Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRIA

Formación y concienciación sobre la ciberseguridad para los empleados del Estado Argentino

AUTOR: Lic. Lukas Pedrotta

DIRECTOR: Mag. Rufino Martin

2024/25

Resumen

La creciente dependencia de las tecnologías de la información y la comunicación han cambiado radicalmente la manera en que funcionan tanto el sector público como el sector privado. Sin embargo, a medida que el uso de las tecnologías crece, también aumentan los riesgos de ciberamenazas, que cada vez se vuelven más complejas y difíciles de detectar. En este contexto, la ciberseguridad se ha convertido en una prioridad global, especialmente para los gobiernos que manejan información sensible, datos personales y sistemas críticos.

En Argentina, uno de los mayores desafíos es mejorar la formación y concienciación en ciberseguridad entre los empleados públicos. La falta de conocimientos adecuados en esta área aumenta el riesgo de vulnerabilidades en las infraestructuras digitales del Estado, lo que podría afectar la seguridad y la continuidad de los servicios públicos.

El objetivo principal de esta tesis es analizar el estado actual de la formación y concienciación en ciberseguridad entre los empleados del Estado Argentino, identificando brechas y áreas de oportunidad. A partir de este análisis, se propondrá una hoja de ruta con planes de formación y estrategias adaptadas a las necesidades específicas del sector público argentino, tomando en cuenta buenas prácticas internacionales. La propuesta busca fortalecer la capacidad de los empleados públicos para prevenir, detectar y responder a incidentes de ciberseguridad, protegiendo así la información crítica y asegurando la continuidad operativa.

La investigación propone planes de formación y políticas públicas de concienciación que fomenten una cultura de ciberseguridad en la administración pública, inspirándose en modelos exitosos implementados en países como Estonia y España. Además, se incluirán métricas de evaluación periódica para medir la efectividad de las políticas y programas implementados.

Este trabajo busca construir un marco integral de ciberseguridad en el sector público argentino, que no solo contemple soluciones tecnológicas, sino también un cambio cultural hacia una mayor conciencia y responsabilidad en la protección de la información. La correcta implementación de estas estrategias será clave para mitigar los riesgos de ciberataques y proteger los activos digitales del Estado, asegurando así una respuesta eficiente ante incidentes que puedan comprometer la seguridad nacional.

Abstract

The growing reliance on information and communication technologies (ICT) has profoundly changed how public and private sectors operate. However, as these technologies become more widely used, the risk of cyber threats also increases, posing more complex challenges to security. In this context, cybersecurity has emerged as a global priority, particularly for governments that manage sensitive information, personal data, and critical systems.

In Argentina, one of the main challenges is to improve cybersecurity training and awareness among public sector employees. The absence of adequate knowledge in this area increases the risk of vulnerabilities within the digital infrastructure of the state, potentially compromising the security and continuity of public services.

This thesis aims to assess the current state of cybersecurity training and awareness among public sector employees in Argentina, identifying gaps and areas for improvement. Based on this assessment, a roadmap will be proposed with tailored training plans and strategies, drawing from international best practices while considering the specific needs of Argentina’s public sector. The goal is to strengthen public employees ability to prevent, detect, and respond to cybersecurity incidents, ensuring the protection of critical information and operational continuity.

The research proposes training plans and public awareness policies designed to build a cybersecurity culture within public administration, inspired by successful models from countries like Estonia and Spain. Additionally, it includes periodic evaluation metrics to measure the effectiveness of the implemented programs and policies.

This study seeks to build a comprehensive cybersecurity framework in Argentina’s public sector, addressing not only technological solutions but also promoting a cultural shift towards greater awareness and responsibility in protecting sensitive information. The effective implementation of these strategies will be essential to mitigate cyber risks and safeguard the state's digital assets, ensuring a swift and effective response to incidents that could threaten national security.

Agradecimientos

En primer lugar, quiero agradecer a mi familia, cuyo apoyo ha sido fundamental para superar los desafíos y alcanzar este objetivo. Su confianza en mí me ha brindado la fuerza necesaria para continuar incluso en los momentos más difíciles.

A mi director de tesis, Rufino Martín, por su orientación, paciencia y sabiduría a lo largo de todo el proceso. Su dedicación y sus valiosos consejos me han permitido estructurar de manera adecuada mis ideas y llegar a una propuesta de investigación sólida. Agradezco su compromiso y su confianza en mi trabajo.

Finalmente, a todas las personas que han sido parte de este recorrido académico y personal. Cada uno de ustedes ha dejado una huella importante en este proyecto.

Lista de Abreviaturas y Acrónimos

A continuación, se presentan las abreviaturas y acrónimos utilizados en esta tesis:

CCDCOE: Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN

CIC: Centro de Información de Ciberseguridad

ICT: Information and Communication Technology (Tecnologías de la Información y la Comunicación)

ISO: International Organization for Standardization (Organización Internacional de Normalización)

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)

CSIRT: Computer Security Incident Response Team (Equipo de Respuesta ante Incidentes de Seguridad Informática)

IoT: Internet of Things (Internet de las Cosas)

RENAPER: Registro Nacional de las Personas

TIC: Tecnologías de la Información y la Comunicación

BCRA: Banco Central de la República Argentina

CVE: Common Vulnerabilities and Exposures (Vulnerabilidades y Exposiciones Comunes)

UIT: Unión Internacional de Telecomunicaciones

VPN: Virtual Private Network (Red Privada Virtual)

Índice

Listado de Figuras

Introducción

Marco de referencia (Contexto y Justificación)

En la era digital, las tecnologías de la información y la comunicación se han convertido en una parte fundamental para las actividades gubernamentales, sociales y económicas a nivel mundial. A medida que el uso de Internet y las tecnologías continúa creciendo, también lo hace la exposición a las ciberamenazas que cada vez son más complejas y difíciles de detectar (ENISA, 2023). En este contexto, la ciberseguridad se ha consolidado como una disciplina clave para proteger las infraestructuras digitales, garantizar la continuidad de los servicios esenciales y seguridad de la información sensible que gestionan los gobiernos.

A nivel global, las amenazas cibernéticas han aumentado considerablemente en los últimos años, abarcando desde robo de información confidencial hasta ataques a infraestructuras críticas. La Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023) señala que "los ataques cibernéticos son cada vez más sofisticados, dirigidos y persistentes, afectando a sectores críticos como la energía, la salud y el transporte"(pág. 5). Estos ciberataques tienen el potencial de interrumpir el funcionamiento de sectores estratégicos, afectando la estabilidad social y económica de las naciones (World Economic Forum, 2023). Sin embargo, la concienciación y formación en ciberseguridad no ha avanzado al mismo ritmo que la evolución tecnológica, dejando a muchas instituciones vulnerables a incidentes de seguridad, especialmente en el sector público (OECD, 2022).

En Argentina, la situación refleja este desafío global. Si bien se han realizado esfuerzos significativos en el desarrollo de infraestructura digital y tecnologías de la información, la falta de formación y concienciación en ciberseguridad dentro de la administración pública aumenta la vulnerabilidad del Estado frente a ciber incidentes. La falta de preparación del factor humano pone en riesgo no solo la confidencialidad y la integridad de la información sensible, sino también la continuidad operativa de los servicios públicos (CERT Argentina, 2022).

La ciberseguridad no es solo un desafío tecnológico, sino también humano. La concienciación y formación en ciberseguridad entre los empleados del Estado es esencial para prevenir ataques, mitigar riesgos y responder eficazmente ante incidentes que puedan comprometer la seguridad del país. En este sentido, las personas son tanto el

eslabón más débil como la primera línea de defensa en el ecosistema de ciberseguridad (SANS Institute, 2022).

Aunque las ciberamenazas han ganado en complejidad, en Argentina persiste la ausencia de un programa integral de formación y concienciación en ciberseguridad, adaptado a las necesidades específicas del sector público. Esta brecha exige la adopción de medidas que refuercen la cultura de ciberseguridad, mitigando las vulnerabilidades resultantes de errores humanos y deficiencias en el conocimiento.[1]

En respuesta a esta necesidad, esta tesis propone una estrategia integral para mejorar la formación y concienciación en ciberseguridad en el sector público argentino. Se busca no solo fortalecer las capacidades de los empleados públicos para prevenir, detectar y responder a ciberamenazas, sino también promover una cultura de ciberseguridad que contribuya a la resiliencia digital del Estado Argentino. Esta investigación se fundamenta en buenas prácticas internacionales, adaptándolas al contexto y necesidades específicas del sector público en Argentina, y y propone políticas públicas de concienciación y planes de formación, basados en los resultados de una encuesta a 157 empleados públicos donde el 59% carece de formación (Cap. 3.2, Fig. 6), que buscan garantizar una protección efectiva de los activos digitales del Estado mediante el fortalecimiento de las capacidades del sector público para prevenir y responder a ciberincidentes.

[1] Según el SANS Institute (2022), a nivel global se estima que hasta el 95% de las brechas de seguridad están vinculadas a errores humanos o a la falta de conocimiento. No obstante, este dato no corresponde específicamente al contexto argentino, donde aún no se cuenta con estudios que cuantifiquen este fenómeno.

Planteamiento del problema

A medida que el mundo avanza hacia una digitalización generalizada, las instituciones públicas, especialmente en Argentina, enfrentan el reto creciente de proteger sus activos digitales y sus infraestructuras críticas frente a ciberataques cada vez más sofisticados. El fenómeno de la datificación, en el cual gran parte de las actividades del Estado se transforman en datos gestionados digitalmente, ha generado una dependencia significativa de los sistemas tecnológicos (Mayer-Schönberger & Cukier, 2013). Sin embargo, esta dependencia también ha expuesto al Estado argentino a ciberamenazas que buscan comprometer la información pública y alterar el funcionamiento de los servicios esenciales.

Los recientes ciberataques dirigidos a instituciones como el Registro Nacional de las Personas, el Sistema Judicial chaqueño y la Legislatura porteña han puesto de manifiesto fallas críticas en la seguridad digital del sector público argentino[2]. Estos incidentes resaltan la necesidad urgente de evaluar y fortalecer la formación y la concienciación en ciberseguridad dentro de las entidades gubernamentales. Aunque existen iniciativas aisladas, como las actividades del CERT Argentina y programas académicos en instituciones como la Universidad de Buenos Aires, una revisión preliminar (Cap. 3.2) indica que la preparación de los empleados públicos en mejores prácticas de seguridad informática sigue siendo limitada, como lo evidencia el 59% de los encuestados que no han recibido formación (Fig. 6). Esta deficiencia ha contribuido a la vulnerabilidad del Estado frente a amenazas, según reportes del CERT Argentina (2022).

La ciberseguridad, un campo multidimensional que va más allá de las soluciones tecnológicas, depende en gran medida del comportamiento humano; los empleados del sector público, frecuentemente objetivo de ataques de ingeniería social como phishing y spear phishing (SANS Institute, 2022), representan un eslabón vulnerable. El problema central de esta tesis radica en que, a pesar de algunos avances, la formación y concienciación en ciberseguridad en el sector público argentino es insuficiente para enfrentar de manera integral las amenazas cibernéticas contemporáneas.

[2] Estos incidentes, documentados en reportes del CERT Argentina (2022) y medios nacionales, incluyen brechas que afectaron la confidencialidad de datos sensibles, subrayando la necesidad de una respuesta coordinada.

En este contexto, la Unión Internacional de Telecomunicaciones (UIT) evalúa periódicamente el nivel de preparación de los países en términos de ciberseguridad a través del Índice Global de Ciberseguridad (Global Cybersecurity Index, GCI). Este índice mide el grado de compromiso de cada nación en la implementación de medidas de protección digital y se calcula en base a cinco dimensiones clave: medidas legales, técnicas, organizacionales, de desarrollo de capacidades y cooperación internacional (UIT, 2021).

Según el informe más reciente de la UIT (2021), Argentina se encuentra en la posición 91 a nivel global y en el puesto 13 dentro de la región de América, como se ilustra en las figuras 1 y 2. Aunque ha avanzado tres posiciones en el ranking global en comparación con la evaluación de 2018, ha experimentado un retroceso de dos puestos en el contexto regional. Esto refleja la necesidad urgente de fortalecer las capacidades de ciberseguridad en el sector público argentino, especialmente en desarrollo de capacidades y concienciación en ciberseguridad.

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15
Netherlands**	97.05	16
Norway**	96.89	17
Mauritius	96.89	17
Brazil	96.6	18
Belgium	96.25	19
Italy	96.13	20
Oman	96.04	21
Finland	95.78	22
Egypt	95.48	23
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43
Thailand	86.5	44
Tunisia	86.23	45
Ireland	85.86	46
Nigeria	84.76	47
New Zealand**	84.04	48
Malta	83.65	49
Morocco	82.41	50
Kenya	81.7	51
Mexico	81.68	52
Bangladesh	81.27	53

(continued)

Country Name	Score	Rank
Iran (Islamic Republic of)	81.07	54
Georgia	81.06	55
Benin	80.06	56
Rwanda	79.95	57
Iceland	79.81	58
South Africa**	78.46	59
Bahrain	77.86	60
Philippines	77	61
Romania	76.29	62
Moldova	75.78	63
Uruguay	75.15	64
Kuwait	75.07	65
Dominican Rep.	75.05	66
Slovenia	74.93	67
Czech Republic	74.37	68
Monaco	72.57	69
Uzbekistan	71.11	70
Jordan	70.96	71
Uganda	69.98	72
Zambia	68.88	73
Chile	68.83	74
Côte d'Ivoire	67.82	75
Costa Rica	67.45	76
Bulgaria	67.38	77
Ukraine	65.93	78
Pakistan	64.88	79
Albania	64.32	80
Colombia	63.72	81
Cuba	58.76	82
Sri Lanka	58.65	83
Paraguay	57.09	84
Brunei Darussalam	56.07	85
Peru	55.67	86
Montenegro	53.23	87
Botswana	53.06	88
Belarus	50.57	89
Armenia**	50.47	90
Argentina	50.12	91
Kyrgyzstan	49.64	92
Cameroon	45.63	93
Nepal (Republic of)	44.99	94
Chad	40.44	95
Burkina Faso**	39.98	96
Malawi	36.83	97
Zimbabwe	36.49	98
Myanmar	36.41	99
Senegal	35.85	100
Liechtenstein**	35.15	101
Sudan	35.03	102
Panama	34.11	103
Algeria	33.95	104
Togo	33.19	105
Jamaica**	32.53	106
Gambia	32.12	107
Suriname	31.2	108
Lebanon**	30.44	109
Bosnia and Herzegovina	29.44	110
Samoa	29.33	111
Fiji	29.08	112
Libya	28.78	113
Guyana	28.11	114
Ethiopia	27.74	115
Venezuela	27.06	116
Andorra**	26.38	117
Papua New Guinea**	26.33	118
Ecuador	26.3	119
Mongolia	26.2	120
Sierra Leone	25.31	121
State of Palestine	25.18	122
Mozambique	24.18	123
Madagascar**	23.33	124
Trinidad and Tobago	22.18	125
Syrian Arab Republic**	22.14	126
Nauru**	21.42	127
Tonga**	20.95	128
Iraq**	20.71	129
Guinea**	20.53	130

Figura 1: Ranking Índice Global de Ciberseguridad

Fuente: Índice Global de Ciberseguridad 2020 – IT

Table 5: GCI results: Americas region

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10
Paraguay	57.09	11
Peru	55.67	12
Argentina	50.12	13
Panama	34.11	14
Jamaica**	32.53	15
Suriname	31.2	16
Guyana	28.11	17
Venezuela	27.06	18
Ecuador	26.3	19

Figura 2: Ranking Índice Global de Ciberseguridad (Región América)

Fuente: Índice Global de Ciberseguridad 2020 – IT

Justificación de la investigación

En la época digital actual, las instituciones públicas argentinas se enfrentan a desafíos significativos en materia de ciberseguridad. Durante el año 2023, Argentina registró más de 2.000 millones de intentos de ciberataques, lo que evidencia la magnitud de las amenazas digitales que enfrenta el país (Forbes Argentina, 2023)[3]. Esta situación subraya la necesidad de proteger la información crítica del Estado y garantizar la continuidad de sus operaciones.

