toninas es el principal punto de ingreso de la fibra óptica submarina que llega a nuestro país, fue elegida esa localidad por no estar afectada por los sedimentos barrosos que arroja el Rio de la Plata a las costas marinas y estar próxima al centro neurálgico del país. Existen también tendidos hacia Chile (posee tendidos sobre el Pacífico) y hacia el norte con otros países.

La Conectividad Satelital como "la alternativa" o "el complemento"

Cobertura universal

El satélite es la solución principal para llevar conectividad a zonas remotas y rurales donde la instalación de fibra óptica es inviable o económicamente inviable. Un satélite puede cubrir vastas áreas geográficas, superando barreras como montañas, océanos o terrenos inaccesibles.

Redundancia y resiliencia

La conectividad satelital juega un papel vital como respaldo en caso de un fallo en los cables submarinos. Si un terremoto, un ancla de barco o un sabotaje corta un cable de fibra, los satélites pueden proporcionar un servicio de emergencia para mantener la conectividad, aunque sea con menor capacidad y mayor latencia. En la era moderna, el uso de constelaciones de satélites de órbita baja (LEO) como Starlink busca mejorar la latencia y la velocidad, acercando el rendimiento satelital al de la fibra óptica, aunque todavía con limitaciones.

Movilidad

La conectividad vía satélite es esencial para aplicaciones que requieren movilidad, como la navegación marítima, la aviación y las comunicaciones militares en el campo. La fibra óptica, al ser una conexión física, no puede ofrecer este tipo de flexibilidad.

Conclusión

La relación entre ambas tecnologías es de complementariedad, no de sustitución.

Fibra Óptica Submarina

Es la infraestructura fundamental que soporta la mayor parte del tráfico global de Internet, ofreciendo una alta capacidad, velocidad y baja latencia a un costo relativamente bajo por unidad de datos.

Conectividad Satelital

Sirve para llevar Internet a lugares donde la fibra no puede llegar, proporcionar redundancia en caso de fallos y habilitar la conectividad en movimiento.

En el futuro, con el auge de las constelaciones de satélites de órbita baja, es posible que la conectividad satelital gane más terreno en la competencia con la fibra óptica, especialmente en términos de latencia. Sin embargo, por el momento, la fibra óptica sigue siendo la tecnología dominante para la interconexión de países y continentes debido a su inigualable capacidad y rendimiento.

Capítulo 1

Ciberseguridad en la órbita privada y en la órbita pública

Eduardo Jorge Martino

¿Qué es la Ciberseguridad?

La ciberseguridad se puede definir como el conjunto de herramientas, procesos y medidas tecnológicas y humanas que tienen como objetivo proteger la información, los sistemas y las redes de computadoras contra ciberataques, daños y accesos no autorizados.

Piensa en ella como la seguridad de tu hogar, pero en el mundo digital. Así como instalas cerraduras, alarmas y sistemas de vigilancia para proteger tu casa de ladrones, la ciberseguridad usa diferentes capas de protección para resguardar tus datos de intrusos malintencionados en línea.

Objetivo principal de la ciberseguridad

El objetivo principal de la ciberseguridad es garantizar la confidencialidad, la integridad y la disponibilidad de la información:

Confidencialidad

Asegurar que la información solo sea accesible por aquellos que tienen la autorización para verla. Por ejemplo, la contraseña de tu correo electrónico.

Integridad

Garantizar que la información no sea alterada o modificada de forma no autorizada. Esto es crucial para los registros médicos o las transacciones bancarias.

Disponibilidad

Asegurar que los sistemas y la información estén accesibles para los usuarios cuando sea necesario. Un ataque que deja un sitio web fuera de servicio afecta la disponibilidad.

En resumen, la ciberseguridad es una disciplina en constante evolución que abarca desde la protección de un simple teléfono móvil hasta la defensa de infraestructuras críticas nacionales, como redes eléctricas o sistemas de transporte. Su importancia radica en que, en un mundo cada vez más digital, la información es uno de nuestros activos más valiosos.

Ciberseguridad Nacional

La ciberseguridad nacional es un concepto amplio que abarca el conjunto de políticas, estrategias, normativas, tecnologías y acciones que un Estado implementa para proteger su ciberespacio. Su principal objetivo es salvaguardar los activos digitales y la infraestructura crítica de la nación, tanto del sector público como del privado.

Eduardo Jorge Martino

¿Qué abarca la ciberseguridad nacional?

Más allá de proteger las computadoras del gobierno, abarca un enfoque integral con varios aspectos clave:

Protección de infraestructuras críticas

Defensa de sistemas vitales (energía, transporte, finanzas, salud, telecomunicaciones y agua). Un ciberataque en estos sectores podría paralizar el país.

Defensa de la información y los datos del Estado

Protege información confidencial y datos sensibles del gobierno, defensa y agencias de inteligencia para evitar espionaje, manipulación y sabotaje.

Prevención y respuesta a amenazas

Previene, detecta y responde eficazmente a ciberataques de cibercriminales, terroristas, Estados o activistas, desarrollando ciberdefensa y ciberinteligencia.

Promoción de la ciberseguridad en la sociedad

Fomenta la concientización y educación de ciudadanos, empresas y administraciones públicas sobre riesgos cibernéticos, creando una cultura de seguridad digital.

Cooperación internacional

Colaboración con otros países y organismos internacionales para compartir información, coordinar respuestas y combatir el cibercrimen global, ya que los ciberataques no tienen fronteras.

En esencia, la ciberseguridad nacional busca garantizar la estabilidad, la soberanía y la resiliencia de un país en el entorno digital, asegurando que sus ciudadanos, su economía y su gobierno puedan operar de forma segura en el ciberespacio.

Países que producen Ciber ataques

Determinar con exactitud qué países son los que más ciberataques producen a nivel mundial es una tarea compleja, ya que la atribución de un ataque es extremadamente difícil. Los atacantes suelen utilizar infraestructuras distribuidas por todo el mundo, como redes de bots, y técnicas de anonimato para ocultar su verdadera ubicación.

Por esta razón, la mayoría de los informes y análisis se basan en el país de origen del tráfico malicioso o en la atribución que realizan las agencias de inteligencia. Sin embargo, los informes de ciberseguridad suelen señalar consistentemente a ciertos países como las principales fuentes de ciberataques, tanto patrocinados por el estado como por grupos criminales.

Países consistentemente señalados como principales fuentes de ciberataques

China

Es frecuentemente citada como la principal fuente de ciberataques, especialmente en el ámbito de la ciberdelincuencia patrocinada por el Estado. Se le atribuyen campañas de espionaje a gran escala dirigidas a la propiedad intelectual, secretos de estado y tecnologías de defensa de países como Estados Unidos y sus aliados. También es uno de los principales orígenes de bots para ataques de denegación de servicio distribuido (DDoS).

Rusia

Es un actor dominante en el ciberespacio, conocido por sus ataques dirigidos a infraestructura crítica, campañas de desinformación, interferencia en procesos electorales y ataques destructivos. Los grupos de cibercrimen de origen ruso son particularmente conocidos por su experiencia en ataques de ransomware y phishing, y se considera que a menudo operan con el beneplácito del gobierno ruso.

Estados Unidos

Aunque a menudo se le ve como el principal objetivo de los ciberataques, Estados Unidos también es una fuente significativa de actividad cibernética, tanto ofensiva como defensiva. Las agencias de inteligencia estadounidenses tienen capacidades ofensivas avanzadas y se les ha atribuido el origen de ciberarmas sofisticadas.

Brasil

En la región de América Latina, Brasil es un importante foco de cibercrimen, siendo una de las principales fuentes de ataques a nivel global. El país ha visto un aumento en la ciberdelincuencia, con una gran cantidad de ataques dirigidos al sector financiero y de gobierno. Esto se debe en parte a su creciente digitalización y a la existencia de grupos de cibercriminales muy activos.

Otros países relevantes

Corea del Norte

Este país es conocido por usar los ciberataques como una fuente de ingresos para el régimen, realizando ataques a bancos, plataformas de criptomonedas y otros objetivos para financiar sus programas nucleares y militares.

Irán

Ha intensificado sus capacidades cibernéticas, realizando ataques de espionaje y destructivos contra sus rivales geopolíticos, especialmente en Oriente Medio y otros países occidentales.

India

Ha escalado en la lista de países origen de ciberataques, impulsado por una combinación de factores, incluyendo la creciente digitalización y la presencia de grupos de hackers.

