Ciberseguridad para redes de comunicación e infraestructura crítica en organismos estatales

Juan Ignacio Munte – Universidad de Palermo – Buenos Aires – Argentina
Tutor: Mgr. Pablo Alejandro Lena.

***Resumen*:** La presente investigación aborda la ciberseguridad desde múltiples perspectivas, comenzando por un análisis de la evolución de los ciberataques y ciberarmas, así como la problemática específica en Argentina, incluyendo los ataques a sectores gubernamentales.

Se proponen soluciones basadas en el marco NIST CSF y el enfoque Zero Trust para abordar los desafíos actuales y futuros en ciberseguridad. Además, se identifican áreas de investigación futura en la optimización de microservicios y la integración de la seguridad en el desarrollo de software. El mismo subraya la importancia de la conciencia y capacitación en ciberseguridad, mientras que los anexos ofrecen información adicional para respaldar los hallazgos y conclusiones presentados.

I. Nomenclatura

OEA: Organización de los Estados Americanos.
VPN: Virtual Prívate Network
CEH: Certified Ethical hacker
WAF: Web Application Firewalls
DMZ: Desmilitarized zone (zona desmilitarizada)
DDOS: Distributed Denial of Service.
SQLi: Structured query language inyection
RCE: Ejecución Remota de Código
NIST: National Institute of Standards and Technology
DC: Data Center
CIP: comunicación e infraestructura crítica
MFA: multi factor authentication.
SOC: Security operation Center.
IDP: Intrusion Detection System
IPS: Intrusion Penetration System
SIEM: Security Information and Event Management
DRP: Disaster Recovery Plan
EDR: Endpoint Detection and Response
ONTI: Oficina Nacional de Tecnologías de la Información
XDR: eXtended Detection & Response

II. Introducción

En la era digital en la que vivimos, el ciberespacio se ha convertido en un campo de batalla cada vez más relevante, donde los conflictos y las confrontaciones adoptan nuevas formas y dimensiones. En este escenario, los ciberataques y las ciberarmas emergen como herramientas de poder y dominio, capaces de desencadenar consecuencias devastadoras a nivel global. Comprender el origen y la evolución de estos fenómenos se vuelve crucial para anticipar y mitigar sus efectos en la seguridad cibernética y la estabilidad internacional.

El presente trabajo se propone indagar en los orígenes de los ciberataques y las ciberarmas, explorando los eventos y actores clave que han marcado su desarrollo. Desde sus primeras manifestaciones hasta las sofisticadas operaciones actuales, estos fenómenos han evolucionado en paralelo al avance tecnológico y a la creciente interconexión de sistemas informáticos a nivel mundial.

Entre los ciberataques más notorios que han sacudido la esfera digital, se destacan nombres como Stuxnet [2], un malware diseñado para sabotear sistemas de control industrial, Flame [3] un malware diseñado para el ciber espionaje y WannaCry[4], un ransomware que afectó a miles de organizaciones en todo el mundo, Conficker, tiene la capacidad de desactivar funciones de seguridad, bloquear actualizaciones del sistema operativo y antivirus, y crear una red de bots controlados remotamente por los atacantes. Estos incidentes ilustran la diversidad de amenazas que enfrenta la ciberseguridad, desde ataques dirigidos a infraestructuras críticas hasta campañas de extorsión masiva.

Asimismo, la proliferación de ciberarmas ha generado una nueva dimensión en el panorama de la seguridad internacional. Ejemplos emblemáticos incluyen programas de espionaje cibernético como Equation Group[1], atribuido a agencias de inteligencia estatales, y el desarrollo de exploit como EternalBlue, utilizado en ataques de alcance global como WannaCry. Estas herramientas no solo representan una amenaza para la integridad de sistemas y datos, sino que también plantean desafíos éticos y legales en el ámbito de la guerra cibernética.

En este contexto, el análisis detallado de los orígenes y características de los ciberataques y las ciberarmas resulta fundamental para comprender la complejidad de los desafíos que enfrenta la seguridad cibernética en la actualidad. Al abordar estos temas, esta investigación busca contribuir al desarrollo de estrategias efectivas de prevención y respuesta, con el objetivo de fortalecer la resiliencia de las sociedades frente a las amenazas emergentes en el ciberespacio.

En este contexto, el análisis detallado de los orígenes y características de los ciberataques y las ciberarmas resulta fundamental para comprender la complejidad de los desafíos que enfrenta la seguridad cibernética en la actualidad. Al abordar estos temas, esta investigación busca contribuir al

desarrollo de estrategias efectivas de prevención y respuesta, con el objetivo de fortalecer la resiliencia de las sociedades frente a las amenazas emergentes en el ciberespacio. Además, se ofrece una sección de capítulos que profundiza en las características específicas de cada tipo de ataque y arma cibernética, proporcionando un marco completo para el análisis y la comprensión de estos fenómenos.