El sector público argentino, responsable de manejar datos sensibles y proporcionar servicios esenciales a la ciudadanía, se ha convertido en un objetivo principal para los ciber atacantes. Informes recientes indican que el phishing representó el 75% de los incidentes reportados en 2023, afectando gravemente a sectores como Finanzas y Gobierno (CERT Argentina, 2023). Estos datos resaltan la importancia de implementar estrategias efectivas de concienciación y formación en ciberseguridad para el personal gubernamental, con el fin de mitigar riesgos asociados a errores humanos y falta de conocimiento.

Además de fortalecer la protección de los sistemas y datos estatales, la capacitación en ciberseguridad es esencial para mantener la confianza de la ciudadanía en las instituciones públicas. La integridad, confidencialidad y disponibilidad de la información son pilares fundamentales para una gobernanza efectiva. En este contexto, el diseño e implementación de políticas de formación adaptadas a las particularidades del sector público argentino, basadas en buenas prácticas internacionales, contribuirán significativamente a reducir los riesgos de ciberataques y a promover una cultura de seguridad sólida.

La relevancia de esta investigación surge en un escenario donde Argentina ha sido objeto de ciberataques de gran magnitud, evidenciando la vulnerabilidad de sus infraestructuras digitales (Brodersen, 2023). A pesar de estos desafíos, el país aún carece de una estrategia integral en ciberseguridad que contemple programas continuos de formación y concienciación para los empleados públicos. Por lo tanto, es imperativo desarrollar políticas públicas efectivas que fortalezcan las capacidades humanas en ciberseguridad, asegurando la protección de los activos digitales del gobierno y garantizando la ciber resiliencia de las instituciones nacionales.

[3] Según datos de FortiGuard Labs, Argentina registró más de 2.000 millones de intentos de ciberataques en 2023, lo que destaca la magnitud de las amenazas digitales en el país (Forbes Argentina, 2023).

Objetivos de la investigación

Objetivo general:

Diseñar un plan integral de formación en ciberseguridad para las instituciones públicas argentinas, orientado a detectar brechas formativas y mejorar el nivel de concienciación y competencias en ciberseguridad de los empleados estatales, con el fin de reducir el riesgo de ciberataques y fortalecer la protección de los activos digitales gubernamentales.

Objetivos específicos:

Identificar las brechas formativas en ciberseguridad existentes en las instituciones públicas argentinas, evaluando el nivel actual de conocimientos, habilidades y concienciación de los empleados estatales frente a amenazas cibernéticas.

Desarrollar un marco de evaluación y métricas de desempeño que permitan medir de manera efectiva el nivel de formación y concienciación en ciberseguridad de los empleados públicos, facilitando el seguimiento continuo y la optimización del plan formativo.

Diseñar un plan de formación integral, adaptado a las necesidades específicas del sector público argentino, que incluya módulos de capacitación en concienciación, conocimientos técnicos básicos y avanzados, y protocolos de respuesta a incidentes de ciberseguridad.

Establecer lineamientos de políticas públicas que garanticen la implementación sostenible del plan de formación en ciberseguridad, promoviendo una cultura de seguridad digital en todos los niveles del sector público y fortaleciendo la ciber resiliencia de las instituciones gubernamentales.

Metodología

Esta investigación adopta un enfoque mixto, combinando métodos cuantitativos y cualitativos para proporcionar una comprensión integral del nivel de formación en ciberseguridad en el sector público argentino. El enfoque cuantitativo se aplicó mediante una encuesta elaborada y administrada por el autor, dirigida a 157 empleados públicos de distintas dependencias estatales. Por su parte, el enfoque cualitativo permite interpretar las percepciones y experiencias de expertos en ciberseguridad respecto a las políticas formativas vigentes y las necesidades de mejora.

Hipótesis

Hipótesis principal:

La falta de concienciación en ciberseguridad entre los empleados del Estado Argentino representa un riesgo significativo para la ciberseguridad y la ciberdefensa de la República Argentina.

Capítulo 1: Marco Teórico

1.1. Conceptos de ciberseguridad

La ciberseguridad se define como el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes y datos contra accesos no autorizados, robos, daños o interrupciones. Su propósito fundamental es garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas tecnológicos. Estos tres principios, conocidos como la tríada CIA (Confidentiality, Integrity, Availability), constituyen el pilar fundamental de la seguridad de la información (ISACA, 2017).

En su definición más básica, la ciberseguridad se enfoca en prevenir amenazas que puedan interrumpir o comprometer los servicios que dependen de sistemas tecnológicos críticos. Además de proteger los datos contra accesos no autorizados, la ciberseguridad también abarca prácticas de gestión de riesgos y capacitación continua para mitigar el factor humano como vulnerabilidad clave (Pfleeger & Margulies, 2023).

El modelo de seguridad de la información se fundamenta en los principios esenciales de confidencialidad, integridad y disponibilidad, conocidos colectivamente como la tríada CIA. La confidencialidad se refiere a la protección de la información contra accesos o divulgaciones no autorizadas, garantizando que solo individuos o sistemas con permisos adecuados puedan acceder a los datos. Según Whitman y Mattord (2022), "la confidencialidad es la piedra angular de la seguridad de la información, asegurando que los datos sensibles permanezcan protegidos de miradas no autorizadas" (pág. 47). En el ámbito de la ciberseguridad, una violación de confidencialidad puede tener consecuencias significativas, como la pérdida de confianza, la divulgación de información protegida por leyes de privacidad y posibles acciones legales contra la organización afectada (Sanchez, 2015).

Por otro lado, la integridad garantiza que la información sea exacta, completa y consistente, y que no haya sido alterada de manera indebida, ya sea de forma intencional o accidental. Este principio protege los datos contra modificaciones no autorizadas que podrían comprometer su precisión y confiabilidad. Anderson (2021) afirma que "la integridad de los datos es esencial en sistemas críticos, donde cualquier alteración puede comprometer decisiones estratégicas o la operatividad de infraestructuras clave" (pág.

112). La pérdida de integridad puede ser el primer paso para un ataque más grave, afectando la confidencialidad o la disponibilidad de la información (ISACA, 2017).

Por último, la disponibilidad garantiza que los datos y los sistemas estén accesibles y operativos cuando sean requeridos por usuarios autorizados. Esto implica la implementación de medidas preventivas contra fallos técnicos, ataques de denegación de servicio (DDoS) y otros incidentes que podrían interrumpir la operatividad de los sistemas. Schneier (2022) destaca que "la disponibilidad es un aspecto clave de la ciberseguridad moderna, pues sin acceso a los datos en el momento adecuado, la funcionalidad del sistema se ve gravemente afectada" (pág. 89). Una violación de disponibilidad puede resultar en pérdidas operativas, afectando la productividad y la continuidad de los servicios esenciales.

El desarrollo de la ciberseguridad ha sido un proceso dinámico y no lineal, evolucionando junto con los avances tecnológicos y el creciente número de amenazas cibernéticas. Inicialmente, los ataques cibernéticos consistían en virus informáticos simples que causaban daños limitados a los sistemas. Sin embargo, en la actualidad, las amenazas han aumentado en sofisticación y complejidad, abarcando desde phishing hasta ataques complejos como ransomware y denegación de servicio distribuido (DDoS).

Estos tipos de amenazas no solo afectan a individuos, sino que también tienen implicancias significativas en organizaciones y gobiernos, comprometiendo infraestructuras críticas y datos sensibles. Esta creciente sofisticación ha convertido la ciberseguridad en un campo interdisciplinario que requiere conocimientos tanto de informática como de gestión de riesgos y psicología humana (ISACA, 2017).

En este contexto, la gestión de riesgos en ciberseguridad desempeña un papel crucial al involucrar no solo la identificación de amenazas, sino también la evaluación de vulnerabilidades y la implementación de políticas de protección adecuadas. Estas políticas incluyen desde firewalls y antivirus hasta sistemas avanzados de monitorización y detección de intrusos. Además, se ha reconocido la necesidad de adoptar una respuesta proactiva ante incidentes, debido a que los ataques cibernéticos son dinámicos y evolucionan constantemente.

En este sentido, la protección de los sistemas no puede limitarse únicamente a soluciones tecnológicas. Es igualmente fundamental la educación y formación continua

de los usuarios, ya que el factor humano sigue siendo la principal vulnerabilidad en ciberseguridad. Según Jouini, Rabai y Azaiez (2014), "la educación y formación continua de los usuarios es fundamental para reducir los errores humanos y fortalecer la seguridad en las organizaciones" (pág. 63).

Los principios de confidencialidad, integridad y disponibilidad operan de manera conjunta para proporcionar un marco robusto de seguridad de la información, asegurando que los datos sean accesibles solo para quienes tienen permiso, permanezcan inalterados y estén disponibles cuando sean necesarios.

1.2. Historia y evolución de la ciberseguridad

La historia y evolución de la ciberseguridad está íntimamente relacionada con el desarrollo de la informática y la expansión del Internet. En sus inicios, cuando los sistemas informáticos eran aislados y no existían redes interconectadas, las amenazas de seguridad eran prácticamente inexistentes. Sin embargo, a medida que las redes comenzaron a expandirse y el acceso a Internet se generalizó, emergió la necesidad de proteger los sistemas y la información ante posibles ataques cibernéticos.

En las décadas de 1980 y 1990, la ciberseguridad empezó a consolidarse como un campo necesario debido al crecimiento de las amenazas informáticas. Uno de los primeros incidentes significativos fue el Morris Worm en 1988, un gusano informático que infectó aproximadamente al 10% de las computadoras conectadas a Internet en ese momento. Este ataque reveló la vulnerabilidad de los sistemas interconectados y motivó el desarrollo de políticas de seguridad informática más robustas (Spafford, 1989). La respuesta a incidentes como este llevó al establecimiento de CERTs (Computer Emergency Response Teams), encargados de gestionar emergencias de seguridad informática, marcando el inicio de una ciberseguridad más estructurada y coordinada.

La evolución de las amenazas continuó con la proliferación de virus informáticos y la expansión de Internet en la década de 1990. Los ataques comenzaron a diversificarse, abarcando desde virus y troyanos hasta técnicas más complejas de phishing y ataques de denegación de servicio (DDoS). Esta diversificación exigió el desarrollo de herramientas más sofisticadas de protección, tales como firewalls, antivirus y sistemas de detección de intrusos. La introducción de las redes sociales y el aumento del comercio electrónico también ampliaron la superficie de ataque, exponiendo a individuos y organizaciones a nuevos riesgos de seguridad. Durante este periodo, la industria comenzó a adoptar estándares de seguridad informática, como la ISO/IEC 27001, que establece un marco para la gestión de la seguridad de la información (Whitman & Mattord, 2022).

Con el auge de Internet en la década de 2000, la ciberseguridad experimentó un cambio significativo. Los ataques informáticos comenzaron a ser organizados y a dirigirse a infraestructuras críticas, como sistemas energéticos, financieros y gubernamentales. La motivación de los atacantes también se diversificó, incluyendo desde la ciberdelincuencia motivada por el lucro hasta el ciber espionaje y la ciber guerra patrocinada por estados. Este periodo marcó el surgimiento de las APT

(Advanced Persistent Threats), ataques altamente sofisticados y prolongados en el tiempo, dirigidos a obtener acceso no autorizado a información sensible.

Uno de los incidentes más significativos de este periodo fue el ataque Stuxnet en 2010, un gusano informático diseñado específicamente para sabotear las instalaciones nucleares de Irán. Este ataque marcó un hito en la historia de la ciberseguridad al demostrar que los ciberataques podían tener efectos devastadores en el mundo físico. Stuxnet atacó las centrifugadoras nucleares, haciéndolas funcionar a velocidades peligrosas mientras mostraba lecturas normales a los operadores, lo que provocó daños físicos significativos sin ser detectado en tiempo real (Zetter, 2014). El impacto de Stuxnet trascendió el ámbito técnico, revelando las capacidades ofensivas de los ciberataques en conflictos internacionales y la necesidad de establecer normativas globales para la ciberseguridad y ciberdefensa. Diversos analistas atribuyen su autoría a operaciones conjuntas de Estados Unidos e Israel. Sin embargo, esta atribución nunca fue confirmada oficialmente, lo que refuerza la complejidad de la atribución en el ciberespacio.[4]

En respuesta a la creciente sofisticación de los ataques cibernéticos, muchos países comenzaron a desarrollar estrategias nacionales de ciberseguridad. Estonia, uno de los países más digitalizados del mundo, fue pionera en esta área tras sufrir un ataque cibernético masivo en 2007 que paralizó sus servicios gubernamentales y financieros. Este ataque, atribuido a Rusia, aunque nunca oficialmente confirmado, demostró la vulnerabilidad de las infraestructuras digitales de una nación y motivó la creación de políticas de ciberseguridad más robustas, así como el establecimiento del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Tallin (Schreier, 2012).

España también ha avanzado significativamente en ciberseguridad mediante la implementación de la Estrategia Nacional de Ciberseguridad, que busca proteger infraestructuras críticas y fomentar la cooperación entre el sector público y privado. Esta estrategia se basa en principios como la prevención, detección y respuesta temprana ante incidentes de ciberseguridad, así como la promoción de la investigación e innovación en ciberseguridad. Además, España ha desarrollado una estructura de gobernanza cibernética sólida, con el Centro Criptológico Nacional (CCN) desempeñando un papel clave en la coordinación de la ciberseguridad a nivel gubernamental (Estrategia Nacional de Ciberseguridad de España, 2019).

4 Langner (2011) y Zetter (2014) debaten la atribución, pero no la confirman oficialmente.

A medida que las amenazas cibernéticas se diversifican y sofistican, la ciberseguridad ha evolucionado hacia un enfoque proactivo y preventivo. Ya no se trata solo de proteger los sistemas informáticos, sino también de anticipar posibles amenazas y responder rápidamente a incidentes de seguridad. La ciber inteligencia y la ciber defensa se han convertido en componentes esenciales para prevenir ataques dirigidos, como el espionaje cibernético y las campañas de desinformación.