Es importante recordar que estas clasificaciones pueden variar según el informe o la agencia que las elabore, y que la naturaleza de la ciberdelincuencia hace que los datos sean dinámicos y difíciles de verificar con total precisión.

Capítulo 2

Diferencias entre Ciberseguridad, Ciber Crimen y Ciberdefensa

Eduardo Jorge Martino

Diferencias entre Ciberseguridad, Cibercrimen y Ciberdefensa

En Argentina, las diferencias entre Ciberseguridad, Cibercrimen y Ciberdefensa están bien definidas, aunque trabajan en conjunto en muchos aspectos. A continuación, se detallan sus funciones y distinciones:

Eduardo Jorge Martino

Ciberseguridad

Esto incluye el uso de firewalls, sistemas de detección de intrusiones, cifrado de datos y gestión de identidades y accesos.

Gestión de Riesgos

Evaluar y minimizar el riesgo al que están expuestos ciudadanos y organizaciones frente a amenazas cibernéticas.

Respuesta a Incidentes

Desarrollar planes de acción y equipos de respuesta (CERT/CSIRT) para gestionar, mitigar y recuperarse de incidentes de seguridad informática. La Dirección Nacional de Ciberseguridad de Argentina, por ejemplo, administra el equipo de respuesta a emergencias informáticas a nivel nacional (CERT Nacional).

Protección de Infraestructuras Críticas

Promover políticas para salvaguardar las infraestructuras críticas del país (energía, comunicaciones, finanzas, etc.).

Capacitación y Concientización

Educar a la población, empresas y empleados públicos sobre las amenazas cibernéticas y las mejores prácticas de seguridad.

Cibercrimen

El cibercrimen se refiere a la comisión de delitos utilizando la tecnología y el ciberespacio como medio o fin. En Argentina, estos delitos están tipificados en el Código Penal y son investigados por las fuerzas de seguridad y el sistema judicial.

Funciones principales:

- **Investigación y Persecución:** La Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI) del Ministerio Público Fiscal y las divisiones especializadas de las fuerzas de seguridad son las encargadas de investigar y perseguir los delitos informáticos.

Tipos de Delitos

El Código Penal argentino sanciona una variedad de ciberdelitos, incluyendo:

Daño informático

Alterar, destruir o inutilizar datos, programas o sistemas.

Acceso ilegítimo

Ingresar a sistemas informáticos restringidos sin autorización.

Grooming

Acoso a menores de edad a través de medios electrónicos.

Fraude informático

Engaños para obtener información o beneficios económicos, como el phishing.

Violación de la privacidad

Divulgación no autorizada de imágenes o grabaciones íntimas, entre otros.

- **Prevención de Delitos:** A través de campañas de sensibilización, se busca educar a la sociedad para que evite ser víctima de ciberdelitos.

Ciberdefensa

La ciberdefensa es el ámbito militar y estatal que se encarga de proteger la soberanía nacional y la seguridad de las infraestructuras críticas del Estado frente a ciberataques de origen estatal o de grupos hostiles.

Eduardo Jorge Martino

Funciones principales de la Ciberdefensa

1

Protección Militar

El Comando Conjunto de Ciberdefensa (CCCD), bajo el Ministerio de Defensa, es el organismo responsable de coordinar y ejecutar las operaciones de ciberdefensa. Su objetivo es proteger las redes y sistemas de las Fuerzas Armadas y el Estado Mayor Conjunto.

2

Respuesta a Ataques

Responder ante ciberataques pergeñados por otros estados o actores que busquen afectar la integridad, disponibilidad y soberanía del ciberespacio nacional.

3

Inteligencia y Monitoreo

Anticipar y prevenir ataques en el ciberespacio, disminuyendo las vulnerabilidades y aumentando la resiliencia de los sistemas y redes.

4

Capacitación y Formación

Impulsar programas de capacitación y formación para personal especializado en ciberdefensa, como los que se realizan a través del Instituto de Ciberdefensa de las Fuerzas Armadas.

Diferencias clave

Alcance

La ciberseguridad es un concepto amplio que busca proteger a todos los actores (ciudadanos, empresas, Estado) de amenazas cibernéticas en general. La ciberdefensa se enfoca exclusivamente en la seguridad y soberanía del Estado, sus Fuerzas Armadas e infraestructuras críticas, frente a amenazas de alto nivel, generalmente de origen estatal. El cibercrimen es la rama que se dedica a la investigación y persecución de los delitos cometidos en el ciberespacio.

Naturaleza de la Amenaza

La ciberseguridad aborda amenazas de diversa índole (ransomware, phishing, malware), independientemente de su origen. La ciberdefensa se centra en amenazas estratégicas, como la ciberguerra, el ciberespionaje o el cibersabotaje patrocinado por estados o grupos organizados con fines geopolíticos. El cibercrimen investiga los delitos informáticos, que pueden ser cometidos por individuos, grupos delictivos o incluso organizaciones criminales.

Actores Involucrados

La ciberseguridad involucra a organismos públicos (Dirección Nacional de Ciberseguridad), empresas privadas, ONGs y la sociedad civil. La ciberdefensa es una función del Estado, a través del Ministerio de Defensa y las Fuerzas Armadas. El cibercrimen involucra a las fuerzas de seguridad, el Ministerio Público Fiscal y el Poder Judicial.

Capítulo 3

Qué función cumple el CERT.ar

Eduardo Jorge Martino

El CERT Nacional para ciberseguridad en Argentina

El CERT Nacional para ciberseguridad en Argentina es el Equipo de Respuesta ante Emergencias Informáticas Nacional (CERT.ar). Se trata del organismo oficial, dependiente de la Dirección Nacional de Ciberseguridad, encargado de gestionar y coordinar la respuesta a incidentes de seguridad informática en el país. Sus funciones principales se centran en:

Gestión de incidentes

Administrar y procesar los reportes de incidentes de seguridad que provienen del Sector Público Nacional.

Asesoramiento técnico

Brindar asistencia técnica y coordinar acciones ante los incidentes de seguridad que afecten a los organismos del Estado.

Prevención y alerta

Contribuir a la capacidad de prevención, detección, alerta y recuperación ante ciberataques. Para ello, elabora guías, publica recomendaciones y buenas prácticas en materia de ciberseguridad.

Colaboración

Coordinar con otros equipos de respuesta a incidentes (tanto públicos como privados) y cooperar con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en la gestión de incidentes.

Protección de infraestructuras críticas

Trabajar en la protección de las infraestructuras de información críticas del país.

En resumen, el CERT.ar actúa como el punto central de contacto y coordinación para la gestión de incidentes de seguridad informática a nivel nacional, con el objetivo de proteger los activos de información del Sector Público y de las infraestructuras críticas, y de fomentar una cultura de ciberseguridad en el país.

¿Cómo funcionan los CERT?

Los CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incident Response Team) son equipos de respuesta a incidentes de seguridad informática. Su función principal es ayudar a prevenir, gestionar y responder a ciberataques y otros incidentes de seguridad. La forma en que funcionan y de qué organismos dependen puede variar, pero hay un marco general que la mayoría sigue.

Los CERT nacionales tienen como objetivo proteger la infraestructura de tecnología de la información de un país y relacionarse con similares de otros paises. Sus funciones pueden dividirse en servicios proactivos y reactivos:

Servicios reactivos (gestión de incidentes)

Monitoreo y detección

Vigilan constantemente las redes y sistemas para identificar posibles amenazas y incidentes de seguridad.

Análisis y evaluación

Una vez que se detecta un incidente, lo analizan para determinar su naturaleza, alcance y gravedad.

Respuesta y coordinación

Ayudan a las organizaciones afectadas a contener el ataque, eliminar el malware, corregir las vulnerabilidades y restaurar los servicios. Actúan como un punto central de contacto para la gestión de incidentes a nivel nacional.

Gestión de vulnerabilidades

Analizan y coordinan la respuesta a vulnerabilidades detectadas en software o hardware.

Servicios proactivos (prevención y concientización)

Alertas y avisos de seguridad

Emiten boletines y alertas sobre nuevas amenazas, vulnerabilidades y campañas de ciberataques.

Capacitación y educación

Ofrecen formación y promueven la concienciación sobre ciberseguridad a nivel gubernamental, empresarial y entre la población en general.

Desarrollo de herramientas de seguridad

Pueden desarrollar o recomendar herramientas para la detección, prevención y respuesta a incidentes.

Auditorías y evaluaciones de seguridad

Realizan auditorías para evaluar la seguridad de los sistemas y redes.

¿De qué organismo internacional dependen?