El desarrollo de este documento se llevará a cabio en las próximas secciones. En primer lugar, el Capítulo II, es crucial para establecer el contexto general, incluyendo la historia y evolución de los ciberataques y ciberarmas. En este capítulo inicial, se puede proporcionar una breve reseña histórica sobre los primeros ciberataques documentados, así como también sobre las primeras ciberarmas desarrolladas y utilizadas. Por otro lado, el Capítulo III proporciona un análisis detallado de los antecedentes y la problemática específica en Argentina en relación con la ciberseguridad en el ámbito gubernamental, sentando las bases para comprender mejor el contexto en el que se enmarca en el trabajo final. Además, en el capítulo IV, se explorarán diversas tecnologías y tipos de ciberataques que representan una amenaza para la seguridad cibernética en la actualidad. Desde ataques dirigidos a la infraestructura hasta distintas tácticas utilizadas por los actores maliciosos. En Consecuencia, en el capítulo V, se analizarán los riesgos, vulnerabilidades y amenazas que enfrentan los activos estratégicos de las organizaciones gubernamentales en Argentina, así como los ciber riesgos asociados a los sistemas estratégicos en las infraestructuras críticas del país. La identificación y comprensión de estas amenazas son fundamentales para desarrollar estrategias efectivas de protección y mitigación de riesgos cibernético. Posteriormente, en el capítulo VI, se proponen soluciones para abordar los desafíos identificados en los capítulos anteriores en relación con la ciberseguridad en las organizaciones gubernamentales de Argentina. Se presentan dos enfoques principales: Normativas y Directrices de Ciberseguridad, y el modelo Zero Trust. Cada uno de estos enfoques se analiza en detalle, destacando su relevancia y aplicabilidad en el contexto local. De esta manera, en el Capítulo VII, se presentan las conclusiones derivadas del análisis y desarrollo de los temas previamente abordados en la tesis. Este capítulo sintetiza los hallazgos obtenidos a partir de la aplicación del framework del NIST y del enfoque de Zero Trust en las infraestructuras de los centros de datos, así como de otros aspectos relevantes de la ciberseguridad y las ciberarmas. Asimismo, en el Capítulo VIII, titulado "Agradecimientos", se brinda la oportunidad al autor de expresar su reconocimiento y gratitud hacia las personas, instituciones o entidades que han contribuido de alguna manera al desarrollo y finalización de la tesis. Por otra parte, en el Capítulo IX, titulado "Referencias", se presenta una lista detallada de todas las fuentes utilizadas y citadas en la tesis. Igualmente, en el capítulo X anexos, se proporciona información adicional que complementa y respalda los argumentos y hallazgos presentados en la tesis. Además, en el capítulo XI, las futuras líneas de investigación en el ámbito de los microservicios, que incluyen tecnologías como Docker y Kubernetes, junto con el desarrollo de software seguro, representan un campo prometedor y en constante evolución en el ámbito de la informática y la seguridad cibernética. Finalmente, en el Capítulo XII, titulado "Biografías", se proporciona información sobre el autor que realizo la tesis.

III. Antecedentes y problemática actual.

En el contexto de la ciberseguridad en Argentina, las páginas y entidades gubernamentales han experimentado una serie de antecedentes que han marcado su evolución en este ámbito. A lo largo de los años, el país ha enfrentado diversos desafíos y ha implementado medidas para fortalecer su infraestructura digital y protegerse contra amenazas cibernéticas.

Uno de los hitos significativos en esta área fue la creación en 2010 de la Oficina Nacional de Tecnologías de la Información (ONTI)[4], dependiente de la Jefatura de Gabinete de ministros. Esta entidad tuvo como objetivo coordinar las políticas y estrategias relacionadas con las tecnologías de la información y la comunicación (TIC) en el ámbito gubernamental, incluyendo aspectos de ciberseguridad.

A medida que la dependencia del gobierno en las TIC aumentaba, también lo hizo la conciencia sobre la importancia de proteger la infraestructura digital del país. En este sentido, se han llevado a cabo diversas iniciativas para mejorar la seguridad cibernética en las páginas y sistemas gubernamentales. Estas incluyen la adopción de estándares de seguridad, la implementación de medidas de protección contra ataques cibernéticos y la capacitación del personal en temas de ciberseguridad.

Sin embargo, a pesar de estos esfuerzos, las páginas y entidades gubernamentales de Argentina no están exentas de incidentes cibernéticos. Se han reportado casos de ataques informáticos, filtraciones de datos y otras amenazas que han puesto a prueba las defensas cibernéticas del país.

A. Renaper

El hackeo al Registro Nacional de las Personas (Renaper) en 2021 representó un evento significativo en la historia reciente de la ciberseguridad en Argentina. Durante julio de ese año, se informó sobre un incidente cibernético que impactó a este organismo gubernamental encargado de la identificación de los ciudadanos argentinos y la emisión de documentos de identidad, entre otros servicios asociados.

El ataque, cuyos detalles específicos no fueron completamente divulgados al público, generó preocupación en todo el país debido a la naturaleza sensible de la información manejada por el Renaper. El 09 de abril del 2024 se pusieron en venta 100.000 datos obtenidos del Renaper la numeración comienza entre los 10 millones hasta 57 millones (significa que hay DNI que son de menores).

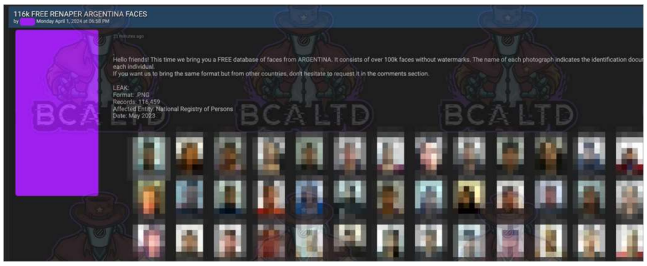


Figura N°1 Base de datos publicada con DNI.

B. Pami

El 02 de agosto 2023 el Programa de Atención Médica Integral (PAMI) fue víctima de un ciberataque un ransomware llamado RHYSIDA[5], el cual se comprometieron los datos de todos los afiliados de la obra social en los cuales se encontraron un total de 1.6 millones de archivos en la dark-web, los mismos contenían historiales clínicos, estudios, otros datos personales. Los usuarios de la obra social no podrían gestionar sus recetas, las compras de medicamentos, las mismas durante las contingencias se realizaron en formato papel.
Dentro de una plataforma de servicios de mensajes publicaron recetas y se podían gestionar desde el mismo.