En este contexto, la cooperación internacional se ha vuelto fundamental. Organizaciones como la OTAN y la Unión Europea han intensificado sus esfuerzos en la colaboración cibernética, desarrollando normativas y estándares internacionales para garantizar la seguridad del ciberespacio. Además, el intercambio de información entre sectores públicos y privados se ha consolidado como una práctica clave para enfrentar amenazas globales que no reconocen fronteras.

La evolución de la ciberseguridad refleja la creciente dependencia de la sociedad en las tecnologías digitales y la necesidad de proteger tanto la información personal como las infraestructuras críticas. Desde los primeros virus informáticos hasta los sofisticados ataques de ciberguerra, la ciberseguridad ha pasado de ser una preocupación técnica para convertirse en un componente esencial de la seguridad nacional y global. A medida que las amenazas continúan evolucionando, la cooperación internacional y el desarrollo de estrategias proactivas serán fundamentales para garantizar un ciberespacio seguro y confiable.

1.3. Amenazas cibernéticas y su impacto en la seguridad pública

Las amenazas cibernéticas han evolucionado significativamente en los últimos años, transformándose en un desafío crítico para la seguridad pública a nivel global. La creciente dependencia de infraestructuras digitales y sistemas interconectados ha ampliado la superficie de ataque, exponiendo a las sociedades a riesgos que afectan desde servicios esenciales hasta la estabilidad económica y política de las naciones. Este contexto ha generado una urgente necesidad de desarrollar estrategias de ciberseguridad más robustas y coordinadas, enfocadas en proteger tanto a individuos como a organizaciones y gobiernos.

El phishing se ha consolidado como una de las técnicas de ingeniería social más utilizadas y efectivas para obtener información confidencial. Este tipo de ataque explota la confianza humana mediante correos electrónicos, mensajes de texto o sitios web fraudulentos que imitan a fuentes legítimas. A pesar de los avances en soluciones de seguridad, el phishing sigue siendo una táctica exitosa debido a su capacidad para adaptarse a diferentes contextos culturales y lingüísticos, utilizando información obtenida de redes sociales para personalizar los ataques. El spear phishing, una variante más sofisticada, dirige sus ataques a individuos o grupos específicos con mensajes altamente personalizados, lo que aumenta su tasa de éxito (Krebs, 2023). La creciente sofisticación del phishing ha afectado a instituciones gubernamentales, financieras y de salud, generando pérdidas económicas significativas y comprometiendo datos personales y sensibles.

Otra amenaza que ha crecido exponencialmente en los últimos años es el ransomware, un tipo de malware que cifra los datos de la víctima y exige un rescate, generalmente en criptomonedas, a cambio de restaurar el acceso a la información. Los ataques de ransomware han afectado a organizaciones de todos los sectores, incluidos los servicios críticos como hospitales, escuelas e infraestructuras gubernamentales. Un ejemplo notable fue el ataque al sistema de salud irlandés en 2021, que paralizó hospitales y centros de atención médica, afectando directamente a la seguridad pública y la prestación de servicios esenciales (Gallagher, 2022). El impacto del ransomware no se limita solo a la pérdida de datos o al costo del rescate, sino que también incluye el tiempo de inactividad de los servicios, el daño a la reputación y las posibles consecuencias legales derivadas de la violación de datos personales. Además, el surgimiento del modelo de negocio Ransomware-as-a-Service (RaaS) ha facilitado la

proliferación de estos ataques al permitir que los cibercriminales alquilen herramientas de ransomware a otros atacantes menos experimentados, democratizando el acceso a este tipo de amenaza y aumentando su alcance global (Check Point Research, 2023).

Los ataques de denegación de servicio distribuido (DDoS) también representan una amenaza significativa para la seguridad pública. Estos ataques buscan saturar el tráfico de un servidor o red, haciéndolos inaccesibles para usuarios legítimos. A diferencia de otros ciberataques, los DDoS no buscan robar información, sino interrumpir la disponibilidad de servicios críticos, generando caos y afectando la confianza en las instituciones. Un ejemplo destacado fue el ataque a los sitios web gubernamentales y bancarios de Ucrania en 2022, considerado uno de los mayores ataques DDoS en la historia del país, y que fue ampliamente interpretado como parte de una estrategia de guerra híbrida en el contexto de las tensiones geopolíticas con Rusia (BBC News, 2022). La creciente utilización de dispositivos del Internet de las Cosas (IoT) ha ampliado el alcance de los ataques DDoS, ya que muchos de estos dispositivos no cuentan con medidas de seguridad adecuadas, lo que los convierte en objetivos vulnerables para la creación de botnets capaces de generar volúmenes masivos de tráfico malicioso (Kaspersky Lab, 2023).

Los ataques a infraestructuras críticas representan una de las amenazas más graves para la seguridad pública, ya que pueden interrumpir servicios esenciales como el suministro eléctrico, el agua potable, el transporte y las comunicaciones. Estos ataques no solo afectan la operatividad de los sistemas, sino que también generan un impacto psicológico y social significativo, creando pánico y desestabilización social. Un ejemplo de esto fue el ataque al sistema de energía eléctrica de Ucrania en 2015, que dejó sin electricidad a más de 220,000 personas, evidenciando la vulnerabilidad de los sistemas de control industrial ante amenazas cibernéticas (Hultquist, 2016). En 2021, un ataque al sistema de tratamiento de agua en Oldsmar, Florida, mostró cómo un atacante intentó aumentar peligrosamente los niveles de hidróxido de sodio en el suministro de agua, lo que podría haber causado daños graves a la salud pública si no hubiera sido detectado a tiempo (CISA, 2021). Estos incidentes subrayan la importancia de proteger las infraestructuras críticas con medidas de ciberseguridad más robustas y la necesidad de una mayor cooperación internacional para abordar estas amenazas transnacionales.

Además de las amenazas técnicas, actores estatales y no estatales han comenzado a utilizar ciberataques como herramientas de guerra híbrida, espionaje y

manipulación de la opinión pública. Estas amenazas cibernéticas no solo buscan obtener información confidencial, sino también influir en elecciones, sembrar desconfianza y desestabilizar políticamente a las naciones. La creciente interconexión global y la dependencia de las infraestructuras digitales han facilitado la capacidad de estos actores para operar de manera remota y anónima, dificultando la atribución de los ataques y aumentando la complejidad de la respuesta y la defensa cibernética (Rid, 2022). La guerra híbrida combina tácticas militares convencionales con ciberataques, sabotajes y desinformación, lo que la convierte en una estrategia compleja y asimétrica que desafía las respuestas tradicionales de seguridad nacional.

En resumen, las amenazas cibernéticas han evolucionado no solo en términos de sofisticación técnica, sino también en su capacidad para generar un impacto profundo en la seguridad pública y la estabilidad global. La necesidad de políticas de ciberseguridad más robustas, junto con una mayor cooperación internacional, es fundamental para mitigar los riesgos asociados con estas amenazas en constante evolución. La creciente dependencia de infraestructuras digitales críticas requiere un enfoque integral de ciberseguridad que abarque tanto las soluciones tecnológicas como la concienciación y educación del factor humano para reducir las vulnerabilidades explotadas por los atacantes.

1.4. El factor humano en la ciberseguridad

El factor humano es ampliamente reconocido como uno de los componentes más vulnerables en el ámbito de la ciberseguridad. A pesar de los continuos avances tecnológicos en protección de sistemas, las acciones, decisiones y comportamientos de los usuarios continúan siendo un punto crítico susceptible de ser explotado por ciberdelincuentes. Se estima que entre el 70% y el 90% de las brechas de seguridad están directamente relacionadas con errores humanos, lo que subraya la necesidad de abordar estas vulnerabilidades desde una perspectiva conductual y educativa (Verizon, 2023).[5]

Uno de los errores más comunes es el uso de contraseñas débiles o fácilmente predecibles. A pesar de las constantes recomendaciones, muchos usuarios siguen utilizando combinaciones simples como "123456" o "password", facilitando el acceso no autorizado a cuentas personales y corporativas (NordPass, 2022). Además, la reutilización de la misma contraseña en múltiples plataformas amplifica el riesgo, ya que una vez comprometida una cuenta, las demás quedan igualmente expuestas. Para mitigar este riesgo, se recomienda la creación de contraseñas robustas que combinen letras, números y caracteres especiales, así como el uso de gestores de contraseñas y la implementación de autenticación multifactorial (NIST, 2022).

La ingeniería social representa otra amenaza significativa en el ámbito de la ciberseguridad, ya que explota la confianza y la vulnerabilidad psicológica de las personas. Este tipo de ataque manipula a los usuarios para obtener información confidencial o acceso a sistemas protegidos, utilizando tácticas de persuasión y engaño. Las técnicas de ingeniería social incluyen el phishing, smishing (phishing mediante SMS) y vishing (phishing mediante llamadas de voz). El phishing, en particular, ha demostrado ser altamente efectivo debido a su capacidad para personalizar los mensajes y hacerse pasar por entidades legítimas. Estos ataques explotan la falta de atención y el exceso de confianza de los individuos, destacando la importancia de la educación y la concienciación en ciberseguridad para reconocer y evitar estas tácticas maliciosas (Krebs, 2023). Según el informe anual de ciberseguridad de Proofpoint (2023), más del

[5] La proporción de brechas de seguridad relacionadas con errores humanos varía según el estudio y el contexto analizado. Sin embargo, informes de seguridad consistentes, como el Data Breach Investigations Report de Verizon (2023), señalan que el factor humano sigue siendo el eslabón más débil en la cadena de ciberseguridad, independientemente de los avances en soluciones tecnológicas.

80% de las organizaciones han experimentado intentos de phishing, lo que subraya la magnitud de este problema global.

La instalación de software no autorizado por parte de empleados es otra vulnerabilidad común en la ciberseguridad organizacional. Al descargar e instalar aplicaciones sin la aprobación del departamento de TI, se pueden introducir programas maliciosos o crear incompatibilidades que comprometan la seguridad de la organización. Esto incluye desde aplicaciones aparentemente inofensivas hasta herramientas de productividad que contienen spyware o malware oculto. Para prevenir este tipo de incidentes, es esencial establecer políticas claras sobre el uso de software y garantizar que los empleados comprendan los riesgos asociados con la instalación de aplicaciones no verificadas (SANS Institute, 2022). Asimismo, el uso de dispositivos personales en entornos laborales (BYOD, Bring Your Own Device) ha aumentado los riesgos de seguridad, ya que estos dispositivos pueden no contar con los mismos estándares de protección que los equipos corporativos.

Otra vulnerabilidad crítica es la omisión en la actualización de software y sistemas. Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades descubiertas, por lo que no aplicarlas oportunamente deja a los sistemas expuestos a posibles explotaciones. Este problema fue evidente en el ataque de ransomware WannaCry en 2017, que aprovechó una vulnerabilidad en el sistema operativo Windows que ya había sido parcheada, pero que muchas organizaciones no habían actualizado (Symantec, 2018). Para mitigar este riesgo, es fundamental implementar procedimientos que aseguren la actualización regular y automática de todos los componentes tecnológicos dentro de una organización.

Además, la divulgación accidental de información sensible es un riesgo latente en el ámbito de la ciberseguridad. Errores como enviar correos electrónicos al destinatario equivocado, compartir documentos confidenciales sin las debidas precauciones o no cifrar datos sensibles pueden resultar en filtraciones de datos con consecuencias legales y reputacionales. La implementación de protocolos rigurosos para el manejo de información y la formación continua en prácticas seguras de comunicación son medidas preventivas indispensables (McAfee, 2022). Un estudio de IBM Security (2023) reveló que el 23% de las filtraciones de datos se debieron a errores humanos, lo que resalta la necesidad de reforzar la concienciación en el manejo de información confidencial.

Para abordar eficazmente estas vulnerabilidades humanas, las organizaciones deben invertir en programas de formación y concienciación en ciberseguridad. La educación regular y actualizada ayuda a los empleados a identificar amenazas potenciales y a adoptar comportamientos que refuercen la seguridad. La formación continua debe abordar temas como la gestión segura de contraseñas, la identificación de correos electrónicos fraudulentos, el manejo adecuado de la información personal y la importancia de las actualizaciones de software. Además, fomentar una cultura organizacional que priorice la ciberseguridad y establezca canales de comunicación abiertos para reportar incidentes puede reducir significativamente el riesgo asociado al factor humano (ENISA, 2023).

A pesar de las soluciones tecnológicas avanzadas, las vulnerabilidades humanas siguen siendo el eslabón más débil en la cadena de ciberseguridad. La creciente sofisticación de las tácticas de ingeniería social, junto con la constante evolución de las amenazas cibernéticas, exige un enfoque integral que combine medidas tecnológicas, educativas y organizacionales. La creación de una cultura de seguridad sólida, respaldada por políticas claras y una formación continua, es esencial para mitigar los riesgos asociados con el factor humano y fortalecer la defensa contra las amenazas cibernéticas modernas.

1.5. Estrategias internacionales en ciberseguridad:

En el contexto global actual, donde la transformación digital y la interconexión de infraestructuras críticas han redefinido el funcionamiento de las sociedades modernas, contar con una estrategia de ciberseguridad sólida y bien articulada se ha convertido en un pilar fundamental para la seguridad nacional y la estabilidad económica (Banco Interamericano de Desarrollo, 2018). La creciente dependencia de tecnologías digitales ha abierto nuevas oportunidades para el desarrollo y la innovación, pero también ha ampliado la superficie de ataque para actores malintencionados, incrementando exponencialmente los riesgos de ciberamenazas complejas y dirigidas (INCIBE, 2021).

Las estrategias de ciberseguridad no solo buscan proteger datos e infraestructuras críticas, sino también garantizar la continuidad operativa de servicios esenciales y salvaguardar la privacidad y la integridad de la información. En un mundo donde los ciberataques pueden paralizar redes eléctricas, interrumpir sistemas de salud o comprometer la seguridad financiera de las naciones, la ciberseguridad ha pasado a ocupar un lugar prioritario en las agendas de políticas públicas a nivel mundial. La sofisticación de las amenazas, que van desde el ransomware hasta los ataques patrocinados por Estados, exige un enfoque integral que combine no solo medidas tecnológicas, sino también educativas, organizacionales y normativas (Centro Criptológico Nacional, s.f.).

La necesidad de una estrategia de ciberseguridad integral no solo responde a la protección de sistemas y datos, sino también a la construcción de una cultura de ciberseguridad que abarque a todos los niveles de la sociedad. Esta cultura debe promover un enfoque preventivo y proactivo, capaz de adaptarse a la rápida evolución de las amenazas cibernéticas (Observatorio de Ciberseguridad, 2022). La formación continua y la concienciación en ciberseguridad son componentes esenciales para mitigar el factor humano, que sigue siendo el eslabón más débil en la cadena de seguridad digital (INCIBE, 2021).