Los CERT nacionales no dependen de un único organismo internacional con autoridad directa sobre ellos, sino que operan en una red de cooperación y colaboración global. Sin embargo, existen organizaciones y foros internacionales que facilitan esta colaboración:

Forum of Incident Response and Security Teams (FIRST)

Es la asociación global más importante de equipos de respuesta a incidentes. FIRST proporciona un foro de confianza para que sus miembros (CERT/CSIRT de todo el mundo) intercambien información, experiencias y conocimientos sobre amenazas y vulnerabilidades.

Organismos regionales

Existen consorcios regionales, como el APCERT (Asia Pacific CERT), que agrupan a equipos de respuesta a incidentes de una región específica para fortalecer la ciberseguridad y compartir información a nivel local.

Coordinación bilateral y multilateral

Los CERT nacionales colaboran entre sí de manera bilateral y multilateral. Comparten inteligencia sobre amenazas, coordinan la respuesta a incidentes que afectan a múltiples países y trabajan juntos para luchar contra la ciberdelincuencia.

En resumen, los CERT nacionales son entidades clave para que la ciberseguridad de un país, actuando como un punto central para la gestión de incidentes y la prevención de amenazas. Aunque no están sujetos a la autoridad directa de un organismo internacional, su efectividad se basa en gran medida en la cooperación y el intercambio de información a través de redes globales como FIRST. El CERT nacional posee un repositorio nacional de incidentes que oportunamente se detallará.

Capítulo 4

Uso de las direcciones IP y función de los DNS

Eduardo Jorge Martino

Las direcciones IP (Protocolo de Internet)

Las direcciones IP (Protocolo de Internet) son identificadores numéricos que se asignan a cada dispositivo conectado a una red que utiliza el protocolo de Internet, ya sea una red local o Internet. Funcionan de manera similar a una dirección postal, permitiendo que los datos se envíen y reciban de manera correcta entre dispositivos.

Hay dos tipos principales de direcciones IP:

Direcciones IP públicas

Son las que se utilizan para la comunicación en Internet y son visibles para el resto del mundo. Son asignadas por el proveedor de servicios de Internet (ISP) a tu router.

Direcciones IP privadas

Se usan dentro de una red local, como la red de tu hogar o empresa, para que los dispositivos se comuniquen entre sí. No son visibles desde Internet.

Administración de las direcciones IP

La administración de las direcciones IP se lleva a cabo a través de una estructura jerárquica a nivel global y regional.

A nivel internacional:

ICANN (Internet Corporation for Assigned Names and Numbers)

Es una organización sin fines de lucro que se encarga de coordinar la asignación de direcciones IP a nivel mundial. Su principal función es garantizar la estabilidad operacional de Internet y evitar la duplicación de identificadores.

IANA (Internet Assigned Numbers Authority)

Es una división de ICANN que supervisa la asignación global de direcciones IP, así como otros identificadores de protocolo.

Registros Regionales de Internet (RIR)

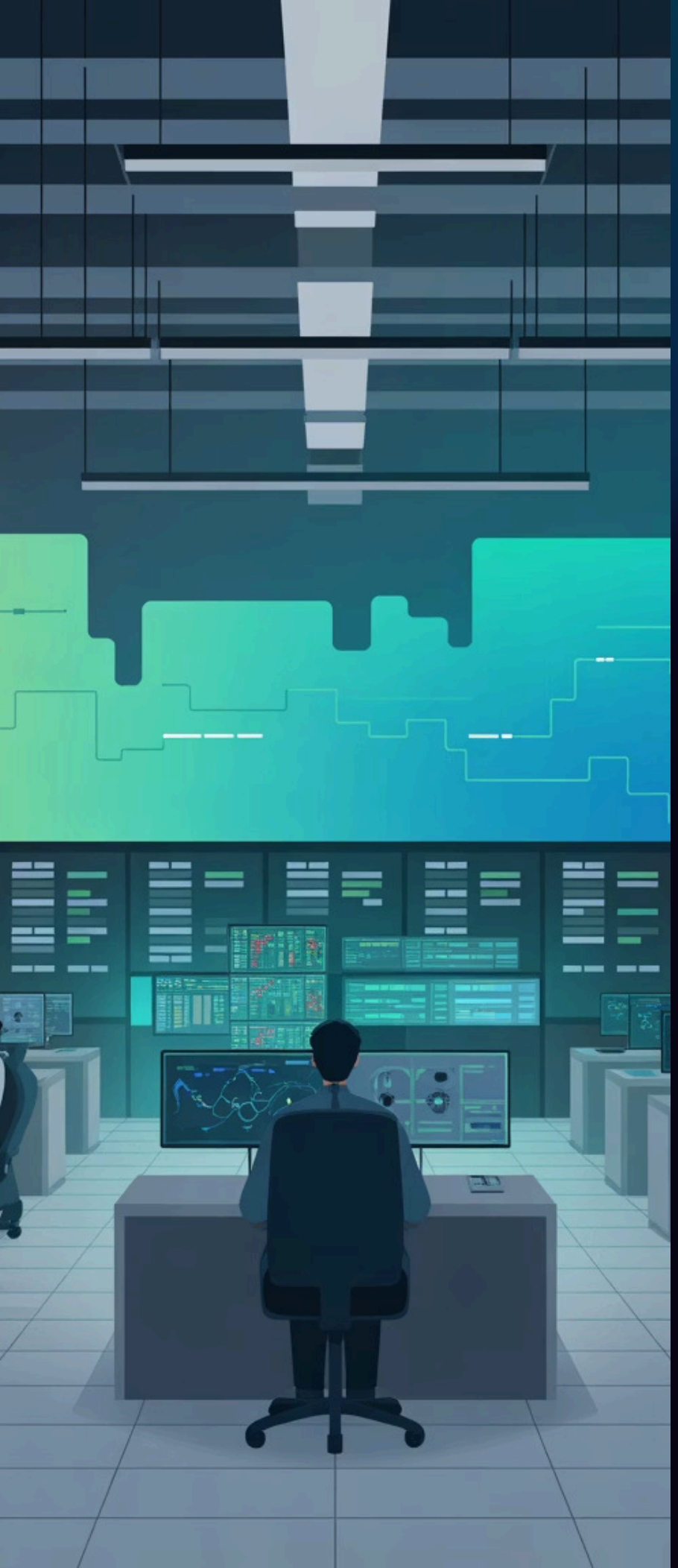
IANA delega la administración de grandes bloques de direcciones IP a cinco RIR, que son los encargados de distribuir las direcciones a nivel regional. Los cinco RIR son: ARIN (América del Norte), RIPE NCC (Europa, Medio Oriente y Asia Central), APNIC (Asia y la región del Pacífico), AFRINIC (África), LACNIC (América Latina y el Caribe).

A nivel nacional en Argentina

La administración de las direcciones IP para Argentina se encuentra bajo la jurisdicción del RIR correspondiente a la región, que es LACNIC (Registro de Direcciones de Internet para América Latina y el Caribe). Aunque LACNIC es el responsable de la asignación y administración de los recursos de numeración de Internet para la región, a nivel local, el ENACOM (Ente Nacional de Comunicaciones) se encarga de regular y supervisar las telecomunicaciones, incluyendo la relación con los organismos internacionales como LACNIC.

Sin embargo, para la asignación y gestión de nombres de dominio de Internet con la extensión ".ar", el organismo que se encarga es NIC Argentina.

Eduardo Jorge Martino



NIC Argentina

NIC Argentina (Network Information Center Argentina) es la Dirección Nacional del Registro de Dominios de Internet de Argentina. Su principal función es:

Administrar el registro de los dominios de Internet bajo el código de país ".ar"

Garantizar la estabilidad y seguridad del sistema de nombres de dominio (DNS) para los dominios ".ar"

Administrar el proceso de registro, renovación, transferencia y disputa de dominios de Internet, y resolver conflictos que puedan surgir en relación con la titularidad de los mismos

Colaborar con organismos de seguridad para combatir amenazas cibernéticas y promover la ciberseguridad

Dependencia del organismo nacional:

NIC Argentina depende de la Secretaría Legal y Técnica de la Presidencia de la Nación.

El DNS (Domain Name System)

El DNS (Domain Name System) o Sistema de Nombres de Dominio es una parte fundamental de las redes de internet. Su función principal es actuar como una especie de "agenda telefónica" de Internet. Para entenderlo mejor, imagina que quieres llamar a un amigo. No te aprendes su número de teléfono completo, sino que lo buscas por su nombre en tu agenda. El DNS hace exactamente lo mismo para internet.