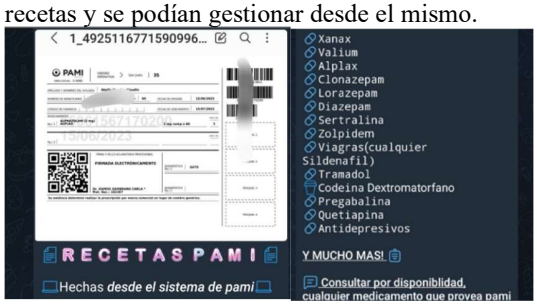


Figura N°2Receta de obra social y medicamentos para solicitar

C. AFIP

En febrero de 2024, un grupo de ciberdelincuentes llevó a cabo un hackeo masivo que comprometió la seguridad de la Administración Federal de Ingresos Públicos (AFIP) en Argentina. Durante este incidente, más de 82,000 claves fiscales fueron filtradas y expuestas en la dark web . Algunos detalles:

Las credenciales fueron obtenidas directamente de los usuarios mediante distintos métodos.

Fueron una filtración de credenciales.

Las 82,000 claves fiscales comprometidas permitían a los usuarios realizar diversas acciones, como inscribirse en impuestos, presentar planes de pago, facturar, presentar declaraciones juradas y más.

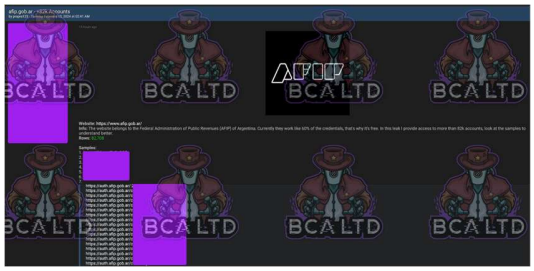


Figura N°3 Listado de contribuyentes y sus Contraseñas.

D. Problemática actual

La problemática actual de los organismos estatales en Argentina abarca una variedad de desafíos que afectan su eficiencia, transparencia y capacidad para brindar servicios públicos de calidad. Algunas de las principales problemáticas incluyen:

Falta de recursos: Muchos organismos estatales enfrentan limitaciones presupuestarias y de personal, lo que afecta su capacidad para cumplir con sus funciones y responder a las necesidades de la población de manera adecuada.

Tecnología obsoleta: La falta de actualización tecnológica en algunos organismos estatales dificulta la implementación de procesos eficientes y la prestación de servicios digitales modernos.

Concientización: La concientización en ciberseguridad es fundamental en la actualidad debido al creciente número de amenazas cibernéticas.

Ver anexo I

IV. Enumeración de la tecnologías y tipos de ciber ataques

A. Enumeración de las tecnologías

En el marco teórico de esta investigación, se abordan distintas tecnologías y tipos de ciberataques que constituyen una amenaza creciente en el panorama de la seguridad cibernética. Comprender estos conceptos es fundamental para contextualizar el análisis de la problemática y las estrategias de mitigación. A continuación, se presenta una enumeración de algunas de las tecnologías y tipos de ciberataques más relevantes:

Tecnologías:

Servidores web:
Los servidores web son sistemas que hospedan sitios web y aplicaciones en línea. Pueden clasificarse en servidores frontend y backend.

Los servidores frontend manejan las solicitudes de los usuarios y sirven contenido estático como HTML, CSS y JavaScript.

Los servidores backend manejan la lógica de la aplicación y la interacción con la base de datos, generando contenido dinámico en respuesta a las solicitudes de los usuarios.

Firewalls:
Los firewalls son dispositivos de seguridad que controlan el tráfico de red entrante y saliente según un conjunto de reglas predefinidas.

Pueden ser hardware o software y se utilizan para proteger la red y los sistemas contra intrusiones no autorizadas y malware.

Web Application Firewall (WAF):
Un WAF es un tipo de firewall diseñado específicamente para

proteger aplicaciones web contra ataques como inyecciones SQL, cross-site scripting (XSS) y ataques de denegación de servicio (DDoS).

Analiza el tráfico HTTP y filtra las solicitudes maliciosas antes de que lleguen al servidor web.

Zona Desmilitarizada (DMZ):

Una DMZ es una red separada y protegida que se encuentra entre la red interna de una organización y la red externa, como Internet.

Se utiliza para alojar servicios públicos, como servidores web y de correo electrónico, mientras se protege la red interna de posibles ataques.

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):

Los IDS monitorean el tráfico de red en busca de actividades sospechosas y generan alertas cuando se detectan posibles intrusiones.

Los IPS van un paso más allá al bloquear automáticamente el tráfico malicioso o sospechoso.

Controles de Acceso e Identidad:

Los controles de acceso definen y regulan quién tiene acceso a los recursos y datos de la red.

La gestión de identidades asegura que solo los usuarios autorizados puedan acceder a sistemas y datos, mediante la autenticación y autorización adecuadas.

Redes Privadas Virtuales (VPN):

Las VPN permiten a los usuarios acceder de forma segura a una red privada a través de una conexión cifrada a través de Internet.

Se utilizan para proteger la comunicación y el intercambio de datos sensibles entre usuarios remotos y la red corporativa.

Virtualización:

La virtualización de servidores y equipos de comunicaciones es una práctica que permite crear múltiples instancias virtuales de sistemas físicos en un entorno compartido. En el caso de los servidores, la virtualización implica la creación de múltiples máquinas virtuales (VM) en un único servidor físico, lo que maximiza la eficiencia del hardware y optimiza la utilización de recursos. Esto se logra mediante un software de virtualización, conocido como hipervisor, que gestiona y asigna los recursos de manera dinámica entre las diferentes VM.

La virtualización de equipos de comunicaciones se refiere a la creación de redes virtuales y dispositivos de red en un entorno virtualizado. Esto permite simular y emular la funcionalidad de dispositivos de red físicos, como routers, switches y firewalls, en un entorno virtual. La virtualización de equipos de comunicaciones proporciona flexibilidad y escalabilidad, permitiendo a las organizaciones implementar y gestionar redes de manera más eficiente y rentable.