En este contexto, Estonia y España han destacado como referentes globales en la implementación de estrategias de ciberseguridad. Estonia, tras sufrir un ataque masivo en 2007, ha construido una infraestructura digital resiliente y ha desarrollado un enfoque de seguridad basado en la colaboración público-privada, la educación continua y la integración de soluciones innovadoras como la identificación electrónica (e-ID) y

los sistemas de votación electrónica segura (Banco Interamericano de Desarrollo, 2018). Además, Estonia ha fomentado la educación en ciberseguridad desde las primeras etapas del sistema educativo, promoviendo una cultura digital segura y resiliente (Observatorio de Ciberseguridad, 2022)

España, por su parte, ha adoptado un enfoque integral a través de la Estrategia Nacional de Ciberseguridad, que combina medidas de protección de infraestructuras críticas, programas de sensibilización y formación, y la coordinación entre organismos públicos y privados a través del Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (INCIBE) (INCIBE, 2021). A través de programas de formación y campañas de concienciación, España ha logrado involucrar a ciudadanos, empresas y organismos públicos en la construcción de una cultura de ciberseguridad compartida (Ministerio de Asuntos Económicos y Transformación Digital, 2020).

La importancia de analizar y comprender las estrategias internacionales de ciberseguridad radica en la necesidad de adaptar las mejores prácticas a contextos específicos, como el sector público argentino, que enfrenta desafíos similares en términos de protección de infraestructuras críticas y formación de sus empleados en ciberseguridad (Banco Interamericano de Desarrollo, 2018). Además, este análisis comparativo permite identificar áreas de mejora y oportunidades para la cooperación internacional, fundamentales en un entorno digital donde las amenazas no conocen fronteras.

En el Capítulo 2: Análisis Comparativo de Estrategias de Ciberseguridad, se explorarán en detalle las estrategias implementadas por Estonia y España, evaluando sus enfoques en políticas públicas, colaboración multisectorial y formación en ciberseguridad. Se analizarán sus éxitos y desafíos, así como su aplicabilidad en el contexto argentino, proporcionando una visión integral que contribuirá al desarrollo de políticas públicas adaptadas y efectivas en materia de ciberseguridad.

Esta introducción contextualiza la relevancia de las estrategias de ciberseguridad en el panorama global actual y establece el marco teórico para el análisis comparativo en el capítulo siguiente, destacando la importancia de adoptar un enfoque holístico y adaptable ante un entorno digital en constante evolución.

1.6. La importancia de la concienciación en ciberseguridad

La concienciación en ciberseguridad se establece como un pilar esencial en la protección de los sistemas de información y la mitigación de riesgos asociados al factor humano. Aunque las soluciones tecnológicas avanzan constantemente, la seguridad integral depende en gran medida del comportamiento y la educación de los usuarios. Sin una cultura sólida de seguridad cibernética, las organizaciones permanecen vulnerables a diversas amenazas, independientemente de las defensas tecnológicas implementadas.

La implementación de programas de concienciación ha demostrado ser efectiva en la reducción de incidentes de seguridad. Estos programas no solo informan, sino que buscan transformar comportamientos mediante enfoques prácticos y participativos. Por ejemplo, un estudio reciente evidenció que entrenamientos interactivos, como discusiones grupales y simulaciones de roles, incrementan la autoeficacia de los empleados y su disposición a buscar apoyo ante correos electrónicos sospechosos, mejorando la detección y reporte de intentos de phishing (Chen et al., 2024).[6]

Además, la educación en ciberseguridad fortalece la primera línea de defensa de una organización: sus empleados. Al estar capacitados para identificar y responder adecuadamente a amenazas como el phishing, el malware y otras formas de ingeniería social, se minimiza el riesgo de brechas de seguridad originadas por errores humanos. La formación continua y adaptada a las necesidades específicas de la organización es crucial para mantener una postura de seguridad robusta (Fortinet, 2024).

Es importante destacar que la concienciación en ciberseguridad no solo protege los activos digitales de una organización, sino que también salvaguarda su reputación. Un incidente de seguridad puede erosionar la confianza de clientes y socios comerciales, afectando negativamente la posición de la empresa en el mercado. Por lo tanto, invertir en programas de concienciación demuestra un compromiso proactivo con la protección de datos y la integridad operativa (Smartfense, 2023).

En resumen, la concienciación en ciberseguridad es un componente indispensable en la estrategia de defensa de cualquier organización. Fomentar una cultura de seguridad a través de programas educativos prácticos y continuos no solo

[6] La autoeficacia se refiere a la creencia en la capacidad propia para ejecutar acciones necesarias que permitan alcanzar objetivos específicos. En el contexto de la ciberseguridad, una mayor autoeficacia implica confianza en la habilidad para identificar y manejar amenazas cibernéticas de manera efectiva.

reduce la incidencia de ataques exitosos, sino que también fortalece la resiliencia organizacional frente a un panorama de amenazas en constante evolución.

Capítulo 2: Análisis Comparativo de Estrategias de Ciberseguridad

2.1. Estrategias nacionales de ciberseguridad en Estonia y España

La ciberseguridad se ha convertido en un pilar esencial para proteger las infraestructuras críticas, la información sensible y la estabilidad económica de los países. En este contexto, Estonia y España han desarrollado estrategias nacionales de ciberseguridad que se destacan no solo por su enfoque tecnológico avanzado, sino también por sus programas integrales de formación y concienciación en ciberseguridad. Ambas naciones han adoptado un enfoque holístico que abarca políticas gubernamentales, colaboración público-privada e iniciativas educativas continuas para fortalecer su postura de ciberseguridad (ENISA, 2023). Este análisis profundiza en las estrategias de ciberseguridad de Estonia y España, con un énfasis particular en sus esfuerzos por promover una cultura de seguridad digital a través de la formación y la concienciación.

Estonia: El modelo de ciberseguridad digital.

Estonia se ha consolidado como un referente mundial en ciberseguridad, especialmente después de los ciberataques masivos de 2007 que paralizaron gran parte de su infraestructura digital, incluido el sistema bancario, el gobierno y los medios de comunicación (Czosseck, Ottis & Talihärm, 2011). Estos eventos impulsaron al país a desarrollar un enfoque integral y proactivo de ciberseguridad que ha servido como modelo para otras naciones. La Estrategia de Ciberseguridad de Estonia 2019-2022 se basa en cuatro pilares clave: protección de la infraestructura crítica, desarrollo de capacidades de ciberdefensa, cooperación internacional y formación continua en ciberseguridad (Ministry of Economic Affairs and Communications of Estonia, 2023).

Uno de los pilares fundamentales de la estrategia es la colaboración internacional. En Estonia se encuentra el Centro de Excelencia Cooperativa de Defensa Cibernética de la OTAN (CCDCOE), una institución de investigación y formación en ciberdefensa que proporciona recursos educativos y programas de capacitación a profesionales de la ciberseguridad a nivel mundial (CCDCOE, 2023). El CCDCOE organiza anualmente el ejercicio Locked Shields, considerado el simulacro de ciberdefensa más grande y avanzado del mundo. Locked Shields permite a los especialistas en ciberseguridad enfrentar escenarios de ataque realistas en un entorno controlado, promoviendo la cooperación internacional y mejorando sus habilidades

tácticas en tiempo real (NATO Cooperative Cyber Defence Centre of Excellence, 2023).

A nivel nacional, Estonia ha implementado programas continuos de formación para sus empleados públicos a través de la e-Governance Academy (eGA). Esta organización, fundada en 2002, ha sido clave en la capacitación de funcionarios gubernamentales en ciberseguridad, protección de datos y e-democracia. La eGA proporciona formación en ciberseguridad tanto a nivel nacional como internacional, compartiendo mejores prácticas y lecciones aprendidas en la protección de infraestructuras digitales gubernamentales (e-Governance Academy, 2023). Estos programas incluyen talleres, seminarios y módulos de formación en línea, cubriendo desde conceptos básicos hasta competencias avanzadas en ciberdefensa.

Estonia ha integrado la ciberseguridad en todos los niveles del sistema educativo. La Universidad Tecnológica de Tallin (TalTech) lidera este esfuerzo mediante su Maestría en Ciberseguridad, un programa desarrollado en colaboración con el CCDCOE y expertos de la industria (TalTech, 2023). Este máster combina teoría y práctica, permitiendo a los estudiantes abordar desafíos complejos de ciberseguridad a través de ejercicios prácticos y simulaciones de ataques. Además, TalTech trabaja en conjunto con el Ministerio de Educación e Investigación de Estonia para actualizar constantemente sus planes de estudio y garantizar que los graduados estén equipados con las competencias más avanzadas en ciberseguridad (Vaher, 2023).

El enfoque de Estonia no se limita a la formación universitaria. El país ha implementado programas de capacitación continua y profesional para asegurar que una amplia gama de profesionales adquiera competencias en seguridad informática. Estos programas abarcan desde la formación técnica avanzada hasta la concienciación general en ciberseguridad, promoviendo una cultura de seguridad digital en todos los sectores. Asimismo, Estonia ha integrado la ciberseguridad en su plan de estudios escolar, enseñando a los estudiantes desde una edad temprana sobre las buenas prácticas en línea y la importancia de la protección de datos (Ministry of Economic Affairs and Communications of Estonia, 2023).

España: Estrategia Nacional de Ciberseguridad

España ha reconocido la formación y capacitación continua de los empleados del sector público como un componente esencial de su Estrategia Nacional de

Ciberseguridad, estableciendo un enfoque integral que abarca desde la educación formal hasta programas especializados en ciberseguridad. Este enfoque se basa en la comprensión de que las amenazas cibernéticas evolucionan constantemente y requieren una preparación adaptativa y continua. La formación en ciberseguridad en España no solo busca dotar a los empleados públicos de competencias técnicas avanzadas, sino también promover una cultura de concienciación que minimice los riesgos derivados de errores humanos (Gobierno de España, 2019).

En este contexto, España ha incrementado significativamente su oferta educativa en ciberseguridad. Actualmente, más de 120 centros educativos imparten titulaciones de Formación Profesional en Ciberseguridad en Entornos de las Tecnologías de la Información (CETI) y Ciberseguridad en Entornos de las Tecnologías de la Operación (CETO) (INCIBE, s.f.). Estas titulaciones ofrecen a los estudiantes habilidades prácticas y actualizadas, preparándolos para abordar desafíos contemporáneos en materia de seguridad digital. Además, en el ámbito universitario, España cuenta con más de 80 programas de máster en ciberseguridad, garantizando un flujo constante de profesionales capacitados para integrarse en el sector público y privado (Huffington Post, 2025). Un ejemplo de ello es la Universidad de Jaén, que ha implementado programas de máster en ciberseguridad enfocados en ciber inteligencia, análisis forense digital y gestión de incidentes cibernéticos, capacitando a los estudiantes para defender tanto a instituciones públicas como a empresas privadas de posibles amenazas cibernéticas (Universidad de Jaén, 2023).

El Instituto Nacional de Ciberseguridad (INCIBE) desempeña un papel clave en la capacitación continua de los empleados del sector público en España. A través de su Catálogo de Formación en Ciberseguridad, INCIBE ofrece cursos en línea gratuitos que abarcan desde conceptos básicos de ciberseguridad hasta técnicas avanzadas de defensa cibernética (INCIBE, s.f.). Estos programas están diseñados específicamente para mejorar las competencias digitales de los empleados públicos y fomentar una cultura de seguridad en las administraciones públicas. Asimismo, el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), proporciona formación especializada a través del CCN-CERT, unidad de respuesta a incidentes de seguridad de la información. Esta formación incluye gestión de incidentes, protección de infraestructuras críticas y ciber inteligencia (CCN-CERT, s.f.). Estos programas no solo dotan a los empleados públicos de conocimientos técnicos avanzados, sino que también

promueven una cultura de ciberseguridad basada en la prevención y respuesta proactiva ante incidentes cibernéticos.

Uno de los aspectos más innovadores de la estrategia española es su enfoque multidimensional en la capacitación en ciberseguridad, integrando la formación técnica con programas de concienciación diseñados para modificar comportamientos y promover buenas prácticas en el uso de tecnologías digitales. La formación no solo se limita al conocimiento técnico, sino que también enfatiza la responsabilidad compartida en la protección de la información pública. Esta estrategia se basa en el principio de que la ciberseguridad no es solo responsabilidad de los especialistas en TI, sino de todos los empleados del sector público, quienes juegan un papel crucial en la protección de la información pública y la resiliencia organizacional.

España ha implementado un sistema de capacitación continua y adaptativa que garantiza que los funcionarios mantengan actualizados sus conocimientos y habilidades en un entorno digital en constante cambio. Un ejemplo de ello es el Programa de Formación Continuada en Ciberseguridad del CCN, que incluye módulos de actualización periódica y simulaciones de ciberincidentes en tiempo real, permitiendo a los empleados practicar en un entorno controlado cómo responder a amenazas cibernéticas complejas (CCN-CERT, s.f.). Este enfoque proactivo no solo mejora la capacidad de respuesta ante incidentes, sino que también fomenta una cultura de resiliencia organizacional.[7]

A nivel regional y local, España ha demostrado un compromiso significativo con la ciberseguridad. En Andalucía, la Agencia Digital de Andalucía ha centralizado el presupuesto TIC con una inversión de 510 millones de euros para fortalecer la ciberseguridad en sus administraciones públicas. Además, se han organizado congresos de ciberseguridad para promover la formación y concienciación en este ámbito (Cadena SER, 2025). En el ámbito local, municipios como Fuenlabrada han establecido comités de seguridad y privacidad para mejorar la protección de sus sistemas de información. La adhesión a la Red Nacional Española de Centros de Operaciones de Seguridad permite a estos municipios colaborar e intercambiar información en tiempo real sobre amenazas y vulnerabilidades, fortaleciendo así su postura de seguridad (Cadena SER, 2025).

[7] La implementación de programas de formación en ciberseguridad para empleados del sector público no solo mejora la capacidad de respuesta ante incidentes, sino que también fomenta una cultura de seguridad digital en todas las esferas gubernamentales, contribuyendo a crear un entorno digital más seguro y resiliente.

A pesar de los avances en formación y capacitación, España enfrenta una creciente demanda de profesionales en ciberseguridad. En 2021, se estimaba que el número de profesionales necesarios en este ámbito ascendía a 63.191, con una proyección de superar los 83.000 en 2024 (INCIBE, s.f.). Esta brecha destaca la necesidad de continuar invirtiendo en programas de formación y atraer talento especializado para satisfacer las demandas del sector público y privado.

La comparación de las estrategias nacionales de ciberseguridad de Estonia y España revela enfoques complementarios y efectivos en la protección de infraestructuras digitales críticas, así como en la formación y concienciación de sus ciudadanos y empleados públicos. Aunque ambos países han adoptado políticas proactivas en ciberseguridad, sus métodos reflejan sus contextos históricos y necesidades particulares.

Estonia, como pionera en gobernanza digital y resiliencia cibernética, ha integrado la ciberseguridad en todos los niveles de su sociedad, desde la educación primaria hasta la capacitación continua de sus empleados públicos. La experiencia de enfrentarse a un ciberataque masivo en 2007 impulsó a Estonia a crear una infraestructura digital segura y eficiente, apoyada por una sólida colaboración público-privada y un enfoque centrado en la prevención de ataques. La inclusión de la identificación digital (e-ID) y la votación electrónica segura han consolidado su posición como líder en seguridad digital y transparencia gubernamental.