Función principal:

Traducción de nombres a direcciones IP

Los humanos utilizamos nombres de dominio fáciles de recordar, como www.google.com o www.wikipedia.org, para acceder a los sitios web. Sin embargo, los dispositivos en red (servidores, computadoras, etc.) se comunican entre sí utilizando direcciones IP, que son cadenas de números (por ejemplo, 172.217.168.14). El DNS se encarga de traducir ese nombre de dominio que escribes en tu navegador a la dirección IP numérica que el ordenador necesita para encontrar el servidor donde se aloja el sitio web.

¿Cómo funciona el DNS?

Cuando escribes una dirección web en tu navegador, se inicia un proceso de "resolución de nombres" que involucra varios servidores DNS distribuidos por todo el mundo:

01

Consulta local

Tu dispositivo primero revisa su propia memoria caché DNS para ver si ya ha resuelto esa dirección IP recientemente.

02

Servidor DNS recursivo

Si no la encuentra, tu solicitud se envía a un servidor DNS recursivo (generalmente proporcionado por tu proveedor de servicios de Internet, ISP). Este servidor actúa como un intermediario.

03

Jerarquía de servidores DNS

Si el servidor recursivo tampoco tiene la información, inicia un viaje a través de la jerarquía de DNS: Pregunta a un servidor raíz (.) dónde encontrar el servidor TLD (.com, .org, .es, etc.). El servidor raíz le indica la dirección del servidor TLD. Luego, pregunta al servidor TLD dónde encontrar el servidor autoritativo para el dominio específico (google.com). Finalmente, el servidor autoritativo (que tiene la autoridad final sobre ese dominio) le da la dirección IP correcta.

04

Respuesta y caché

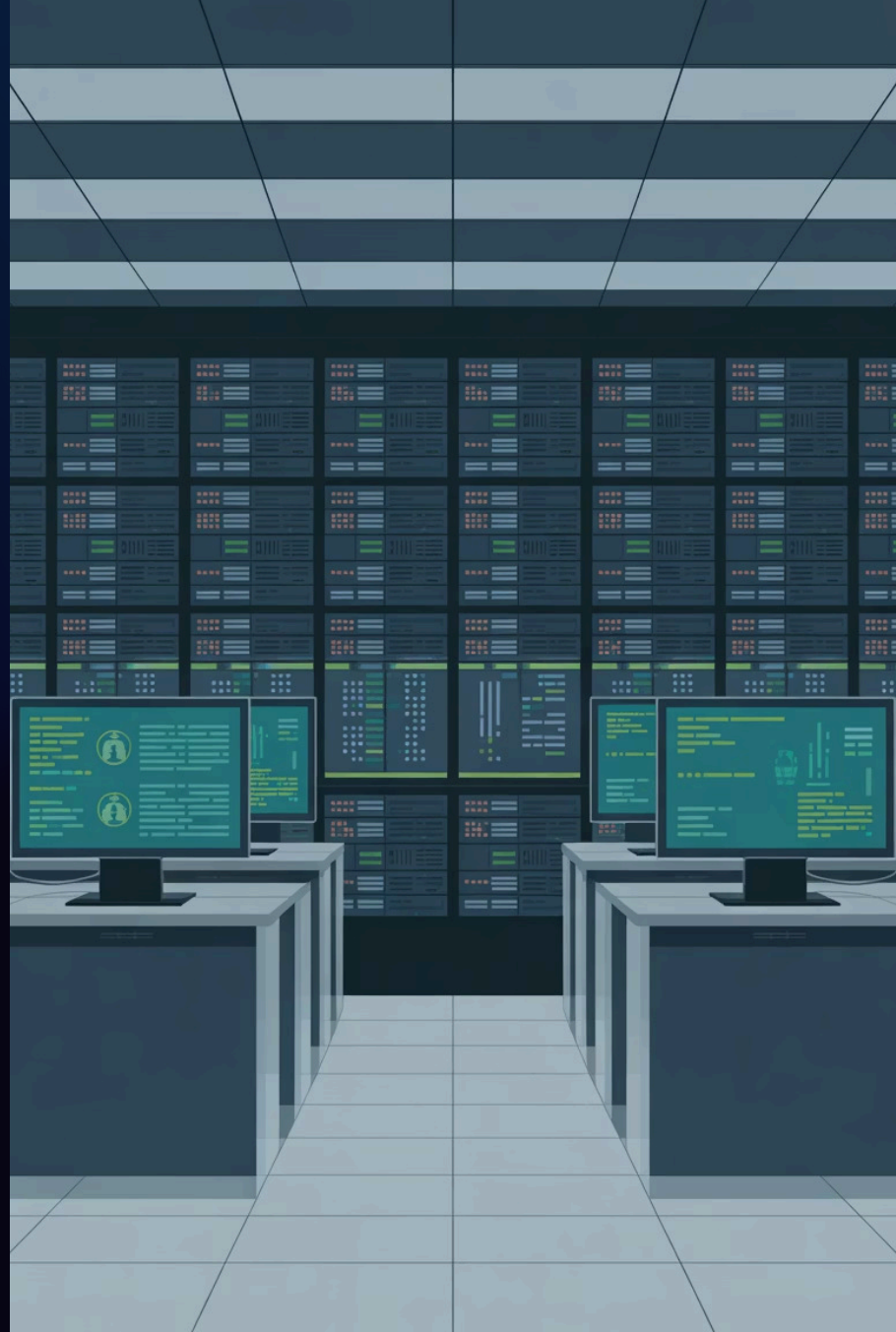
El servidor recursivo recibe la dirección IP y se la devuelve a tu dispositivo. Además, la almacena en su caché para futuras solicitudes, lo que acelera el proceso la próxima vez que intentes acceder al mismo sitio.

En resumen, el DNS es un sistema esencial para la navegación web, ya que elimina la necesidad de que los usuarios memoricen largas y complejas direcciones IP, permitiendo una experiencia de Internet más intuitiva y fácil de usar.

Eduardo Jorge Martino

Capítulo 5

Importancia de contar con un Repositorio Nacional de Incidentes



Eduardo Jorge Martino

Importancia de un Repositorio Nacional de Ciberseguridad

Centralización de la información

Un repositorio permite compilar y centralizar datos sobre incidentes de seguridad, vulnerabilidades, amenazas y tácticas de ataque a nivel nacional. Esto evita que cada organismo público o entidad privada actúe de forma aislada, creando una visión holística y actualizada del panorama de riesgos.

Análisis de tendencias y patrones

Al compartir información sobre indicadores de compromiso (IPs maliciosas, hashes de archivos, dominios fraudulentos, etc.), se pueden identificar patrones y tendencias de ataque. Esto permite a los distintos actores anticiparse a los ciberataques, tomar medidas preventivas y fortalecer sus defensas antes de ser víctimas.

Mejora de la capacidad de respuesta

En caso de un incidente de gran envergadura que afecte a múltiples sectores (por ejemplo, un ataque de ransomware masivo), un repositorio facilita la coordinación entre los equipos de respuesta. Se pueden compartir conocimientos, herramientas y estrategias para mitigar el impacto y restaurar los servicios de manera más rápida y eficiente.

Beneficios Institucionales del Repositorio

Coordinación interinstitucional

Un repositorio facilita la colaboración entre diferentes organismos del Estado (como el CERT.AR, la Dirección Nacional de Ciberseguridad, fuerzas de seguridad, etc.) y con el sector privado, permitiendo una respuesta coordinada ante incidentes de gran escala.

Transparencia y rendición de cuentas

Permite al Estado demostrar su compromiso con la ciberseguridad y rendir cuentas sobre las acciones tomadas para proteger a los ciudadanos y las infraestructuras críticas.

Cumplimiento normativo

Ayuda a cumplir con las obligaciones legales y regulatorias en materia de ciberseguridad, tanto a nivel nacional como internacional.

Dependencia y Acceso

En Argentina, la responsabilidad de la ciberseguridad en el sector público recae principalmente en la Dirección Nacional de Ciberseguridad, que se encuentra dentro de la órbita de la Jefatura de Gabinete de Ministros. Esta dirección es la encargada de coordinar las acciones de ciberseguridad, elaborar estrategias nacionales y, en este marco, operar el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR).

El CERT.AR es el principal punto de contacto para la gestión de incidentes de seguridad informática en el sector público y es el organismo que gestiona y administra la información relativa a ciberataques.

¿Cómo se ingresa para conformar esa información?