Antivirus:

Los antivirus son programas diseñados para detectar, prevenir y eliminar software malicioso, como virus, gusanos, troyanos y spyware, de los sistemas informáticos. Utilizan una variedad de técnicas, como la detección de firmas, análisis heurísticos y técnicas de comportamiento, para identificar y neutralizar amenazas. Los antivirus juegan un papel fundamental en la protección de los dispositivos y redes contra ataques cibernéticos al detectar y eliminar programas maliciosos antes de que puedan causar daño.

EDR / XDR (Endpoint Detection and Response / Extended Detection and Response):

EDR es una solución de seguridad que se centra en la detección y respuesta a amenazas en los puntos finales de una red. Utiliza tecnologías avanzadas de detección de amenazas, como el análisis de comportamiento y la correlación de eventos, para identificar actividades sospechosas y responder a ellas de manera oportuna. XDR va más allá de EDR al integrar datos de múltiples fuentes, como puntos finales, redes y nubes, para proporcionar una visión más completa de las amenazas y facilitar una respuesta coordinada y efectiva.

DLP (Data Loss Prevention):

DLP es una estrategia y conjunto de herramientas diseñadas para prevenir la fuga de datos confidenciales fuera de una organización. Esto se logra mediante la identificación, supervisión y control de la transferencia de datos confidenciales dentro y fuera de la red de la organización. Las soluciones de DLP pueden utilizar técnicas como el cifrado, la monitorización de contenido y el bloqueo de transferencias no autorizadas para proteger datos sensibles y cumplir con regulaciones de privacidad y seguridad de datos.

B. Tipos de ciberataques:

Ransomware:

El ransomware es un tipo de malware que cifra los archivos o sistemas de una víctima y exige un pago de rescate a cambio de la clave de descifrado. Este ataque puede paralizar las operaciones comerciales, comprometer datos críticos y causar daños financieros significativos a las organizaciones afectadas [6].

Phishing:

El phishing es una técnica utilizada por ciberdelincuentes para obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por entidades legítimas a través de correos electrónicos, mensajes de texto o llamadas telefónicas. Este tipo de ataque puede resultar en robo de identidad, fraude financiero y compromiso de cuentas en línea [7].

Pharming:

Es una técnica de ciberataque en que se redirige el tráfico de un sitio web legítimo a un sitio web falso que parece idéntico al original. El objetivo principal de un ataque de pharming es engañar a los usuarios para que proporcionen información confidencial, como nombres de usuario, contraseñas y datos financieros, creyendo que están interactuando con el sitio web legítimo.

Se puede llevar a cabo de varias maneras:

DNS cache poisoning (*Envenenamiento de caché DNS*): En

este método, los atacantes comprometen los servidores DNS, y que resuelvan un nombre de dominio legítimo con la dirección IP del sitio falso. Esto puede afectar a múltiples usuarios, ya que los servidores DNS son utilizados por muchas computadoras para la resolución de nombres de dominio.

Manipulación del archivo hosts: El archivo hosts de una computadora es un archivo de texto que traduce nombres de dominio en direcciones IP. Los atacantes pueden modificar este archivo para que el nombre de dominio de un sitio web legítimo se traduzca en la dirección IP del sitio web falso, para realizar la modificación el malware necesita privilegios de administrador para poder realizar los cambios.

Ataques de Denegación de Servicio (DDoS):

Los ataques de denegación de servicio buscan sobrecargar los recursos de un sistema o red mediante el envío masivo de tráfico, lo que provoca una interrupción en el acceso a los servicios legítimos. Estos ataques pueden causar pérdidas financieras, dañar la reputación de la marca y afectar la disponibilidad de servicios en línea[8].

Ingeniería Social:

La ingeniería social es una técnica que implica manipular a las personas para obtener información confidencial o persuadirlas a realizar acciones perjudiciales. Esto puede incluir el uso de pretextos, la falsificación de identidades o la explotación de la confianza de las víctimas para obtener acceso no autorizado a sistemas o datos. Los ataques de ingeniería social pueden resultar en robo de información confidencial, acceso no autorizado a sistemas y compromiso de la seguridad de la información [9].

Inyección SQL (SQLi):

La inyección SQL es un tipo de ataque que aprovecha las vulnerabilidades en las aplicaciones web para ejecutar comandos SQL no deseados en la base de datos subyacente. Esto puede permitir a un atacante acceder, modificar o eliminar datos confidenciales, comprometiendo la integridad y la seguridad de la aplicación y los datos almacenados [10].

Cross-Site Scripting (XSS):

El Cross-Site Scripting (XSS) es un tipo de vulnerabilidad que permite a un atacante insertar scripts maliciosos en páginas web visitadas por otros usuarios. Estos scripts pueden ejecutarse en el navegador de la víctima y robar cookies de sesión, redirigir a páginas fraudulentas o modificar el contenido de la página, comprometiendo la seguridad y la privacidad de los usuarios afectados[10].

Ataques de Fuerza Bruta:

Los ataques de fuerza bruta son intentos repetidos de adivinar credenciales de acceso mediante la prueba sistemática de todas las combinaciones posibles de nombres de usuario y contraseñas. Esto puede permitir a un atacante obtener acceso no autorizado a sistemas y aplicaciones protegidos, comprometiendo la confidencialidad y la seguridad de la información[11].

Ataques de Explotación de Vulnerabilidades:

Los ataques de explotación de vulnerabilidades aprovechan las debilidades en el software y los sistemas para ejecutar código malicioso o acceder a recursos no autorizados. Esto puede incluir ataques contra sistemas operativos, aplicaciones web, servidores y dispositivos de red, comprometiendo la integridad y la seguridad de los sistemas afectados.

Estos ataques web adicionales representan amenazas significativas para la seguridad cibernética y la integridad de los sistemas y datos en línea[10].

V. Riesgos, Vulnerabilidades y amenazas

A. Activos estratégicos de las organizaciones.

Estos activos estratégicos están expuestos a una serie de amenazas cibernéticas, como se menciona en el Capítulo III, que incluyen malware, ataques de phishing, vulnerabilidades de seguridad en sistemas operativos y aplicaciones, entre otros. La explotación de estas vulnerabilidades puede poner en riesgo la integridad, la confidencialidad y la disponibilidad de la información crítica para el funcionamiento del gobierno y la prestación de servicios públicos.