Por otro lado, España ha adoptado un enfoque integral y colaborativo, desarrollando una Estrategia Nacional de Ciberseguridad que no solo protege infraestructuras críticas, sino que también fomenta una cultura de concienciación en ciberseguridad a través de programas educativos y de formación continua. La participación activa del Instituto Nacional de Ciberseguridad (INCIBE) y del Centro Criptológico Nacional (CCN) en la capacitación de empleados públicos y la concienciación ciudadana ha permitido una respuesta coordinada ante incidentes cibernéticos. Además, España ha demostrado un compromiso significativo a nivel regional y local, fomentando la cooperación entre comunidades autónomas y municipios, y promoviendo el intercambio de información en tiempo real sobre amenazas cibernéticas.

Ambos países han logrado avances significativos en la capacitación continua de empleados públicos y en la sensibilización de la ciudadanía frente a las amenazas

digitales. Sin embargo, la experiencia estonia resalta la importancia de integrar la ciberseguridad desde la educación básica, mientras que el enfoque español destaca el valor de la coordinación interinstitucional y la cooperación regional y local. Estas diferencias reflejan sus contextos políticos y culturales, pero también ofrecen lecciones valiosas para otros países, especialmente para Argentina, que enfrenta desafíos similares en la protección de sus infraestructuras digitales.

En conclusión, las estrategias de ciberseguridad de Estonia y España ofrecen modelos complementarios y exitosos que pueden servir como referencia para otros países en la construcción de resiliencia cibernética. La integración educativa y la colaboración público-privada en Estonia, junto con el enfoque integral y la cooperación regional en España, muestran que una estrategia de ciberseguridad efectiva requiere no solo tecnologías avanzadas, sino también una cultura de concienciación y responsabilidad compartida. En el próximo apartado, se analizará la situación actual de la ciberseguridad en Argentina, comparando sus políticas y desafíos con los modelos exitosos de Estonia y España, con el fin de identificar oportunidades de mejora y recomendaciones estratégicas

2.2. Ciberseguridad en Argentina y Comparativa Internacional

La ciberseguridad se ha consolidado como un componente esencial en la protección de las infraestructuras digitales y la información sensible de las naciones. En este contexto, Argentina ha avanzado en la implementación de políticas y estrategias para fortalecer su seguridad cibernética. Sin embargo, al comparar su enfoque con el de países como Estonia y España, se evidencian diferencias significativas en términos de desarrollo, implementación y eficacia de las estrategias nacionales de ciberseguridad. Estas diferencias no solo reflejan las prioridades políticas y económicas de cada país, sino también sus respectivos niveles de madurez digital y su capacidad de respuesta ante las crecientes amenazas cibernéticas (National Cyber Security Index, s.f.).

Estonia, tras los ciberataques de 2007, se posicionó como líder en ciberdefensa y seguridad. Estos eventos impulsaron al país a desarrollar una infraestructura digital robusta y a promover una cultura de seguridad cibernética entre sus ciudadanos. La colaboración público-privada y la educación en ciberseguridad desde etapas tempranas son pilares fundamentales de su estrategia nacional (Consumer Choice Center, 2019). La creación del Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN en Tallin ha sido clave para consolidar su posición en la vanguardia de la ciberseguridad global (FDRA, 2024). En 2017, Estonia alcanzó la posición más alta de Europa y la quinta a nivel mundial en el Ranking Global de Ciberseguridad (FDRA, 2024), lo cual evidencia la eficacia de sus políticas de ciberseguridad.

Por otro lado, España ha desarrollado una Estrategia Nacional de Ciberseguridad que enfatiza la protección de infraestructuras críticas y la concienciación pública. A través del Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Criptológico Nacional (CCN), lidera iniciativas de formación y respuesta a incidentes cibernéticos. Además, España ha avanzado en la implementación de la Directiva NIS 2 de la Unión Europea, reforzando las normas de ciberseguridad para entidades críticas en diversos sectores (El País, 2025). La cooperación interinstitucional y la formación continua para empleados públicos han sido factores determinantes en el fortalecimiento de su postura en ciberseguridad.

En contraste, Argentina ha mostrado progresos en su enfoque hacia la ciberseguridad, aunque enfrenta desafíos en comparación con Estonia y España. En 2021, Argentina aprobó su Segunda Estrategia Nacional de Ciberseguridad, actualizando la versión de 2019, con el objetivo de enfrentar los nuevos desafíos que

presentan los constantes avances tecnológicos (Argentina.gob.ar, 2021). Sin embargo, según el National Cyber Security Index (NCSI), Argentina se posiciona en el puesto 38 a nivel global, con una puntuación de 58.33, mientras que Estonia ocupa el quinto lugar con 88.33, y España se sitúa en la posición 21 con 73.33 (National Cyber Security Index, s.f.). Este posicionamiento refleja la necesidad de fortalecer sus políticas y marcos regulatorios en ciberseguridad.

Figura 3: Indice Nacional de Ciberseguridad

Fuente: National Cyber Security Index, s.f.

Uno de los desafíos clave para Argentina es la adopción de tecnologías de ciberseguridad. Se estima que el país está entre dos y tres años por detrás de mercados más avanzados en la implementación de soluciones de seguridad cibernética (Argentina.gob.ar, 2023). Esta brecha tecnológica puede atribuirse a factores como la inestabilidad económica y la priorización de otras preocupaciones, como la seguridad física. Además, la falta de recursos y la escasa inversión en investigación y desarrollo limitan la capacidad del país para innovar y adaptarse a las nuevas amenazas digitales.

A pesar de estos desafíos, Argentina ha tomado medidas para mejorar su postura en ciberseguridad. La creación del Observatorio Argentino del Ciberespacio y la implementación de programas de formación en seguridad informática son pasos positivos hacia la construcción de una cultura de ciberseguridad más sólida (Fundación Sadosky, s.f.). No obstante, es crucial que el país continúe desarrollando e implementando una estrategia nacional de ciberseguridad coherente y efectiva,

aprendiendo de las experiencias de Estonia y España. La colaboración público-privada y la cooperación internacional son aspectos clave para fortalecer la resiliencia cibernética en Argentina.

En resumen, mientras que Estonia y España han establecido marcos robustos y proactivos en ciberseguridad, Argentina se encuentra en una fase de desarrollo que requiere atención y recursos adicionales. La adopción de políticas integrales, la inversión en infraestructura de seguridad y la promoción de la concienciación pública son elementos esenciales para que Argentina fortalezca su resiliencia cibernética y se alinee con las mejores prácticas internacionales. La experiencia de Estonia en la integración de la ciberseguridad desde etapas tempranas en el sistema educativo, así como el enfoque integral de España en la cooperación interinstitucional, ofrecen lecciones valiosas que Argentina puede adaptar a su contexto local.

2.3. Lecciones aprendidas y recomendaciones para Argentina

La experiencia de Estonia y España en la implementación de estrategias nacionales de ciberseguridad proporciona valiosas lecciones para Argentina, especialmente en lo que respecta a la organización, colaboración intersectorial y concienciación pública. Al analizar las políticas de ciberseguridad de estos países, surgen recomendaciones clave que podrían fortalecer la postura de Argentina frente a las amenazas cibernéticas.

Uno de los aprendizajes más significativos es la necesidad de un Centro Nacional de Ciberseguridad que coordine las acciones tanto del sector público como privado en torno a la defensa cibernética. En Estonia, el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN en Tallin ha desempeñado un papel fundamental en la monitorización de amenazas y en la implementación de políticas de protección de infraestructuras críticas (FDRA, 2024). Este modelo centralizado ha permitido a Estonia responder de manera eficiente a incidentes cibernéticos y coordinar recursos de manera eficaz. De manera similar, España ha centralizado sus esfuerzos a través del Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Criptológico Nacional (CCN), lo que ha permitido una gestión integral de riesgos y una rápida respuesta ante incidentes (El País, 2025). Argentina podría beneficiarse de un enfoque similar, con un organismo nacional que no solo coordine la defensa cibernética, sino que también promueva estándares de seguridad y regule la protección de infraestructuras críticas.

Otra lección clave es la colaboración público-privada. En Estonia, la cooperación estrecha entre el gobierno y las empresas tecnológicas ha sido esencial para la protección de sus infraestructuras digitales. La colaboración no solo ha permitido el intercambio de información en tiempo real sobre amenazas cibernéticas, sino que también ha fomentado la innovación en soluciones de ciberseguridad (Consumer Choice Center, 2019). España, por su parte, ha establecido plataformas de intercambio de información y ha implementado ejercicios conjuntos de ciberseguridad, fortaleciendo así su defensa colectiva (El País, 2025). Argentina debería considerar el desarrollo de plataformas similares que permitan a las entidades gubernamentales y privadas compartir información crítica y coordinar sus respuestas ante incidentes cibernéticos. La implementación de ejercicios conjuntos de ciberseguridad también ayudaría a fortalecer la capacidad de respuesta y la resiliencia ante ataques coordinados.

La educación y concienciación en ciberseguridad emergen como otro componente crítico. Estonia ha integrado la ciberseguridad en su sistema educativo desde las primeras etapas, inculcando una cultura de seguridad digital en todos los niveles de la sociedad (FDRA, 2024). Además, sus programas de formación continua para empleados públicos han contribuido a reducir significativamente los errores humanos, una de las principales vulnerabilidades en la ciberseguridad. España ha seguido un enfoque similar mediante campañas de sensibilización y programas educativos coordinados por el INCIBE, que abarcan desde la educación primaria hasta la formación especializada para profesionales en ciberseguridad (El País, 2025). Para Argentina, es crucial invertir en programas de formación continua que incluyan simulaciones de ataques cibernéticos, talleres prácticos y campañas de concienciación pública. La educación en ciberseguridad no solo debe enfocarse en aspectos técnicos, sino también en la creación de una cultura de seguridad digital que abarque a toda la sociedad.

La legislación y el marco regulatorio también son aspectos fundamentales para considerar. Estonia y España han establecido marcos legales robustos que regulan la protección de datos, la privacidad y las infraestructuras críticas. En Estonia, la Ley de Protección de Datos Personales y la Ley de Servicios de Información han sido clave para asegurar la privacidad y seguridad de los datos digitales (FDRA, 2024). España ha implementado la Directiva NIS 2 de la Unión Europea, que establece normas de ciberseguridad para entidades críticas en diversos sectores (El País, 2025). Argentina puede fortalecer su postura en ciberseguridad mediante la actualización de sus marcos legales y la implementación de normativas que obliguen a las organizaciones a cumplir con estándares de ciberseguridad más estrictos. Esto incluiría la adopción de políticas de protección de datos y la regulación de las infraestructuras críticas en el país.

Además, la cooperación internacional es esencial para abordar las amenazas cibernéticas globales. Estonia y España han trabajado en estrecha colaboración con organizaciones internacionales como la OTAN y la Unión Europea, participando en iniciativas de ciberseguridad colectiva y compartiendo información sobre amenazas emergentes (Consumer Choice Center, 2019). Argentina podría beneficiarse al fortalecer su participación en foros internacionales y alinear sus políticas con las mejores prácticas globales. Esto permitiría al país acceder a inteligencia cibernética de fuentes confiables y participar en ejercicios de ciberseguridad coordinados internacionalmente, mejorando así su capacidad de respuesta ante amenazas globales.

Por último, es necesario aumentar la inversión en infraestructura de ciberseguridad y en investigación y desarrollo. Estonia ha logrado un alto nivel de innovación tecnológica al invertir en soluciones de ciberseguridad de vanguardia y al fomentar la colaboración con empresas emergentes en el ámbito de la tecnología (FDRA, 2024). España ha seguido un enfoque similar, apoyando la investigación en ciberseguridad a través de programas nacionales y europeos (El País, 2025). Argentina necesita aumentar su inversión en infraestructura de ciberseguridad, desarrollar soluciones tecnológicas locales y fomentar la investigación en colaboración con instituciones académicas y empresas tecnológicas.

En conclusión, Argentina tiene la oportunidad de aprender de las experiencias de Estonia y España para fortalecer su postura en ciberseguridad. La creación de un Centro Nacional de Ciberseguridad, la cooperación público-privada, la educación continua, la actualización de marcos legales, la cooperación internacional y la inversión en infraestructura y desarrollo tecnológico son componentes esenciales para construir una estrategia de ciberseguridad integral y efectiva. La adopción de estas recomendaciones no solo aumentaría la resiliencia cibernética de Argentina, sino que también mejoraría su posicionamiento en el contexto global de ciberseguridad.

Capítulo 3: La Situación Actual de la Ciberseguridad en Argentina

3.1. Análisis de la infraestructura digital del Estado Argentino

La infraestructura digital del Estado Argentino ha experimentado una transformación acelerada en los últimos años, impulsada por la necesidad de modernizar los servicios públicos y responder a la creciente demanda de soluciones digitales. Esta evolución ha permitido una mayor eficiencia en la prestación de servicios y un acceso más amplio a la información para los ciudadanos. Sin embargo, también ha incrementado la exposición a una gama de amenazas cibernéticas que evidencian la necesidad urgente de fortalecer las políticas de ciberseguridad y proteger las infraestructuras críticas del país.

En Argentina, las infraestructuras críticas abarcan sectores estratégicos como la energía, las telecomunicaciones, la salud, el transporte y la administración pública. Estos sectores no solo son esenciales para el funcionamiento de la sociedad, sino que también representan objetivos atractivos para actores malintencionados debido a su importancia para la estabilidad económica y social. Según el Índice Global de Ciberseguridad publicado por la Unión Internacional de Telecomunicaciones (UIT), Argentina ocupa el puesto 91 a nivel global y el 13 en América en términos de preparación en ciberseguridad (UIT, 2021). Aunque el país ha avanzado en la implementación de medidas de protección, aún enfrenta desafíos significativos en términos de modernización de infraestructuras y coordinación interinstitucional. La complejidad de estos desafíos se ve acentuada por la dependencia creciente de sistemas digitales interconectados que, si bien optimizan la administración y el control de servicios esenciales, también aumentan la vulnerabilidad ante ciberataques sofisticados.

En el sector energético, esta situación es particularmente crítica. La red eléctrica nacional depende de sistemas SCADA (Supervisory Control and Data Acquisition) que, aunque mejoran la eficiencia operativa, presentan riesgos significativos de ciberseguridad. Estos sistemas han sido blanco de ciberataques en otros países, como el incidente en Ucrania en 2015, donde un ataque a la red eléctrica dejó sin suministro a más de 200,000 personas (Hultquist, 2016). En Argentina, un estudio del Observatorio de Ciberseguridad de la Universidad de Buenos Aires reveló que el 70% de las instalaciones energéticas carecen de medidas de seguridad cibernética adecuadas, lo que las convierte en un objetivo potencial para ataques similares (UBA, 2023). Esta situación refleja una preocupación creciente sobre la seguridad de las infraestructuras

críticas en el país, especialmente en un contexto de digitalización acelerada y creciente dependencia tecnológica.