Para organismos públicos

Los organismos de la Administración Pública Nacional deben reportar los incidentes de ciberseguridad a través de los canales establecidos por la Dirección Nacional de Ciberseguridad, usualmente a través de la comunicación con el CERT.AR. Esta es una obligación que se desprende de las normativas de ciberseguridad del Estado. La información se gestiona de manera confidencial para proteger la identidad de las organizaciones afectadas.

Para el sector privado

No existe una obligación general y estandarizada para todas las empresas de reportar a un único repositorio. Sin embargo, en el ámbito financiero, el Banco Central ha establecido la obligatoriedad de reportar incidentes. Por otro lado, la Dirección Nacional de Ciberseguridad y el CERT.AR también ofrecen canales para que empresas privadas y particulares puedan reportar incidentes de manera voluntaria, con el fin de contribuir a la inteligencia nacional en materia de ciberseguridad.

En resumen, la Dirección Nacional de Ciberseguridad, a través del CERT.AR, es la dependencia clave que actúa como un "repositorio" de facto y punto de coordinación para la respuesta a ciberataques en Argentina.

Organismo coordinador a nivel nacional sobre ciberseguridad

El organismo nacional que coordina las estrategias y procedimientos en materia de ciberseguridad con las provincias en Argentina es el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR), que opera bajo la órbita de la Dirección Nacional de Ciberseguridad de la Jefatura de Gabinete de Ministros.

Aunque las provincias tienen sus propios equipos de respuesta a incidentes (conocidos como CSIRTs o CERTs provinciales, como el CSIRT-PBA de la provincia de Buenos Aires), el CERT.AR es el punto de enlace y el organismo central que promueve la coordinación a nivel federal.

Las funciones del CERT.AR en la coordinación con las provincias incluyen:

Asistencia y cooperación

El CERT.AR coopera con los gobiernos provinciales en la gestión de incidentes de seguridad informática, brindando asistencia técnica y facilitando el intercambio de información.

Creación de capacidades

Trabaja para impulsar la formación y el fortalecimiento de las capacidades de prevención, detección, alerta y recuperación en las provincias, a través de capacitaciones y la promoción de buenas prácticas.

Articulación de la respuesta

Actúa como el principal punto de contacto a nivel nacional para la respuesta a incidentes de seguridad, lo que le permite articular los esfuerzos del gobierno nacional con los de las provincias ante amenazas que puedan tener un impacto en múltiples jurisdicciones.

Impulso de un enfoque federal

Las estrategias nacionales de ciberseguridad, como el Plan Federal de Prevención de Ciberdelitos, buscan específicamente adoptar un enfoque integral y colaborativo, invitando a las jurisdicciones provinciales a adherir a sus lineamientos.

En resumen, si bien cada provincia puede tener su propio equipo de ciberseguridad, el CERT.AR es la dependencia del Estado Nacional que actúa como el organismo de coordinación central, fomentando la colaboración y unificando la respuesta a nivel federal.

Capítulo 6

Tipos y nombres de los Malware más usados para producir ataques informáticos

Eduardo Jorge Martino

Malware (software malicioso)

Es el término genérico para cualquier software diseñado para infiltrarse o dañar un sistema informático. Dentro de esta categoría se encuentran los ejemplos más conocidos:

Virus

Se adjunta a un archivo o programa legítimo y se replica cuando el usuario lo ejecuta. Necesita de la intervención humana para propagarse.

Troyano

Es un programa que se disfraza de algo útil o inofensivo para engañar al usuario y que lo instale. Su objetivo es abrir una "puerta trasera" para que otros programas maliciosos accedan al sistema, robar datos o tomar el control del equipo de forma remota. No se replica por sí mismo.

Gusano

A diferencia del virus, un gusano se replica por sí mismo y se propaga a través de redes, explotando vulnerabilidades de seguridad. No necesita de la intervención del usuario para infectar otros sistemas.

Ransomware

Un tipo de malware que cifra los archivos de la víctima y exige un rescate (ransom) para liberarlos. Es uno de los ataques más devastadores para empresas y particulares.

Malware (software malicioso) - Continuación

Otros tipos comunes de malware que afectan a usuarios y organizaciones:

Spyware

Su objetivo es espiar las actividades del usuario sin su consentimiento. Puede registrar las pulsaciones de teclado (keyloggers), capturar la pantalla, o recopilar información personal para enviársela al atacante.

Adware

Muestra anuncios publicitarios no deseados e invasivos en la pantalla del usuario. Aunque su intención principal no es dañar, puede ralentizar el sistema y, en casos más peligrosos, ser un vehículo para otro tipo de malware.

Botnet

Es una red de dispositivos infectados (llamados "bots" o "zombies") que son controlados de forma remota por un ciberdelincuente. Se utilizan para llevar a cabo ataques a gran escala, como el envío masivo de spam o ataques de denegación de servicio.

Ataques de Ingeniería Social

Estos ataques se basan en la manipulación psicológica de las personas para que revelen información confidencial o realicen acciones que comprometan su seguridad.

Phishing

El atacante se hace pasar por una entidad de confianza (un banco, una empresa, una red social) para engañar a la víctima y que revele datos personales, contraseñas o información bancaria a través de correos electrónicos, mensajes de texto o páginas web falsas.

Spear Phishing

Una variante del phishing que es más dirigida y personalizada. El atacante investiga a su objetivo para crear un mensaje muy convincente y específico, como un correo electrónico que parece provenir de un colega o superior.

Whaling

Un ataque de spear phishing dirigido específicamente a directivos de alto nivel (CEO, CFO, etc.) dentro de una organización. El objetivo es obtener acceso a información crítica o realizar transferencias de dinero fraudulentas.

Ataques a la Red y la Infraestructura

Estos ataques se dirigen a las redes y servidores para interrumpir servicios o interceptar datos.

Ataque de Denegación de Servicio (DoS) y Denegación de Servicio Distribuido (DDoS)

El atacante inunda un servidor, un servicio o una red con una cantidad masiva de tráfico, haciendo que colapse y no pueda atender a los usuarios legítimos. En un ataque DDoS, este tráfico proviene de múltiples fuentes, como una botnet, lo que lo hace más difícil de mitigar.

Ataque Man-in-the-Middle (MITM)

El atacante se interpone entre dos partes que se están comunicando (por ejemplo, tu navegador y un sitio web) e intercepta, lee y posiblemente modifica la información que se transmite entre ellos sin que ninguna de las partes lo sepa.

Inyección SQL

Un ataque dirigido a bases de datos en sitios web. El atacante inserta código malicioso en los campos de entrada de una página web (como formularios de búsqueda o de inicio de sesión) para manipular la base de datos y obtener, modificar o eliminar información confidencial.

Capítulo 7

La ONTI (Oficina Nacional de Tecnologías de la Información), qué función cumple

Eduardo Jorge Martino

La Oficina Nacional de Tecnologías de la Información (ONTI)

La Oficina Nacional de Tecnologías de la Información (ONTI) en Argentina ha emitido diversas disposiciones y recomendaciones para proteger los Centros de Datos (DataCenters) y la información, especialmente en el ámbito de la Administración Pública Nacional (APN). A continuación, se resumen algunas de las principales directrices y recomendaciones emitidas por la ONTI, que se encuentran en documentos como los Estándares Tecnológicos para la Administración Pública Nacional (ETAP) y otras normativas:

Eduardo Jorge Martino

Protección Física y Ambiental de los Data Centers

1

Control de Acceso Físico

Se deben implementar controles estrictos para el acceso a las áreas donde se procesa o almacena información sensible. Esto incluye el registro de entradas y salidas de visitantes, y el uso de controles de autenticación para restringir el acceso solo a personal autorizado. Los derechos de acceso deben ser revisados y actualizados regularmente.

2

Protección contra Desastres

Incendios: Se debe contar con equipos contra incendios ubicados de manera adecuada.
Materiales Peligrosos: Los materiales combustibles o peligrosos deben almacenarse a una distancia segura del área asegurada.
Respaldo y Recuperación: El equipo de reemplazo y los medios de respaldo deben ubicarse a una distancia segura para evitar daños en caso de un desastre que afecte la ubicación principal.

3

Infraestructura

Cableado: Se recomienda separar el cableado de energía del de datos para evitar interferencias y proteger el tendido troncal (vertical) con ductos blindados. **Ambiente:** Un Data Center de nivel básico, según los ETAP, debe contar con una sala específica, provisión de energía y aire acondicionado.

4

Ubicación del Equipo

El equipo debe ubicarse de manera que se minimice el acceso innecesario y se restrinja el ángulo de visión de pantallas que manejan datos confidenciales para reducir el riesgo de que la información sea vista por personas no autorizadas.