Por lo tanto, proteger estos activos estratégicos es crucial para garantizar la seguridad y la estabilidad del gobierno y la sociedad en su conjunto. Esto implica implementar medidas de seguridad cibernética robustas, como firewalls, sistemas de detección de intrusiones, cifrado de datos, autenticación de usuarios, entre otros, como se menciona en el Capítulo 3.

B. Ciber riesgos para los sistemas estratégico

En el contexto de las aplicaciones e infraestructura gubernamentales en Argentina, las amenazas cibernéticas representan un desafío significativo para la seguridad y la integridad de los sistemas críticos. Estas aplicaciones e infraestructuras, que pueden incluir sistemas de gestión de servicios públicos, plataformas de información ciudadana, sistemas administrativos, así como la infraestructura subyacente de red y servidores, son esenciales para el funcionamiento eficiente del gobierno y la prestación de servicios esenciales a la población.

Las amenazas cibernéticas a las aplicaciones e infraestructura gubernamentales en Argentina pueden manifestarse de diversas formas, dentro del capítulo IV se detallan varios ciber ataques.

C. Organismos de control de ciberseguridad en Argentina

Dirección Nacional de Ciberseguridad:

La Dirección depende de la Secretaría de Innovación Pública. Es la encargada de coordinar y supervisar las políticas de ciberseguridad a nivel nacional. Su misión incluye la creación de estrategias, normativas y programas de formación en ciberseguridad [13].

Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERT.ar):

Forma parte de la Dirección Nacional de Ciberseguridad, es el equipo de respuesta a incidentes de seguridad informática del país. Su función principal es gestionar y coordinar la respuesta a incidentes de ciberseguridad, así como ofrecer servicios de alerta temprana y análisis de amenazas[14].

Ministerio de Seguridad:

Tiene diversas áreas que trabajan en ciberseguridad, como la Policía Federal Argentina y la Gendarmería Nacional. Estas fuerzas de seguridad cuentan con unidades especializadas en delitos cibernéticos que investigan y persiguen actividades ilícitas en línea[15].

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI):

Dependiente del Ministerio Público Fiscal, es responsable de la investigación y persecución de delitos informáticos. Su objetivo es combatir la ciberdelincuencia y coordinar con otros organismos y fuerzas de seguridad para la efectiva persecución penal de estos delitos[16].

Defensoría del Pueblo de la Nación:

Es un área dedicada a la protección de los derechos de los ciudadanos en el ámbito digital, incluyendo la protección de datos personales y la privacidad [17].

Agencia de Acceso a la Información Pública (AAIP):

Es la autoridad de control en materia de protección de datos personales. Aunque su foco principal es la privacidad y protección de datos, sus funciones se extienden a la seguridad de la información y el cumplimiento de las normativas relacionadas[18].

Ente Nacional de Comunicaciones (ENACOM):

Regula las telecomunicaciones y los servicios de Internet en Argentina. Trabaja en la implementación de políticas y normativas que aseguran la seguridad y resiliencia de las infraestructuras críticas de información y comunicación[19].

VI. SOLUCIONES PROPUESTAS

A. Normativas y Directrices de Ciberseguridad

Este primer enfoque se centra en la importancia de establecer normativas y directrices específicas de ciberseguridad para las organizaciones gubernamentales en Argentina. Se exploran las mejores prácticas internacionales en materia de regulación y se examina cómo estas pueden adaptarse y aplicarse de manera efectiva en el ámbito local. El framework del NIST CSF (Framework de Ciberseguridad del Instituto Nacional de Estándares y Tecnología) [12] proporciona un marco estructurado y adaptable para fortalecer la postura de seguridad cibernética de las organizaciones gubernamentales en Argentina.

Al iniciar la descripción de este enfoque en el capítulo, se puede hacer énfasis en la importancia de contar con un marco reconocido a nivel internacional, como el NIST CSF, que ofrece una guía integral para evaluar, mejorar y comunicar la postura de ciberseguridad de una organización. Este marco se basa en cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperarse, y ofrece un enfoque holístico para abordar los riesgos cibernéticos de manera efectiva.

Dentro del marco de trabajo para la ciberseguridad, la Organización de los Estados Americanos (OEA) y el Instituto Nacional de Estándares y Tecnología (NIST) son responsables del desarrollo del Cibersecurity Framework (CSF 2.0). Este marco permite un enfoque de seguridad aplicable en todos los sectores de infraestructura crítica, donde se prioriza la orientación hacia la prioridad, el respeto, el rendimiento y la rentabilidad en la identificación, evaluación y gestión del riesgo. Además, busca identificar áreas de mejora para cada sector, facilitando así la implementación de medidas de seguridad cibernética efectivas y consistentes en todo el espectro de infraestructuras críticas.

El Framework CIS 2.0 consta de tres componentes principales, diseñados para proporcionar una estructura sólida y adaptable para mejorar la ciberseguridad en las organizaciones:

CSF Core: Este componente establece un conjunto central de actividades, categorizadas en las funciones principales de ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperarse. Estas actividades son fundamentales para la gestión integral del riesgo cibernético y sirven como base para el desarrollo de estrategias y controles de seguridad específicos.