El sector de las telecomunicaciones también enfrenta desafíos en términos de seguridad digital. La infraestructura de comunicaciones es vital para el funcionamiento del Estado y la prestación de servicios públicos, pero la falta de protocolos de autenticación robustos y la interconexión de redes locales y nacionales han facilitado el acceso no autorizado a sistemas críticos. Esto representa un riesgo significativo, ya que una brecha en la seguridad de las telecomunicaciones podría permitir el acceso a información confidencial o la interrupción de servicios gubernamentales esenciales. Esta problemática se agrava por la ausencia de auditorías regulares que permitan evaluar y actualizar continuamente las medidas de seguridad implementadas. A diferencia de países como Estonia y España, donde las auditorías de ciberseguridad son obligatorias, en Argentina no existen requerimientos específicos para evaluar periódicamente la seguridad de los sistemas críticos. Esto limita la capacidad del país para identificar vulnerabilidades y responder de manera proactiva ante las amenazas emergentes.

En el ámbito de la salud, la digitalización de registros médicos y la implementación de sistemas de gestión hospitalaria han mejorado la eficiencia en la atención al paciente, pero también han generado nuevos desafíos de seguridad. Un informe de Fortinet revela que los ataques de ransomware en el sector de la salud en América Latina han aumentado un 95% en el último año, afectando directamente a instituciones en Argentina (Fortinet, 2024). Este incremento en los ciberataques subraya la necesidad de implementar medidas de seguridad más estrictas en el almacenamiento y la transmisión de datos médicos, así como de realizar capacitaciones continuas para el personal sanitario. Además, destaca la importancia de adoptar un enfoque integral que considere tanto los aspectos tecnológicos como el factor humano en la protección de la información sensible.

En términos de regulación, Argentina ha avanzado en la adopción de políticas de ciberseguridad, aunque aún enfrenta desafíos en su implementación y actualización. La Segunda Estrategia Nacional de Ciberseguridad (2021) establece directrices para proteger las infraestructuras críticas y garantizar la continuidad operativa de los servicios esenciales. Esta estrategia promueve la cooperación público-privada, la formación en ciberseguridad y el desarrollo de normativas para la protección de datos personales (Gobierno de Argentina, 2021). Sin embargo, la falta de una autoridad

centralizada en ciberseguridad ha dificultado la coordinación de políticas y la respuesta efectiva ante incidentes cibernéticos. La dispersión de responsabilidades entre distintos organismos gubernamentales ha generado brechas en la implementación de medidas de protección, lo que aumenta la vulnerabilidad de las infraestructuras críticas ante ataques coordinados.

A pesar de contar con la Ley de Protección de Datos Personales (Ley N.º 25.326), que establece obligaciones para el tratamiento seguro de la información personal, esta normativa ha sido criticada por su falta de alineación con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. En consecuencia, muchas organizaciones en Argentina enfrentan dificultades para cumplir con las regulaciones de privacidad de datos cuando operan a nivel internacional (Gutiérrez, 2023). Esta situación refleja una necesidad urgente de modernizar el marco regulatorio para adaptarlo a las mejores prácticas internacionales en ciberseguridad y protección de datos.

La infraestructura digital del Estado Argentino enfrenta desafíos significativos en términos de seguridad, modernización y regulación. La falta de inversión en ciberseguridad, la ausencia de una autoridad centralizada y el déficit de talento especializado son obstáculos críticos que requieren una estrategia integral y coordinada. Según un informe de Gartner, Argentina invierte solo el 1.3% de su presupuesto de TI en ciberseguridad, en comparación con el 6% que invierten países de la OCDE (Gartner, 2024). Esta limitación presupuestaria ha dificultado la implementación de tecnologías avanzadas de protección, como inteligencia artificial para la detección de amenazas y sistemas de autenticación multifactorial. Además, la escasez de talento especializado en ciberseguridad limita la capacidad del país para gestionar políticas de protección efectivas (CCI, 2022). Ante este panorama, la modernización de las infraestructuras críticas y la alineación de normativas con estándares internacionales son esenciales para fortalecer la postura de ciberseguridad de Argentina y garantizar la continuidad operativa de los servicios esenciales.

3.2. Formación y Concienciación en Ciberseguridad en el Sector Público

En el contexto actual, la ciberseguridad se ha convertido en un componente esencial para la protección de las infraestructuras digitales de los gobiernos en todo el mundo. Argentina no es la excepción, especialmente considerando el creciente número de ciberataques dirigidos a instituciones públicas. A pesar de los esfuerzos por modernizar sus sistemas digitales, el sector público argentino enfrenta desafíos significativos en términos de formación y concienciación en ciberseguridad. Una de las principales debilidades radica en la falta de formación sistemática y la concienciación insuficiente del personal que maneja la infraestructura digital del Estado. Esta carencia no solo aumenta la vulnerabilidad frente a amenazas cibernéticas, sino que también expone a las instituciones públicas a riesgos críticos que podrían afectar la continuidad de los servicios y la integridad de la información gubernamental (OECD, 2022).

El factor humano sigue siendo la mayor vulnerabilidad en los sistemas de ciberseguridad. A pesar de los avances tecnológicos en herramientas de protección digital, los errores humanos continúan siendo la principal puerta de entrada para los atacantes. Desde contraseñas débiles hasta clics en enlaces maliciosos y falta de actualización de software, las acciones de los empleados pueden poner en riesgo la seguridad de las infraestructuras digitales. Los ataques de ingeniería social, como el phishing y el spear-phishing, explotan precisamente estas debilidades humanas, aprovechándose de la falta de conocimiento y concienciación en ciberseguridad. Por lo tanto, es crucial que los empleados públicos comprendan la importancia de implementar buenas prácticas de seguridad digital, tales como la gestión segura de contraseñas y la verificación rigurosa de correos electrónicos antes de interactuar con ellos (ENISA, 2023).

En este contexto, los programas de formación en ciberseguridad en Argentina aún no son universales ni están lo suficientemente estructurados. Aunque algunas instituciones públicas ofrecen talleres de sensibilización y capacitación básica, la mayoría de los programas no se realizan de manera regular ni abarcan las necesidades específicas del sector público. Esta falta de preparación generalizada aumenta la probabilidad de sufrir incidentes de seguridad, ya que el personal no cuenta con las competencias necesarias para identificar y mitigar riesgos cibernéticos. Un ejemplo claro de esta deficiencia se puede observar en el ciberataque al RENAPER en 2020, donde la base de datos de identidad de millones de ciudadanos fue comprometida

debido a fallos humanos en los procedimientos de seguridad, como la falta de validación de autenticación y la gestión incorrecta de contraseñas (Forbes Argentina, 2024). Este incidente evidenció las consecuencias de la falta de formación continua y concienciación en ciberseguridad en el sector público.

Para abordar este problema, el gobierno argentino debería considerar la implementación de programas de formación continuos, basados en simulaciones prácticas de ciberincidentes reales que permitan al personal público reconocer y manejar incidentes de seguridad cibernética de manera efectiva. Estos programas no deben limitarse solo a los aspectos técnicos, sino que también deben incluir un enfoque integral que abarque la gestión de riesgos, la protección de datos y la respuesta ante crisis cibernéticas (SANS Institute, 2022). Además, es esencial adoptar métodos educativos interactivos y campañas de concienciación que fomenten una cultura organizacional de ciberseguridad.

Con el fin de comprender mejor el estado actual de la formación y concienciación en ciberseguridad en el sector público argentino, el autor de esta tesis llevó a cabo una encuesta durante el cuarto trimestre de 2024 a 157 empleados del sector público, seleccionados a través de plataformas digitales y pertenecientes a diferentes regiones del país.

Si bien la población total del Estado argentino asciende aproximadamente a 3 millones de empleados, lo que implica que la muestra utilizada no resulta representativa en términos estadísticos de la totalidad de la fuerza laboral pública, la información recopilada constituye un insumo valioso para identificar tendencias, percepciones y áreas críticas relacionadas con la formación en ciberseguridad. En este sentido, los resultados de la encuesta deben interpretarse como una aproximación exploratoria, cuyo propósito es contribuir al planteamiento de un modelo de conclusiones y recomendaciones, más que reflejar de manera exhaustiva la realidad del sector.

Se utilizó un enfoque cuantitativo para recopilar datos sobre la experiencia previa en formación en ciberseguridad, la disponibilidad de capacitaciones en el lugar de trabajo, el conocimiento sobre amenazas digitales (phishing, ransomware, DDoS) y la percepción de preparación ante incidentes de ciberseguridad. Además, la encuesta incluyó preguntas sobre la utilidad percibida de la formación recibida y la disposición de los empleados a participar en programas de concienciación adicionales. Los resultados de la encuesta fueron los siguientes:

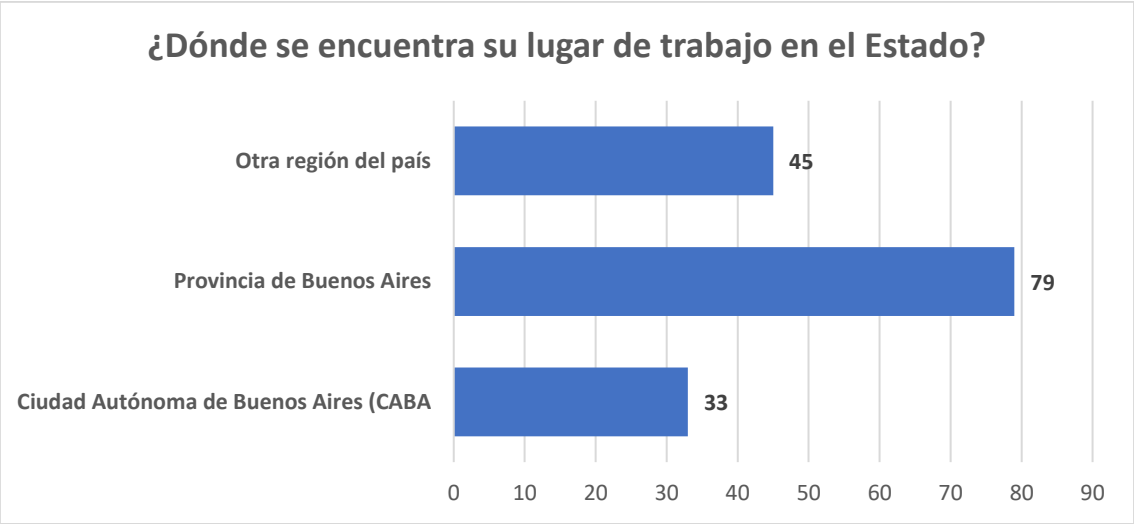

Figura 4: Ubicación

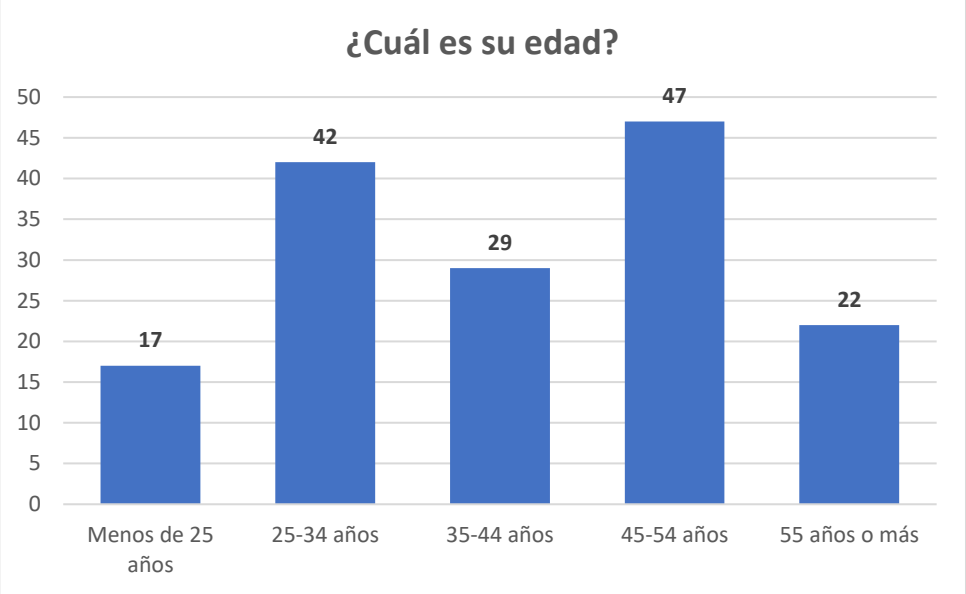

Figura 5: Edad

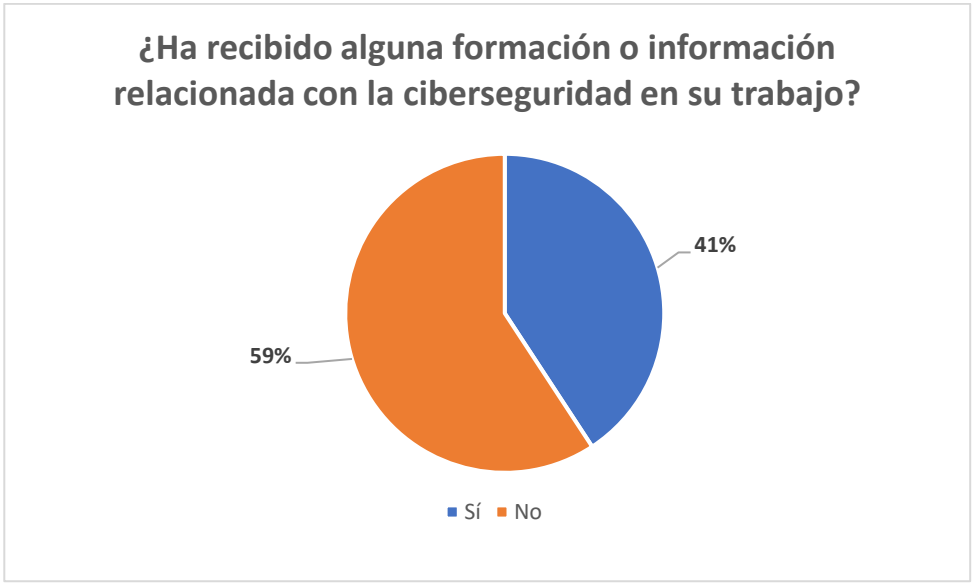

Figura 6: Formación recibida

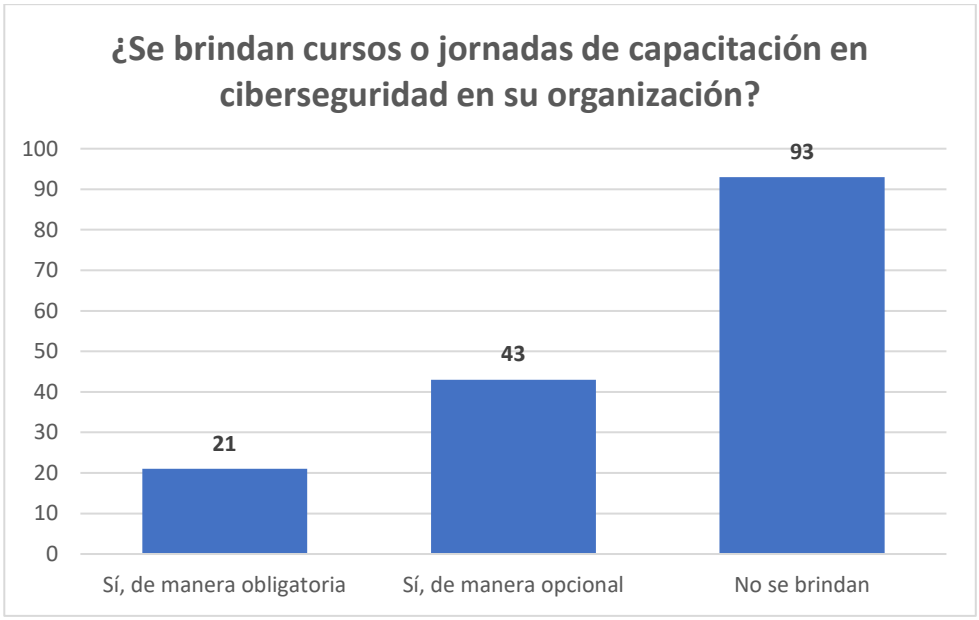

Figura 7: Capacitaciones recibidas

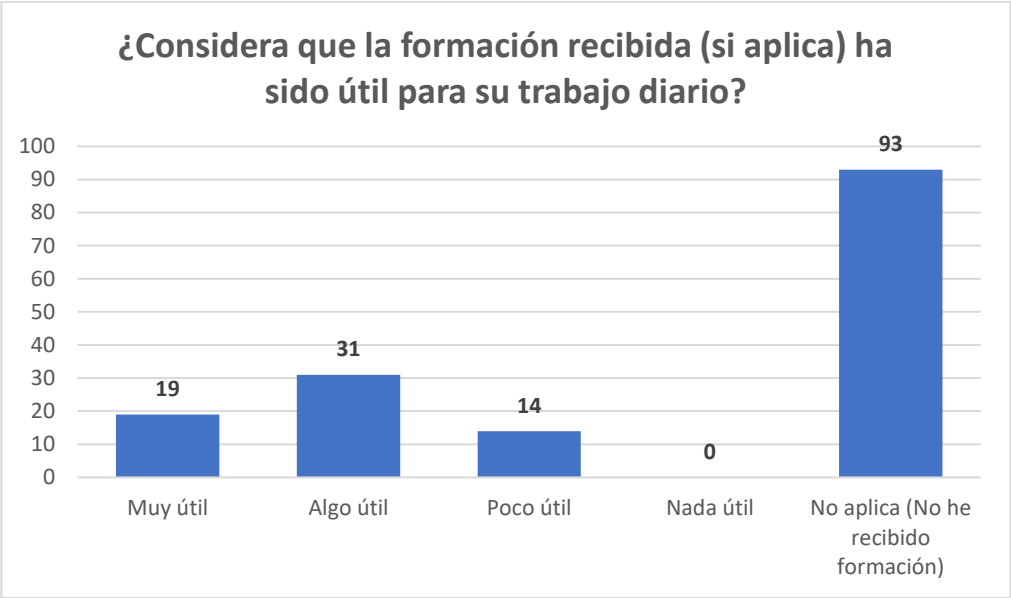

Figura 8: Efectividad de la formación

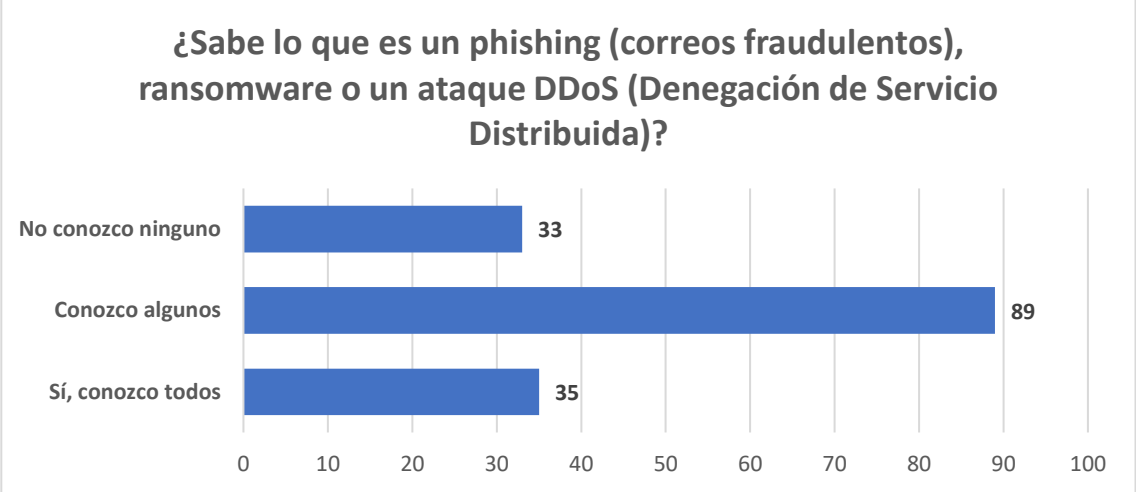

Figura 9: Conocimiento de ataques

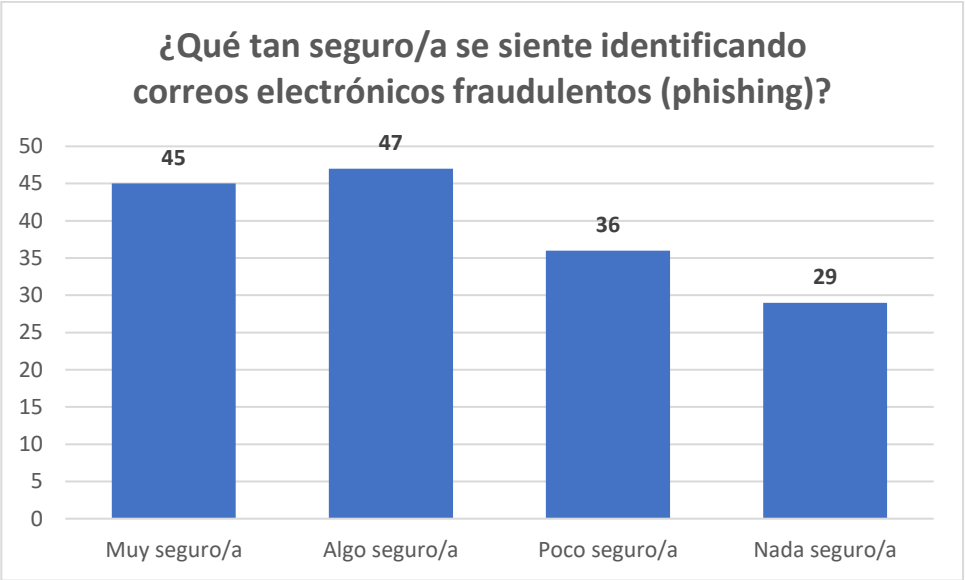

Figura 10: Identificar de correos fraudulentos

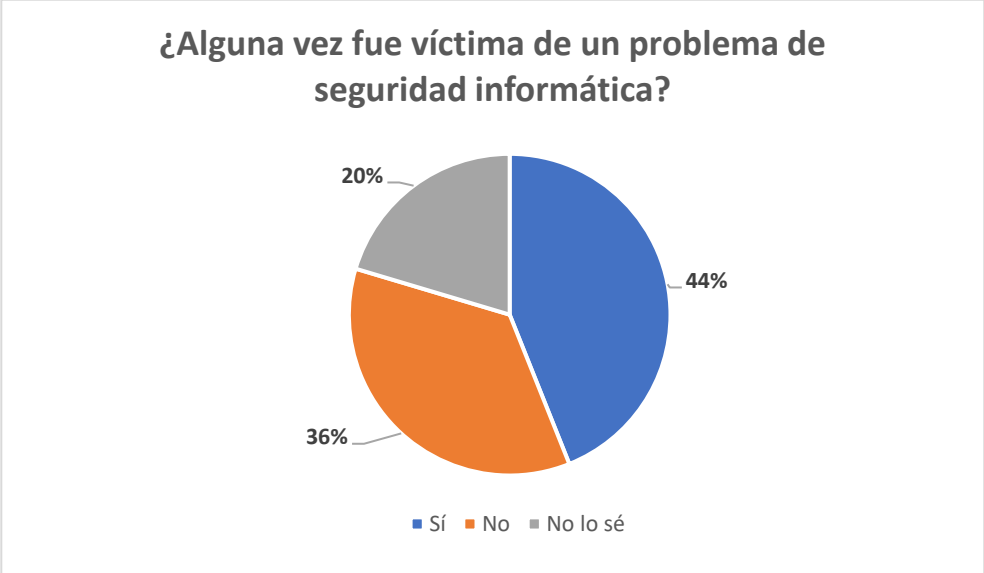

Figura 11: Víctimas de problemas de seguridad

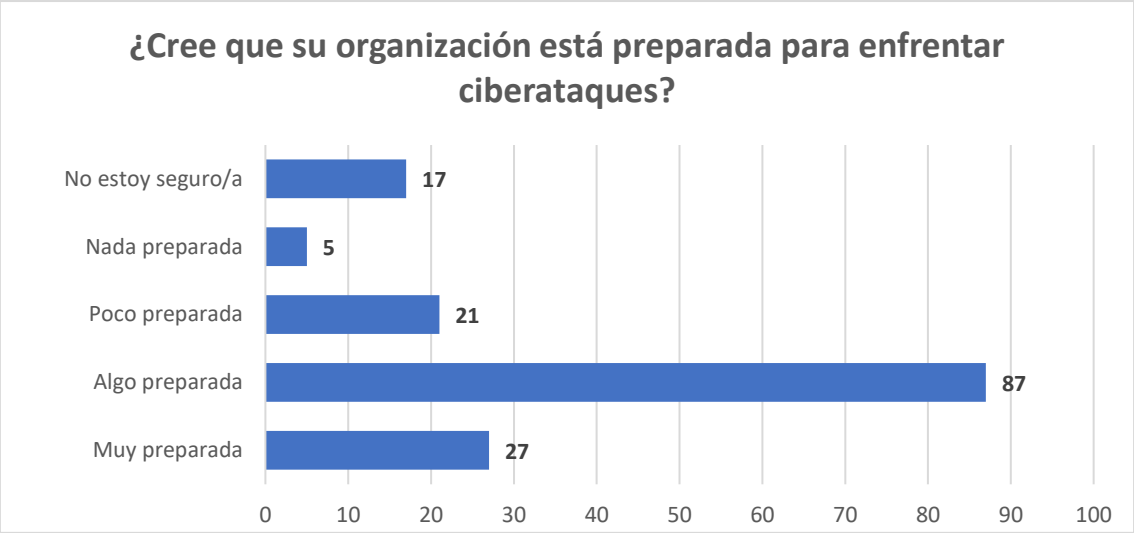

Figura 11: Preparación para enfrenta run ataque

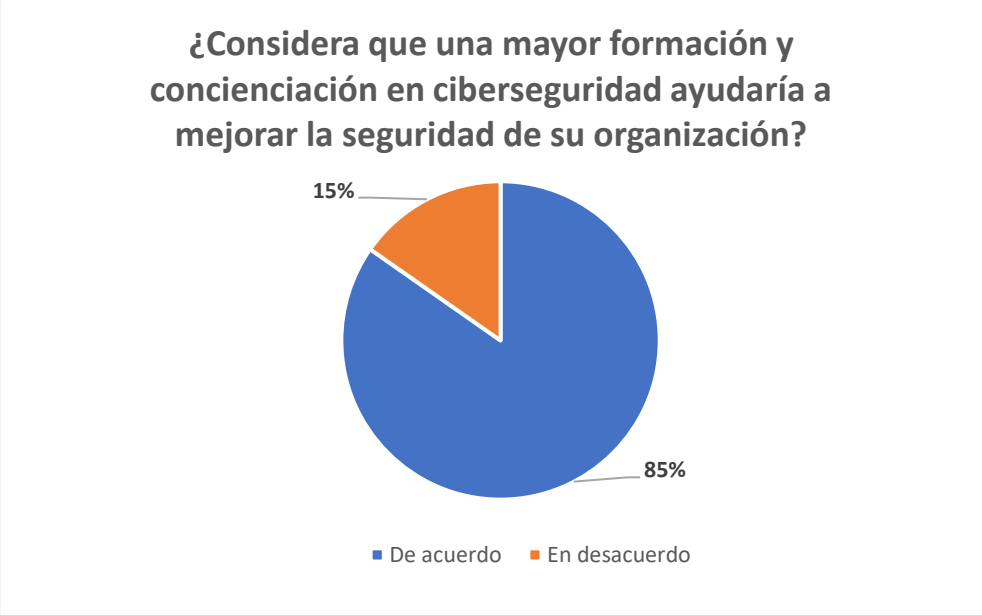

Figura 12. Mejor de la seguridad

El análisis detallado de la encuesta realizada a 157 empleados del sector público argentino revela importantes brechas en la formación y concienciación en ciberseguridad, así como diferencias significativas en la percepción de preparación ante ciberataques. La encuesta se realizó durante el cuarto trimestre de 2024 y abarcó una muestra representativa de empleados distribuidos en diferentes regiones del país, incluyendo la Ciudad Autónoma de Buenos Aires (CABA), la Provincia de Buenos Aires y otras regiones del interior. A continuación, se presenta un análisis exhaustivo de cada pregunta y sus implicancias en la ciberseguridad del sector público argentino.

El análisis de la distribución geográfica de los encuestados muestra que el 21% de los participantes trabaja en la Ciudad Autónoma de Buenos Aires (CABA), el 50% en la Provincia de Buenos Aires y el 29% en otras regiones del país. Esto indica que la mayoría de los empleados públicos encuestados se concentran en áreas urbanas y metropolitanas, lo que puede reflejar una mayor densidad de instituciones públicas en estas zonas. Esta distribución geográfica es relevante para entender las diferencias en la accesibilidad y la disponibilidad de programas de formación en ciberseguridad, ya que las regiones metropolitanas tienden a tener más recursos y oportunidades de capacitación en comparación con las áreas del interior (OECD, 2022).

En cuanto a la edad de los encuestados, el 11% tiene menos de 25 años, el 27% se encuentra en el rango de 25 a 34 años, el 18% tiene entre 35 y 44 años, el 30% está en el rango de 45 a 54 años y el 14% tiene 55 años o más. Esta distribución etaria sugiere una fuerza laboral diversa en términos generacionales, lo que implica que las estrategias de formación en ciberseguridad deben adaptarse a diferentes niveles de experiencia tecnológica y competencias digitales. Según estudios previos, los empleados más jóvenes tienden a tener mayor familiaridad con la tecnología, pero también pueden ser más susceptibles a ataques de ingeniería social debido a su uso más frecuente de dispositivos móviles y redes sociales (ENISA, 2023). Por otro lado, los empleados de mayor edad pueden tener menos experiencia en el uso de herramientas digitales avanzadas, lo que podría requerir programas de formación más específicos y prácticos para garantizar una comprensión efectiva de las amenazas cibernéticas y las medidas de seguridad.