Seguridad de la Información

Gestión de la Seguridad de la Información

La ONTI promueve la implementación de un marco de gestión de la seguridad de la información que permita la identificación, prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad.

Políticas de Seguridad

Los organismos públicos deben contar con Políticas de Seguridad de la Información escritas. La ONTI ha desarrollado modelos de políticas para que los organismos se adecuen a ellos.

Clasificación de la Información

Se debe clasificar la información, especialmente la sensible o confidencial, para asegurar que sea protegida durante todo su ciclo de vida, desde la recolección hasta su almacenamiento.

Gestión de Riesgos

Las entidades deben establecer una metodología para la gestión de riesgos, incluyendo la identificación y evaluación de los mismos, y determinar la tolerancia al riesgo en función del apetito de riesgo de la entidad.

Seguridad de la Información (continuación)

Protección de Datos Personales

Se debe cumplir con la Ley de Protección de Datos Personales (Ley N° 25.326) y sus decretos reglamentarios. En el contexto de servicios en la nube (Cloud Computing), la ONTI ha establecido requisitos para la adecuación del tratamiento de datos, la garantía de localización de los mismos, la propiedad, la seguridad del borrado de la información y mecanismos de auditoría.

Coordinación de Emergencias

La ONTI cuenta con una Coordinación de Emergencias en Redes Teleinformáticas (CERT) que centraliza y coordina los esfuerzos para el manejo de incidentes de seguridad que afecten a los recursos informáticos del sector público.

Aspectos Tecnológicos

Monitoreo del Tráfico

Se debe tener conocimiento del tráfico de la red, tanto el necesario como el innecesario, para poder eliminarlo o aislarlo.

Dispositivos Móviles y Teletrabajo

Se han emitido directrices para asegurar la información cuando se utilizan dispositivos móviles y se realiza trabajo remoto, considerando los riesgos de trabajar en ambientes no protegidos.

Estándares Tecnológicos

La ONTI aprueba los Estándares Tecnológicos para la Administración Pública Nacional (ETAP), que son un conjunto de normas técnicas y recomendaciones que los organismos de la APN deben seguir en materia de tecnologías de la información. Estos estándares cubren diversos aspectos de la seguridad.

En resumen, las disposiciones de la ONTI se centran en un enfoque integral de la seguridad que abarca desde el control físico de los espacios donde se aloja la información, hasta la implementación de políticas, procedimientos y tecnologías para proteger los datos de amenazas internas y externas, asegurando la continuidad del negocio y el cumplimiento de la normativa vigente.

Capítulo 8

Legislación vigente

Eduardo Jorge Martino

Legislación vigente en Argentina

En Argentina, la protección de personas y organizaciones víctimas de un ataque de ciberseguridad se rige por un conjunto de leyes y normativas que abarcan desde el Código Penal hasta regulaciones específicas sobre protección de datos. La legislación busca castigar los delitos informáticos y, al mismo tiempo, proteger la información y los derechos de las víctimas. Las principales normas que entran en juego son:

Ley 26.388 de Delitos Informáticos

Esta es la ley fundamental que tipifica y sanciona los ciberdelitos en Argentina. Algunos de los delitos que contempla y que pueden aplicar a una víctima de ciberseguridad incluyen:

Acceso ilegítimo a sistemas informáticos

Penado para quienes ingresan a un sistema informático de forma no autorizada.

Intercepción o interferencia de datos o comunicaciones electrónicas

Sanciona a quienes capturan o alteran comunicaciones sin autorización judicial.

Daño a datos o sistemas informáticos

Castiga la eliminación, deterioro, alteración o supresión no autorizada de datos, documentos o programas. Las penas son mayores si se afectan sistemas públicos o de servicios esenciales (salud, comunicaciones, energía, etc.).

Otras leyes relevantes

Ley 25.326 de Protección de Datos Personales

Esta ley es crucial para las organizaciones, ya que establece la obligación de proteger los datos personales que recopilan y almacenan. Si un ciberataque resulta en la filtración o exposición de datos personales, la organización víctima puede enfrentar consecuencias legales si se demuestra que no cumplió con las medidas de seguridad adecuadas. Por otro lado, esta ley también protege a las personas, dándoles el derecho a: Acceder, rectificar, actualizar o suprimir sus datos personales. Presentar denuncias ante la Agencia de Acceso a la Información Pública (AAIP) si sus datos se han visto comprometidos.

Ley 25.506 de Firma Digital

Esta ley reconoce la validez legal de la firma digital, equiparándola con la firma manuscrita. Su importancia radica en que promueve la seguridad jurídica en las transacciones electrónicas y puede ser relevante en casos donde los ciberataques involucran documentos o transacciones digitales.

Convención de Budapest sobre Ciberdelincuencia (Ley 27.411)

Argentina adhirió a esta convención internacional, lo que significa que el país está alineado con un marco legal global para la cooperación en la lucha contra los ciberdelitos. Esto facilita la colaboración con otros países en la investigación de ataques transnacionales.

Qué hacer en caso de ser víctima de un ciberataque

Para una persona u organización víctima de un ciberataque, la legislación vigente permite:

01

Realizar una denuncia penal

Los delitos informáticos se denuncian ante la justicia, que iniciará una investigación para identificar a los responsables y aplicar las sanciones correspondientes del Código Penal.

02

Ejercer acciones civiles

Las víctimas pueden reclamar una compensación por los daños y perjuicios sufridos, ya sean económicos, a la reputación, o de otro tipo, a través de acciones civiles.

03

Notificar a las autoridades competentes

CERT.ar: Es el Centro Nacional de Respuesta a Incidentes Informáticos, que depende de la Dirección Nacional de Ciberseguridad. Su función es asistir a las entidades en la gestión de incidentes de seguridad.
AAIP: La Agencia de Acceso a la Información Pública debe ser notificada en caso de una violación de seguridad que afecte datos personales.

04

Consultar con profesionales

La legislación argentina en ciberseguridad es compleja. Es fundamental buscar asesoramiento legal y técnico para gestionar la crisis, preservar evidencia digital y seguir los pasos correctos para mitigar los daños y hacer valer los derechos.

Caso Testigo

En oportunidad de abrirse una causa en el ámbito de la Pcia. De Buenos Aires, por la denuncia realizada por un Multimedio, que consistía en que un usuario del Multisitio al ingresar a la web, era derivado a una sala de juegos virtuales (Pfishing). Una vez determinado que el ataque provenía del exterior del país, la policía Provincial determinó su incompetencia, solicitando ayuda a la Dirección Nacional de Ciberseguridad, en primera instancia se solicitó a la autoridad judicial si podía designar a la Dirección Nacional para avanzar en una causa internacional. Una vez logrado ese requisito se procede a determinar el país de origen, eso se realizó con ayuda de otros CERT de países adheridos y se logró determinar que habiendo rebotado en 4 países, siendo su origen un usuario de Polonia. Lo primero que se hizo fue consultar a Interpor, que posee 180 delegaciones con especialistas en Ciberseguridad si el Pfishing era delito en Polonia, de no ser así, era imposible seguir con una causa judicial. Verificado que esa figura era penalizada en ese país, se requirió a la autoridad judicial originaria que autorice a la Dirección Nacional para su intervención y se presentó la denuncia en el Ministerio de Relaciones Exteriores para ser dirigido a Polonia con los datos de mes, día, hora y minutos exactos de la IP utilizada para identificar al usuario que produjo es ataque, me es imposible asegurar el resultado final de esa intervención, puedo determinar que fue una de las únicas denuncias realizadas con esa práctica, la cual es muy normal en otros países comprometidos con la Ciberseguridad.

Capítulo 9

Obligación de Denunciar un Ciberataque

Eduardo Jorge Martino

Organismos del Estado, Ámbito Bancario y Financiero

Sector Público

Las normativas de ciberseguridad, como la Segunda Estrategia Nacional de Ciberseguridad, establecen protocolos y responsabilidades para los organismos del Estado. Aunque la ley no lo establece explícitamente con una sanción para el incumplimiento en todos los casos, la naturaleza de la información manejada y el potencial impacto en la seguridad nacional y los servicios públicos hacen que la denuncia y la colaboración sean una práctica obligatoria y fundamental para la coordinación de la respuesta.

Sector Bancario y Financiero

El Banco Central de la República Argentina (BCRA) ha emitido comunicaciones que exigen a las entidades financieras notificar y reportar incidentes de ciberseguridad. Si bien no se trata de una ley penal que imponga una pena de prisión por no denunciar, el incumplimiento de estas disposiciones del BCRA puede acarrear sanciones regulatorias, multas y la pérdida de confianza de los clientes, además de la obligación de resarcir a las víctimas.