Tabla 1 Nombres e identificadores de funciones y categorías principales de CSF 2.0

Función	Categoría	Identificador de Categoría
Gobernar (GV)	Contexto organizacional	GV.OC
	Estrategia de Gestión de riesgo	GV.RM
	Funciones, responsabilidades y autoridades	GV.RR
	Politica	GV.PO
	Vigilancia	GV.OV
	Gestión de riesgos de la cadena de suministro de ciberseguridad	GV.SC
Identificar (ID)	Gestion de Archivos	ID.AM
	Evaluacion de riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de identidades, Autenticación y control de acceso	PR.AA
	Concientización y capacitación	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de la plataforma	PR.PS
	Resiliencia de la infraestructura tecnológica	PR.IR
Detectar (DE)	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder (RS)	Administración de Incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Informes y comunicación de respuesta a incidentes	RS.CO
	Mitigación de Incidente	RS.IR
Recuperar (RC)	Ejecución de un plan de recuperación de incidentes	RC.RP
	Comunicación de recuepración de incidentes	RC.CO

CSF Tiers: Los Tiers (Niveles) del Framework CIS representan la madurez de la ciberseguridad de una organización. Estos niveles van desde "Inicial" hasta "Optimizado" e indican el grado de formalización y eficacia de los procesos de ciberseguridad implementados. Cada nivel refleja una progresión en la capacidad de la organización para gestionar y mitigar los riesgos cibernéticos de manera efectiva.

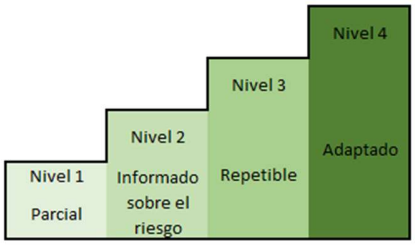


Figura N° 4 Niveles del CSF para la gobernanza y gestión de riesgo de ciberseguridad

CSF Profile: El Perfil del Framework CIS permite a las organizaciones personalizar y adaptar el marco a sus necesidades específicas de ciberseguridad. Esto se logra mediante la selección y la priorización de actividades y controles relevantes de acuerdo con los objetivos de negocio, los riesgos identificados y los recursos disponibles. El Perfil ayuda a las organizaciones a establecer un enfoque de ciberseguridad que sea práctico, eficiente y alineado con sus metas y prioridades.



Figura N°5 Pasos para crear y utilizar un perfil organizacional

La evaluación del impacto de la implementación del framework mencionado (CSF) requiere un enfoque integral que abarque todos los aspectos de la infraestructura de un data center, desde los dispositivos de red hasta los sistemas y estaciones de trabajo. Además, se destaca la necesidad de capacitar a los operadores que administran los sistemas, así como a los usuarios finales, para prevenir eventos anómalos, realizar pruebas de seguridad, llevar a cabo el relevamiento y mantenimiento de todos los dispositivos con sus actualizaciones correspondientes. A continuación, se analizan algunos posibles impactos:

Mejora en la seguridad de CIP: La implementación de medidas y controles de seguridad sólidos contribuirá a proteger la infraestructura del datacenter contra amenazas cibernéticas. La identificación del riesgo, la implementación de controles y la respuesta a incidentes permitirán una protección mejorada contra las nuevas amenazas.

La disponibilidad de servicios se asegura mediante una estrategia de respaldo y recuperación ante desastres que garantiza la continuidad del servicio afectado por un incidente de ciberseguridad.

La protección de datos confidenciales es fundamental, y se logra implementando medidas como la autenticación de usuarios al acceder a recursos, la encriptación de documentos y la implementación de controles y auditorías de accesos. Estos mecanismos contribuyen a proteger los datos dentro del organismo.

Dentro del Anexo II se encuentra una descripción más detallada sobre el tema del CSF.

B. Zero trust

El modelo Zero Trust es un enfoque de seguridad cibernética que desafía el concepto tradicional de confianza implícita dentro de las redes corporativas. En lugar de confiar en la seguridad perimetral y en la autenticación basada en la red, el modelo Zero Trust asume que tanto los usuarios internos como externos, así como los dispositivos y las aplicaciones, pueden ser comprometidos en cualquier momento.

En este modelo, se implementa una estrategia de seguridad que verifica constantemente la identidad y la seguridad de cada usuario y dispositivo antes de permitir el acceso a los recursos de la red. Esto se logra mediante la aplicación de políticas de seguridad granulares y basadas en el contexto, que controlan y restringen el acceso a los sistemas y datos según la identidad del usuario, el estado del dispositivo, el comportamiento de la red y otros factores relevantes.

Para ser completamente efectivos en la minimización del riesgo y en la habilitación de respuestas sólidas y oportunas, los principios y conceptos de Zero Trust deben impregnar la mayoría de los aspectos de la red y su ecosistema de operaciones. Desde el director ejecutivo hasta el ingeniero o el operador, es crucial que las organizaciones comprendan y se comprometan con la mentalidad de Zero Trust antes de proceder con la implementación.

Los actores de amenazas contemporáneos, que van desde los ciberdelincuentes hasta los actores de los Estados-nación, han demostrado ser más persistentes, sigilosos y sutiles en sus ataques. Han logrado penetrar las defensas del perímetro de la red con regularidad, poniendo en peligro e infligiendo daño a la seguridad nacional y económica. Incluso los profesionales de ciberseguridad más capacitados enfrentan desafíos al defender redes empresariales dispersas de amenazas cibernéticas cada vez más sofisticadas.

Zero Trust cuestiona la premisa de confiar implícitamente en usuarios, dispositivos y componentes de la red en función de su ubicación dentro de la red. Incorpora un monitoreo de seguridad integral, controles de acceso granulares, dinámicos y basados en riesgos, así como automatización de la seguridad del sistema coordinada en todos los aspectos de la infraestructura. Este modelo de seguridad centrado en datos permite la aplicación del concepto de acceso con privilegios mínimos para cada decisión de acceso, donde las respuestas a las preguntas de quién, qué, cuándo, dónde y cómo son fundamentales para permitir o denegar adecuadamente el acceso a los recursos.

Para implementar adecuadamente el entorno de amenazas dinámico moderno, es necesario adoptar los siguientes principios dentro del marco de Zero Trust:

Desconfianza en todo: Se debe asumir que todas las solicitudes de recursos críticos y todo el tráfico de red pueden ser maliciosos. Además, es fundamental considerar que todos los dispositivos y la infraestructura pueden verse comprometidos en cualquier momento.