Particulares

Particulares

Para los ciudadanos comunes y corrientes, la denuncia de un ciberdelito no es una obligación legal en el mismo sentido que para un organismo del Estado o un banco. Sin embargo, se recomienda encarecidamente realizarla a las autoridades y a CERT.AR para ayudar a combatir el ciberdelito y proteger a otras posibles víctimas. La denuncia es fundamental para que se inicie una investigación penal, se persiga a los responsables y se pueda intentar recuperar los bienes perdidos o restaurar los daños.

Empresas

Para las empresas, especialmente aquellas en sectores críticos o que manejan datos sensibles, reportar incidentes de ciberseguridad no es solo una buena práctica, sino que puede ser un requisito de regulaciones específicas dependiendo de la industria (como servicios financieros, telecomunicaciones o infraestructura crítica).

Tener protocolos de respuesta a incidentes	Reportar a CERT.AR para asistencia técnica	Considerar las obligaciones legales basadas en su sector
Proteger los datos de clientes y partes interesadas	Mantener la transparencia con las partes afectadas	

Capítulo 10

Función de la OEA como Coordinador Regional

Realizar una estrategia nacional de ciberseguridad que sea compatible con los países de la región, y con la Organización de los Estados Americanos (OEA) como coordinador, es una iniciativa crucial y compleja que requiere un enfoque multidimensional y colaborativo.

Eduardo Jorge Martino

Coordinación y Liderazgo Regional

La OEA, a través de su Comité Interamericano contra el Terrorismo (CICTE), ya tiene un programa de ciberseguridad activo que apoya a los países miembros en esta tarea, lo que sienta una base sólida para la cooperación. La OEA sería el ente ideal para liderar y coordinar esta iniciativa, actuando como un catalizador y punto de encuentro. Su rol debería incluir:

Establecimiento de un marco de referencia

Definir los principios y estándares mínimos que cada país debe seguir en su estrategia nacional. Esto no busca homogeneizar, sino asegurar la compatibilidad y la interoperabilidad de las políticas.

Facilitar el intercambio de información

Crear una plataforma regional segura para el intercambio de inteligencia sobre amenazas, vulnerabilidades y ciberataques. Esto podría basarse en redes de Centros de Respuesta a Incidentes de Seguridad Informática (CSIRTs) nacionales, como la red CSIRTAmericas que ya promueve la OEA.

Armonización de legislaciones

Trabajar con los países miembros para alinear sus marcos legales sobre cibercrimen, siguiendo modelos como el Convenio de Budapest, para facilitar la cooperación judicial en la región.

Capacitación y desarrollo de capacidades

Organizar programas de formación, talleres y ejercicios cibernéticos regionales (como los "CyberEx") para fortalecer las habilidades de los profesionales en ciberseguridad en todos los países.

Promoción de la confianza y el diálogo

Servir como un foro neutral para el diálogo entre gobiernos, sector privado y sociedad civil, abordando temas sensibles como la ciberdiplomacia y el comportamiento responsable de los estados en el ciberespacio.

Pilares de la Estrategia Nacional Compatible

Una estrategia nacional compatible con el enfoque regional se basa en estos pilares:

Gobernanza y Marco Normativo

- Establecer una autoridad nacional de ciberseguridad para coordinar esfuerzos.
- Desarrollar legislación actualizada sobre ciberdelitos y protección de infraestructura crítica.

Construcción de Capacidades Técnicas

- Fortalecer o crear un CSIRT nacional para detectar y responder a incidentes.
- Invertir en tecnología de seguridad y laboratorios forenses digitales.

Cooperación Público-Privada y Regional

- Establecer colaboración con el sector privado y la academia.
- Participar en la cooperación regional (OEA) para compartir prácticas y responder a amenazas.

Cultura y Concientización

- Implementar campañas de concientización y educación sobre riesgos cibernéticos.
- Integrar ciberseguridad en currículos educativos y desarrollar fuerza laboral.

Pasos para la Implementación

La implementación de esta estrategia debería seguir una metodología estructurada, en la cual la OEA podría ofrecer su apoyo técnico:

- **Diagnóstico y Evaluación**

  Cada país debe diagnosticar su madurez en ciberseguridad, usando informes regionales de la OEA como base.

- **Formulación de la Estrategia**

  Basado en el diagnóstico, se formula la estrategia nacional, alineada con los principios regionales de la OEA.

- **Plan de Acción**

  Desarrollar un plan de acción detallado con objetivos a corto, mediano y largo plazo, asignando responsabilidades y recursos.

- **Implementación y Monitoreo**

  Implementar el plan y monitorear el progreso, ajustando la estrategia según la evolución de las ciberamenazas.

- **Evaluación y Revisión Continua**

  Evaluar y revisar periódicamente la estrategia para asegurar su efectividad, relevancia y resiliencia ante el entorno digital cambiante.

Una estrategia nacional de ciberseguridad coordinada por la OEA fortalece la protección individual y construye una defensa regional sólida contra las ciberamenazas globales.

Pérdidas Económicas en Países de la Región

Estimar las pérdidas económicas por ciberataques es un desafío complejo, ya que muchas empresas no reportan estos incidentes o el costo real se extiende más allá de la pérdida financiera directa (incluyendo daños a la reputación, costos de recuperación, multas regulatorias, etc.). Sin embargo, se pueden obtener algunas estimaciones y datos relevantes para Brasil, Colombia, Chile y Argentina.

Brasil

- **Costo promedio por violación de datos:** Un informe de IBM para el año 2025 estima que el costo promedio de una violación de datos en Brasil alcanza los R$ 7.19 millones.
- **Volumen de ataques:** En 2024, se registraron 356 mil millones de intentos de ciberataques en Brasil.
- **Impacto en empresas:** Un informe de PwC indica que el costo promedio de un ciberataque para una empresa puede ser de hasta 5.3 millones de dólares en pérdidas de flujo de caja, sin contar otros daños a la reputación.

Colombia

- **Volumen de ataques:** En 2023, Colombia experimentó 28 mil millones de ciberataques, y se espera que esta cifra sea superada ampliamente en 2024.
- **Costos para empresas:** Las empresas colombianas pueden incurrir en costos que oscilan entre USD 200,000 y USD 1,000,000 para mitigar ciberataques.
- **Sectores más afectados:** Los sectores financiero, empresarial, legal y gubernamental son los más atacados, aunque los ataques se están expandiendo a otras áreas como la salud y la construcción.

Pérdidas Económicas en Chile

Chile

- **Aumento de ataques:** Chile ha visto un aumento alarmante en los ciberataques, afectando especialmente a las pequeñas y medianas empresas (PyMEs) debido a la falta de recursos para invertir en ciberseguridad.
- **Costo estimado:** Según estudios, el costo de los ciberataques en Chile podría alcanzar los 3.000 millones de dólares anuales, considerando tanto pérdidas directas como indirectas (tiempo de inactividad, recuperación de datos, daño reputacional).
- **Sectores más afectados:** Los sectores financiero, de salud y retail son los más vulnerables y los que más pérdidas han reportado.

Pérdidas Económicas en Argentina

Argentina

- **Crecimiento de incidentes:** Argentina también ha experimentado un incremento significativo en los ciberataques. El país es uno de los más atacados de América Latina, con un aumento del 50% en incidentes reportados en los últimos años.
- **Impacto económico:** Aunque no existen cifras oficiales consolidadas, se estima que las pérdidas por ciberataques en Argentina podrían superar los 1.500 millones de dólares anuales. Esto incluye pérdidas por ransomware, fraudes financieros, robo de datos y ataques a infraestructuras críticas.
- **Sectores vulnerables:** Los sectores más afectados incluyen el financiero, el gubernamental y las empresas de servicios. Las PyMEs argentinas también son un blanco frecuente debido a la falta de inversión en ciberseguridad.

Es importante destacar que las estimaciones específicas para cada país pueden variar significativamente, ya que dependen de la metodología del estudio (encuestas, reportes de incidentes, análisis de costos, etc.). Sin embargo, la tendencia general es clara: **las pérdidas económicas por ciberataques están aumentando de manera exponencial en la región**, impulsadas por la sofisticación de las amenazas y la creciente dependencia de la tecnología. La ciberdelincuencia se está convirtiendo en una de las mayores economías ilícitas a nivel mundial, y los países de la región enfrentan un gran desafío para fortalecer sus defensas y proteger sus economías.

Capítulo 11

Resumen y Propuestas

Análisis de lo planteado, problemas registrados y propuestas para mejorar esta problemática

Eduardo Jorge Martino

Propuestas para Fortalecer la Ciberseguridad Nacional

Para enfrentar los desafíos identificados en materia de ciberseguridad, es fundamental implementar un conjunto de medidas estratégicas que fortalezcan las capacidades nacionales de prevención, detección y respuesta ante amenazas cibernéticas.

1

Implementar Control Estratégico en Puntos Críticos

Establecer centros de monitoreo y análisis de tráfico en puntos estratégicos como Las Toninas, donde ingresan los cables submarinos de fibra óptica, para detectar amenazas en tiempo real.

2

Fortalecer el Repositorio Nacional de Incidentes

Consolidar y expandir el repositorio nacional de ciberseguridad para centralizar información sobre amenazas, vulnerabilidades y ataques, facilitando el análisis de tendencias y la toma de decisiones.

3

Aumentar la Coordinación Interinstitucional

Mejorar la colaboración entre CERT.ar, la Dirección Nacional de Ciberseguridad, fuerzas de seguridad y el sector privado para una respuesta coordinada ante incidentes de gran escala.

4

Desarrollar Capacidades Técnicas y Humanas

Invertir en formación especializada y actualización continua del personal dedicado a la ciberseguridad en todos los niveles del Estado.

5

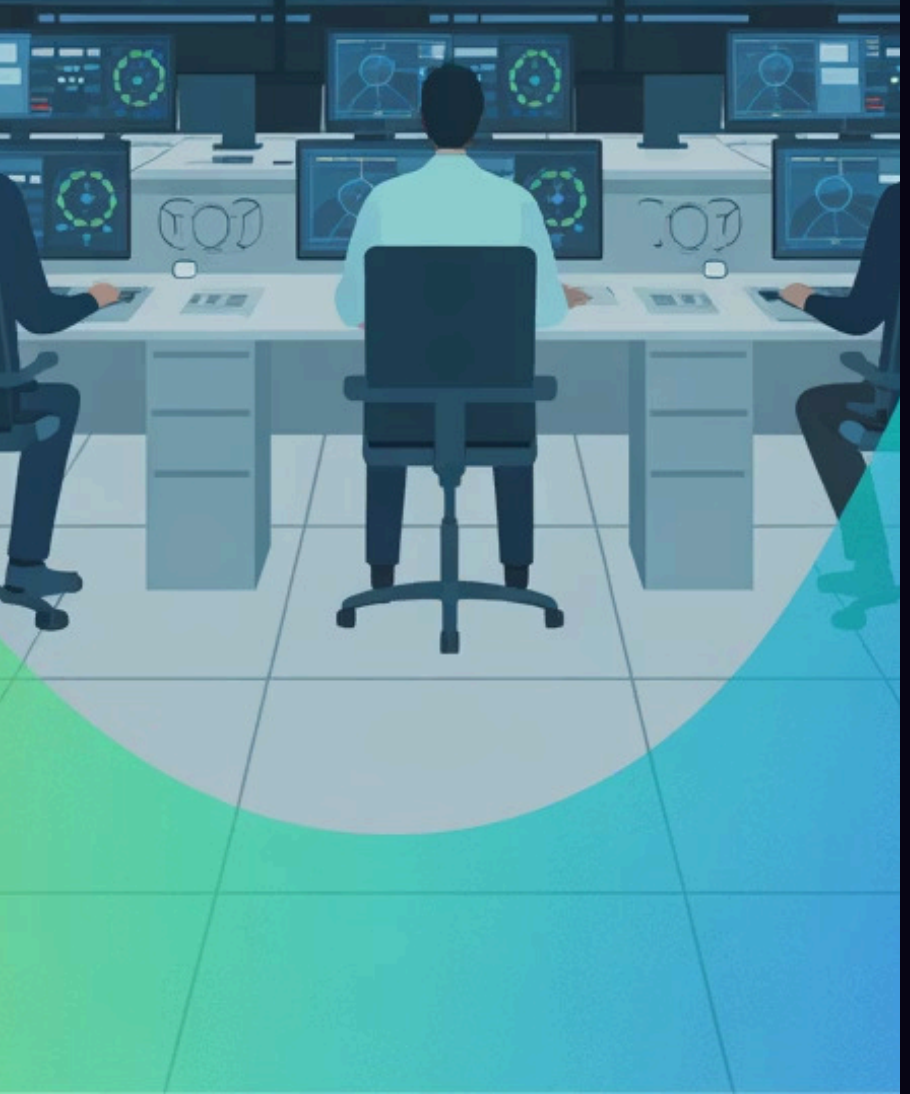
Promover la Concientización Ciudadana

Implementar campañas de educación y sensibilización sobre ciberseguridad dirigidas a ciudadanos, empresas y organismos públicos.

6

Actualizar el Marco Normativo

Revisar y actualizar la legislación vigente para adaptarla a las nuevas amenazas y tecnologías emergentes, asegurando su compatibilidad con estándares internacionales.



Control y Gestión de Amenazas

En el ámbito de la ciberseguridad, es fundamental establecer un control y monitoreo de la red en puntos estratégicos, con especial atención a la infraestructura crítica, donde el Estado debe ejercer una supervisión activa. Esto no solo garantiza la seguridad de los sistemas vitales, sino que también permite la coordinación efectiva entre las diferentes agencias de seguridad para una respuesta unificada.

La gestión de amenazas implica la implementación de mecanismos robustos de detección de amenazas y la capacidad de respuesta rápida ante incidentes, con la participación activa de cuerpos nacionales de ciberseguridad como CERT.ar y otras entidades dedicadas a la gestión y análisis de ciberincidentes.

Monitoreo de Infraestructura Crítica

Supervisión continua y control de tráfico en puntos estratégicos de la red, especialmente en infraestructura crítica esencial, garantizando la resiliencia de los servicios fundamentales.

Coordinación Interinstitucional

Fomento de la colaboración y el intercambio de información entre las agencias de seguridad, tanto a nivel nacional como regional, para una respuesta cohesionada y eficaz ante ciberamenazas.

Capacidades de Respuesta y Marco Normativo

La efectividad en la gestión de ciberamenazas requiere no solo de capacidades técnicas avanzadas, sino también de un marco legal y regulatorio sólido que establezca las bases para una protección integral del ciberespacio nacional.

Detección y Respuesta

Desarrollo e implementación de capacidades avanzadas para la detección temprana de ciberataques y la ejecución de planes de respuesta rápida para mitigar su impacto, con el apoyo de entidades como CERT.ar.

Marco Regulatorio

Establecimiento de una normativa clara y robusta que regule las prácticas de ciberseguridad, defina responsabilidades y promueva la inversión en protección digital para todos los sectores.

Problemática de la Ciberseguridad Nacional

En los diferentes Capítulos se ha tratado de hacer entender la problemática de la Ciberseguridad. En la introducción se diferencia la importancia de las conexiones de nuestro país utilizando Fibra Óptica submarina o terrestre con otros países y los enlaces satelitales, marcando la enorme diferencia de capacidad de tráfico de la Fibra Óptica con respecto a la conectividad satelital.

Entendiendo que la conexión con el mundo por medio de tendidos de fibra óptica representa una necesidad humana en todo sentido de su desarrollo, pero por esos vínculos somos susceptibles todo tipo de ataque que ponen en riesgo no solo a los usuarios particulares sino también a las grandes infraestructuras nacionales y privadas. Ya hemos tenido en nuestro país perdida de información del Registro Nacional de las Personas, del Automotor, etc.

> "Una alerta que se debe tener en cuenta es que siendo la localidad de Las Toninas un punto tan estratégico no haya un control del estado analizando el trafico que ingresa y sale de nuestro territorio."

Conclusiones y Camino a Seguir

En resumen, tenemos mucho por hacer y el primer paso es **reconocer que somos vulnerables**, contar con una estrategia nacional de Ciberseguridad consensuada con la OEA.

Esto permite que los países miembros definamos los distintos malware con los mismos términos para facilitar los trabajos de cooperación internacional y aporte a la justicia.

Reconocimiento de Vulnerabilidades

Aceptar nuestra exposición a amenazas cibernéticas como primer paso hacia una defensa efectiva.

Estrategia Nacional Consensuada

Desarrollar una estrategia de ciberseguridad alineada con los estándares regionales de la OEA.

Cooperación Internacional

Establecer terminología común y protocolos compartidos para facilitar la colaboración entre países miembros.

Apoyo a la Justicia

Crear marcos legales armonizados que permitan una persecución efectiva del cibercrimen transnacional.