Gestión de Riesgos Continua: Se debe aceptar que todas las aprobaciones de acceso a recursos críticos conllevan riesgos y estar preparados para realizar operaciones rápidas de evaluación, control y recuperación de daños en caso de incidentes.

Así mismo se puede diseñar una solución de Zero Trust, es posible aprovechar algunos conceptos de seguridad clave:

Definir los resultados de la misión: Derivar la arquitectura Zero Trust a partir de los requisitos específicos de la misión de

la organización, identificando los datos, activos, aplicaciones y servicios críticos.

Arquitectura desde el interior hacia el exterior: Centrarse inicialmente en proteger los datos, activos, aplicaciones y servicios críticos, y luego asegurar todas las rutas para acceder a ellos.

Determinar quién/qué necesita acceso: Crear políticas de control de acceso basadas en la identificación de quién o qué necesita acceso a los recursos críticos, y aplicar estas políticas de manera consistente en todos los entornos.

Inspeccionar y registrar todo el tráfico: Establecer una visibilidad completa de toda la actividad en todas las capas desde los puntos finales y la red para permitir análisis que puedan detectar actividades sospechosas.

El propósito fundamental de Zero Trust es comprender y controlar cómo interactúan los usuarios, los procesos y los dispositivos con los datos. La combinación del usuario, el dispositivo y cualquier otra información contextual relevante para la seguridad (como ubicación, hora del día, comportamiento registrado previamente del usuario o dispositivo) que se utiliza para tomar una decisión de acceso se denomina tupla. Como parte de esta tupla, se requiere autenticación explícita tanto del usuario como del dispositivo para tener información confiable en la tupla. El motor de decisión Zero Trust examina la tupla en la solicitud de acceso y la compara con la política de seguridad de los datos o recursos solicitados. Luego, toma una decisión basada en el riesgo sobre si permitir el acceso y envía una entrada de registro de esa solicitud de acceso y la decisión para ser parte de futuros análisis de actividades sospechosas. Este proceso se lleva a cabo para cada solicitud de acceso individual a cada recurso confidencial y se puede repetir periódicamente durante el acceso extendido a un recurso.

VII. Conclusiones

Se destacan tres conclusiones principales relacionadas con la efectividad y utilidad de estas metodologías en la mejora de la seguridad cibernética y la protección contra ciberataques. Además, se enfatiza la importancia de mantenerse al día con las últimas amenazas y tendencias en ciberseguridad, así como de promover la conciencia y la capacitación en ciberseguridad entre los usuarios y el personal de la organización.

La implementación del framework del NIST en las infraestructuras de los centros de datos ha demostrado ser una estrategia efectiva para mejorar la seguridad y eficiencia en la protección contra ciberataques. Al seguir las pautas y controles recomendados por el NIST, las organizaciones pueden fortalecer sus defensas cibernéticas y garantizar la disponibilidad de los servicios críticos.

El enfoque de Zero Trust ofrece una metodología sólida para controlar y gestionar el acceso a los recursos confidenciales en un entorno de amenazas dinámico. Al adoptar los principios de Zero Trust, las organizaciones pueden reducir el riesgo de compromisos de seguridad al validar constantemente la identidad y el estado de los usuarios, dispositivos y procesos que intentan acceder a datos sensibles.

La ciberseguridad y el uso de ciberarmas continúan evolucionando rápidamente, presentando desafíos cada vez más complejos para las organizaciones y los gobiernos. Es fundamental que las estrategias de defensa cibernética se mantengan al día con las últimas amenazas y tendencias, y que se implementen medidas proactivas para proteger los activos digitales contra ataques cada vez más sofisticados y persistentes.

Adicionalmente la conciencia y la capacitación en ciberseguridad son cruciales para fortalecer la postura de seguridad de una organización. Los usuarios deben estar informados sobre las mejores prácticas de seguridad, cómo reconocer y reportar actividades sospechosas, y cómo colaborar en la protección de los activos digitales contra amenazas cibernéticas y ciberarmas.

La ciberseguridad en Argentina es un desafío complejo que involucra a múltiples organismos y agencias gubernamentales. Los ataques dirigidos a entidades estatales han puesto de manifiesto la necesidad de estrategias integradas y medidas robustas para proteger las infraestructuras críticas y la información sensible. A continuación, se presentan algunas conclusiones sobre la situación actual y las medidas necesarias para enfrentar estas amenazas:

Importancia de la Coordinación y Colaboración Multilateral

La necesidad de una coordinación efectiva entre diversos organismos nacionales e internacionales en el ámbito de la ciberseguridad es crucial para enfrentar amenazas cada vez más sofisticadas. Los ataques a organismos estatales suelen ser complejos y requieren una respuesta integrada que combine recursos y conocimientos de múltiples entidades, tanto dentro de Argentina como en colaboración con organismos globales como la Organización de los Estados Americanos (OEA) y el Foro Global de Expertos en Ciberseguridad (GFCE). Esta colaboración es esencial para compartir información sobre amenazas, estrategias de mitigación y mejores prácticas.

Vulnerabilidad de las Infraestructuras Críticas

Las infraestructuras críticas de un país, que incluyen sistemas de telecomunicaciones, servicios públicos y entidades gubernamentales, son objetivos prioritarios para los ciber atacantes. La regulación y supervisión adecuadas de estas infraestructuras, lideradas por entidades como *el Ente Nacional de Comunicaciones* (ENACOM) y la *Dirección Nacional de Ciberseguridad*, son vitales para prevenir interrupciones significativas y proteger la información sensible. La implementación de medidas de seguridad robustas y actualizaciones constantes son necesarias para reducir la vulnerabilidad ante ataques cibernéticos.

Evolución y Sofisticación de los Ataques Cibernéticos

Los ataques cibernéticos dirigidos a organismos estatales están evolucionando en términos de sofisticación y alcance. Los atacantes utilizan técnicas avanzadas como el envenenamiento de caché DNS, el malware y la ingeniería social para

comprometer sistemas gubernamentales. Organismos como la *Unidad Fiscal Especializada en Ciberdelincuencia* (UFECI) y *CERT.ar* desempeñan un papel fundamental en la detección, investigación y mitigación de estos ataques. La formación continua y la actualización de las estrategias de defensa son esenciales para adaptarse a este entorno dinámico y asegurar la resiliencia de los sistemas estatales frente a ciberamenazas en constante cambio.

Necesidad de Fortalecer la Capacitación y Concienciación

La capacitación y concienciación en ciberseguridad son esenciales para todos los niveles de la administración pública. Los empleados gubernamentales deben estar bien informados sobre las amenazas cibernéticas y las mejores prácticas para prevenir ataques. Programas de formación continuos y campañas de concienciación liderados por la Dirección Nacional de Ciberseguridad pueden aumentar significativamente la capacidad de defensa contra ciberataques.

Desafíos en la Implementación de Políticas de Ciberseguridad

La implementación efectiva de políticas de ciberseguridad enfrenta varios desafíos, incluyendo limitaciones presupuestarias, resistencia al cambio y la rápida evolución de las amenazas. Las políticas deben ser dinámicas y adaptables, requiriendo una colaboración estrecha entre entidades reguladoras, operativas y de investigación. La Agencia de Acceso a la Información Pública (AAIP) y otras entidades deben trabajar en conjunto para superar estos desafíos y asegurar un marco de ciberseguridad robusto y eficaz.

VIII. Futuras Líneas de Investigación

El estudio continuado de los microservicios y sus herramientas de implementación, como Docker y Kubernetes, ofrece oportunidades para explorar nuevos enfoques en la gestión de aplicaciones distribuidas, escalabilidad y eficiencia operativa. Investigaciones adicionales podrían centrarse en optimizar la orquestación y gestión de contenedores, mejorar la seguridad y robustez de las arquitecturas de microservicios, así como en la integración de tecnologías emergentes para maximizar su rendimiento y utilidad práctica.

Paralelamente, el desarrollo de software seguro sigue siendo un área crítica de interés, especialmente en un entorno de creciente amenaza cibernética. Investigaciones futuras podrían explorar nuevas metodologías, herramientas y mejores prácticas para integrar la seguridad en todas las etapas del ciclo de vida del desarrollo de software. Esto incluye la identificación y mitigación proactiva de vulnerabilidades, la aplicación de técnicas de análisis estático y dinámico de código, así como la promoción de una cultura de seguridad en el desarrollo de software.

IX. Agradecimientos

Se desea expresar un profundo agradecimiento por todo el apoyo brindado a Mary, mi novia, y a mi familia, quienes lo respaldaron incluso cuando no pude asistir a celebraciones familiares debido a parciales o finales. También se agradece a mis amigos de toda la vida, desde los tres años, quienes siempre estuvieron presentes, aunque en varias ocasiones no pude reunirse con ellos debido a compromisos académicos.

Se extiende un especial agradecimiento al Ingeniero Jesús Alejandro Lugo, un gran profesional de quien se aprendió mucho en sus materias, las cuales se abordaron en profundidad y con explicaciones muy claras.

Finalmente, se agradece al Magister Pablo Alejandro Lena por su capacidad de ayuda y guía en la elaboración de la tesis, así como por los valiosos consejos brindados que facilitaron la culminación de este trabajo.

X. Referencias

Publicaciones periódicas:

[1] https://es.wikipedia.org/wiki/Equation_Group
[2] https://es.wikipedia.org/wiki/Stuxnet
[3] https://es.wikipedia.org/wiki/Flame_(malware)
[4] https://www.argentina.gob.ar/jefatura/innovacion-ciencia-y-tecnologia/onti
[5] https://www.forbesargentina.com/innovacion/como-opera-grupo-ciberdelincuencia-rhysida-logro-afectar-sistemas-pami-n38592
[6] https://es.malwarebytes.com/ransomware/
[7] https://www.avast.com/es-es/c-phishing
[8] https://www.akamai.com/es/glossary/what-is-ddos#:~:text=En%20un%20ataque%20distribuido%20de,de%20red%20con%20tr%C3%A1fico%20malicioso
[9] https://www.telefonica.com/es/sala-comunicacion/blog/que-es-ingenieria-social/
[10] https://owasp.org/Top10/
[11] https://www.fortinet.com/lat/resources/cyberglossary/brute-force-attack
[12] https://www.nist.gov/cyberframework
[13] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad
[14] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar
[15] https://www.argentina.gob.ar/seguridad
[16] https://www.mpf.gob.ar/ufeci/
[17] https://www.dpn.gob.ar/
[18] https://www.argentina.gob.ar/aaip
[19] https://www.enacom.gob.ar/

XI. Anexos

Anexo I: Investigación de Stuxnet, Desarrollo de Malware que Afectaron a Organismos, su Arquitectura y Propagación, y Análisis de Grupos APT que Utilizan Malware para Atacar Organismos.

Anexo II: Desarrollo en profundidad sobre el framework del NIST.

XII. Biografías



Juan Ignacio Munté nació en Banfield partido de Lomas de Zamora, el 9 de septiembre de 1983. Es Técnico superior en análisis de sistemas en el IFTS 5. Próximo a graduarse en la universidad de Palermo de Licenciado en tecnología de la información.

Su experiencia laboral cuenta con más de 20 años en la rama de pentester y ciberseguridad. Actualmente está como

especialista en ciberseguridad y security research. Actualmente se encuentra trabajando para la AFIP hace dos años como especialista en ciberseguridad y arquitecto, anteriormente trabajo 12 años en el Banco icbc como especialista en ciberseguridad.

Actualmente cuenta con certificaciones Internacionales de Microsoft, Cisco, VMware, CEH.