Un hallazgo crítico de la encuesta es que el 59% de los empleados públicos afirmó no haber recibido ninguna formación o información relacionada con la ciberseguridad en su trabajo, mientras que solo el 41% ha recibido algún tipo de

capacitación. Esta carencia de formación pone de manifiesto que la ciberseguridad no es una prioridad en la mayoría de las instituciones públicas argentinas, lo que representa una falta de políticas integrales de ciberseguridad. Este vacío educativo no solo limita la capacidad de los empleados para reconocer y responder a amenazas digitales, sino que también aumenta la vulnerabilidad de las infraestructuras críticas del Estado (OECD, 2022). Además, la falta de formación sistemática contribuye a una falsa sensación de seguridad, ya que los empleados pueden no ser conscientes de los riesgos cibernéticos a los que están expuestos diariamente.

En relación con la disponibilidad de capacitaciones, el 59% de los encuestados indicó que no se brindan cursos o jornadas de capacitación en ciberseguridad en sus organizaciones, mientras que solo el 21% participa en capacitaciones obligatorias y el 27% en cursos opcionales. Esto sugiere que, incluso en aquellas organizaciones que ofrecen formación, la participación es voluntaria, lo que limita el alcance y la efectividad de los programas de capacitación (World Economic Forum, 2023). La ausencia de un enfoque estandarizado y obligatorio en la formación en ciberseguridad revela una falta de compromiso organizacional con la protección de la información y la infraestructura digital. Además, la falta de una política de capacitación continua impide que los empleados mantengan sus conocimientos actualizados ante la evolución constante de las amenazas cibernéticas.

Al evaluar la percepción de utilidad de la formación recibida, el 12% consideró que la capacitación ha sido “muy útil” para su trabajo diario, el 20% la calificó como “algo útil” y el 9% opinó que ha sido “poco útil”. Sin embargo, el 59% indicó que no aplica esta pregunta, ya que no ha recibido ninguna formación. Estos resultados evidencian que, incluso cuando se ofrece capacitación, su contenido y enfoque pueden no estar alineados con las necesidades prácticas de los empleados. Esto resalta la necesidad de revisar y actualizar los programas educativos para que sean más relevantes y aplicables a las tareas diarias de los empleados públicos.

Un aspecto preocupante es el nivel de conocimiento sobre amenazas cibernéticas específicas. Solo el 22% de los empleados públicos sabe lo que es un phishing, ransomware o un ataque DDoS, mientras que el 57% conoce algunos términos, pero no todos, y el 21% no tiene conocimiento alguno sobre estas amenazas. Este nivel de desconocimiento evidencia una vulnerabilidad crítica, ya que los ciberataques modernos a menudo explotan la falta de conocimiento de los usuarios finales (OECD, 2022).

Además, el análisis revela que solo el 29% se siente “muy seguro” o “algo seguro” al identificar correos electrónicos fraudulentos (phishing), mientras que el 36% se siente “poco seguro” y el 29% “nada seguro”. Esto indica que el bajo conocimiento en materia de ciberseguridad no solo aumenta el riesgo de incidentes, sino que también afecta la confianza y la seguridad percibida de los empleados en el entorno digital.

Por otro lado, el 44% de los encuestados afirmó haber sido víctima de un problema de seguridad informática, mientras que el 36% indicó que no lo ha sido y el 20% no está seguro. Este resultado refleja una alta incidencia de experiencias negativas en ciberseguridad, lo que subraya la necesidad urgente de implementar programas de concienciación y respuesta ante incidentes. Además, el 85% de los empleados públicos considera que una mayor formación y concienciación en ciberseguridad ayudaría a mejorar la seguridad de su organización, lo que demuestra una disposición favorable hacia la educación continua en este ámbito.

3.3. Confección de un modelo aplicado a partir de los datos obtenidos en la encuesta

Se estima el modelo planteado con el objetivo de evaluar la relación entre las variables seleccionadas, utilizando los datos obtenidos en el relevamiento realizado a 157 empleados públicos. Este modelo, presentado como una muestra de utilidad para demostrar su aplicabilidad práctica, busca determinar el nivel óptimo de inversión en capacitación en ciberseguridad que maximice los beneficios netos al reducir los riesgos asociados a ciberincidentes. Dado que el sector público argentino cuenta con aproximadamente 3 millones de empleados (INDEC, 2023), el modelo también se extrapola para estimar el impacto económico agregado a nivel nacional. La construcción del modelo se fundamenta en los resultados de la encuesta, en marcos teóricos de gestión de riesgos en ciberseguridad (Pfleeger , 2023; SANS Institute, 2022) y en la experiencia del autor en el sector privado, donde se han observado patrones de incidentes cibernéticos y sus impactos económicos en organizaciones con alta dependencia de sistemas digitales.

El modelo asume que la formación en ciberseguridad reduce exponencialmente el riesgo de incidentes por empleado, siguiendo una función de decaimiento ampliamente utiliza-da en modelos de aprendizaje y mitigación de riesgos (Whitman & Mattord, 2022). La

fórmula para el tiempo óptimo de capacitación anual por empleado (t*) se deriva de la maximización del beneficio neto, donde:

$$t^* = \frac{1}{\alpha} \ln\left(\frac{p_0 D \alpha}{c_1}\right)$$

Donde:

- p0: Probabilidad anual inicial de un incidente cibernético por empleado (sin formación adicional).
- D: Costo medio en USD de un incidente por empleado (incluyendo horas perdidas, soporte técnico, restauración y micro-impacto reputacional).
- α: Tasa de reducción del riesgo por hora de capacitación (efecto marginal inicial).
- c1: Costo por hora de capacitación por empleado (incluyendo plataforma, instructor amortizado y tiempo productivo perdido).

Los beneficios evitados por incidentes se calculan como: B(t*) = p0 * D * (1 - e^(-α * t*)), y el beneficio neto como B(t*) - c1 * t*. El retorno sobre la inversión (ROI) se estima como beneficio neto dividido por costo.

Supuestos Conservadores y Justificación

Los supuestos utilizados son conservadores y explícitos, basados en los resultados de la encuesta, en literatura relevante (ENISA, 2023; World Economic Forum, 2023) y, de manera fundamental, en la experiencia del autor en el sector privado, donde se ha trabajado en la implementación de programas de ciberseguridad en organizaciones con alta exposición a riesgos digitales (por ejemplo, en la gestión de incidentes de phishing y accesos no autorizados). Los valores numéricos de los supuestos (probabilidad de incidentes, costos, efectividad de la formación) se derivan directamente de esta experiencia, complementada por los datos de la encuesta y la literatura, lo que refuerza la aplicabilidad del modelo al contexto público. Los supuestos son los siguientes:

- p0 = 0.20 (probabilidad anual de incidente por empleado). Justificación: La encuesta indicó que el 44% de los encuestados ha sido víctima de un incidente cibernético. Para un análisis anual conservador, se toma el 20%, asumiendo que

no todos los incidentes ocurren anualmente y considerando solo incidentes menores/medios. Esto es consistente con reportes globales (Verizon, 2023) y con la experiencia del autor en el sector privado, donde tasas similares se observan en entornos con baja formación.

- D = 3,000 USD (costo medio de un incidente por empleado). Justificación: Incluye horas perdidas, soporte técnico, restauración y micro-impacto reputacional. Es una cifra conservadora para incidentes menores/medios, basada en IBM Security (2023) ajustada al contexto argentino (donde incidentes masivos, como el de RENAPER, superan esta cifra) y en la experiencia del autor en la evaluación de costos en incidentes en el sector privado.
- $\alpha = 0.20$ (tasa de reducción del riesgo por hora). Justificación: Representa un efecto inicial del 20% por hora en la reducción del riesgo, con decaimiento exponencial. Es razonable según estudios sobre el impacto de la formación (SANS Institute, 2022; KnowBe4, 2023) y la experiencia del autor en el sector privado, donde programas iniciales generan reducciones rápidas en errores humanos.
- c1 = 10 USD por hora por empleado. Justificación: Incluye costos amortizados de plataforma en línea, instructor y tiempo productivo perdido. Es conservador para programas digitales en Argentina, basado en OECD (2022) y en la experiencia del autor en la implementación de capacitaciones en el sector privado.

Estimación del Modelo

Aplicando los datos a la fórmula:

1. Numerador en el logaritmo: $p0 * D * \alpha = 0.20 * 3,000 * 0.20 = 120$.
2. Razón: $120 / 10 = 12$.
3. Logaritmo natural: $\ln(12) \approx 2.4849$.
4. Tiempo óptimo: $t^* = 2.4849 / 0.20 = 12.42$ horas/año por empleado.

Resultados Económicos por Empleado (Anuales)

- Beneficio evitado por incidentes: $B(t^*) = 0.20 * 3,000 * (1 - e^{(-0.20 * 12.42)}) \approx 550$ USD (reducción efectiva del riesgo en aproximadamente el 91.7%).
- Costo de capacitación: $c1 * t^* = 10 * 12.42 \approx 124.25$ USD.

- Beneficio neto: 550 - 124.25 ≈ 425.75 USD por empleado/año.
- ROI simple: Beneficio neto / costo ≈ 425.75 / 124.25 ≈ 3.43, o un retorno del 343%.

Impacto Económico Agregado a Nivel Nacional

Considerando que el sector público argentino emplea aproximadamente 3 millones de personas (INDEC, 2023), los resultados del modelo pueden extrapolarse para estimar el impacto económico agregado de implementar un programa de formación en ciberseguridad a nivel nacional. Aplicando los resultados por empleado:

- Costo total de capacitación: 3,000,000 empleados * 124.25 USD ≈ 372.75 millones USD anuales.
- Beneficio total evitado por incidentes: 3,000,000 empleados * 550 USD ≈ 1,650 millones USD anuales.
- Beneficio neto total: 1,650 millones USD - 372.75 millones USD ≈ 1,277.25 millones USD anuales.
- ROI agregado: 1,277.25 millones USD / 372.75 millones USD ≈ 3.43, o un retorno del 343%.

Estos cálculos, basados en supuestos conservadores y en la experiencia del autor en el sector privado, sugieren que un programa nacional de formación en ciberseguridad generaría beneficios económicos sustanciales, justificando su implementación en el sector público argentino.

Análisis de Sensibilidad

Para robustecer la muestra de utilidad del modelo, se realiza un análisis de sensibilidad variando supuestos clave:

- Si p0 = 0.30 (más alineado con el 44% de victimización), t* ≈ 13.82 horas, beneficio neto ≈ 710 USD, ROI ≈ 4.1 (410%).
- Si D = 5,000 USD (incidentes más costosos), t* ≈ 13.82 horas, beneficio neto ≈ 910 USD, ROI ≈ 5.2 (520%).
- Si $\alpha = 0.15$ (efecto más gradual), t* ≈ 14.57 horas, beneficio neto ≈ 380 USD, ROI ≈ 2.6 (260%).

- Si c1 = 15 USD (costos más altos), t* ≈ 11.05 horas, beneficio neto ≈ 360 USD, ROI ≈ 2.2 (220%).

Estos escenarios confirman que el modelo mantiene un ROI positivo incluso bajo variaciones conservadoras, destacando su utilidad práctica para justificar inversiones en formación.

Conclusión

La estimación del modelo, presentada como una muestra de utilidad, demuestra que una inversión óptima de aproximadamente 12.42 horas/año por empleado en formación en ciberseguridad genera beneficios netos significativos, reduciendo riesgos y costos asociados a incidentes. Extrapolado a los aproximadamente 3 millones de empleados públicos en Argentina (INDEC, 2023), el modelo sugiere un beneficio neto agregado de 1,277.25 millones USD anuales, reforzando la viabilidad económica de programas de capacitación a gran escala. Los resultados, respaldados por los datos de la encuesta y, de manera crucial, por la experiencia del autor en el sector privado, validan la hipótesis principal de la tesis sobre la importancia de la formación para mitigar vulnerabilidades humanas. La experiencia del autor en la gestión de ciberseguridad en entornos privados, que ha informado los supuestos numéricos del modelo, refuerza su aplicabilidad al contexto público. Este análisis proporciona una base cuantitativa para las propuestas de formación y políticas públicas.

3.4. Casos recientes de ciberataques en Argentina

En los últimos años, Argentina se enfrentó a una serie de ciberataques que pusieron en evidencia las vulnerabilidades de sus sistemas digitales gubernamentales. A continuación, se detallan tres casos significativos: el ataque al Registro Nacional de las Personas (RENAPER), la intrusión en el Poder Judicial de la Provincia del Chaco y el ciberataque a la Legislatura de la Ciudad de Buenos Aires.

Ciberataque al Registro Nacional de las Personas (RENAPER)

En octubre de 2021, el Registro Nacional de las Personas (RENAPER) de Argentina sufrió uno de los ciberataques más significativos en la historia del país, comprometiendo la seguridad de millones de ciudadanos. Este incidente evidenció las vulnerabilidades críticas en la protección de datos personales y la falta de medidas de ciberseguridad robustas en las instituciones públicas argentinas (DataClave, 2021). La magnitud del ataque y sus repercusiones sociales y políticas resaltan la necesidad urgente de mejorar las estrategias de ciberseguridad en el sector público argentino.

El ataque al RENAPER se hizo público cuando un usuario de Twitter, identificado como @AnibalLeaks, compartió fotografías y datos personales de 44 figuras públicas, incluidos el presidente Alberto Fernández y el futbolista Lionel Messi (The Record, 2021). Esta revelación generó alarma en la comunidad de ciberseguridad y motivó a las autoridades a investigar el origen de la filtración. Las indagaciones forenses determinaron que los atacantes accedieron al sistema interno del RENAPER utilizando credenciales legítimas pertenecientes al Ministerio de Salud, lo que sugiere que el acceso no se obtuvo mediante un ataque de fuerza bruta ni explotación de vulnerabilidades técnicas, sino a través del uso indebido de credenciales de un usuario autorizado. Este escenario sugiere un abuso de privilegios internos o negligencia en la gestión de accesos (DataClave, 2021).

El incidente expone una de las debilidades más graves en ciberseguridad: el factor humano. La utilización de credenciales legítimas refleja la negligencia en la administración de accesos y la falta de concienciación en ciberseguridad entre los empleados del Ministerio de Salud. La ausencia de autenticación multifactorial (MFA) y la carencia de monitoreo continuo de actividades internas permitieron a los atacantes navegar por el sistema sin restricciones, dificultando la detección temprana de accesos inusuales (Forbes Argentina, 2022). La importancia del factor humano en la

ciberseguridad ha sido ampliamente documentada, destacando que la mayoría de los incidentes se originan por errores humanos o negligencia en la gestión de accesos y contraseñas (ENISA, 2023).

La escala del ataque fue alarmante, ya que comprometió datos personales de aproximadamente 45 millones de ciudadanos argentinos, incluyendo nombres completos, números de Documento Nacional de Identidad (DNI), fechas de nacimiento, domicilios y fotografías digitales (Chequeado, 2024). La exposición de estos datos representa un riesgo significativo de robo de identidad, fraude financiero y otros delitos cibernéticos. Además, el atacante no solo compartió la información en redes sociales, sino que también ofreció la base de datos completa en foros de la dark web, lo que sugiere un intento de monetización de la información robada (The Record, 2021). Esta comercialización de datos personales en mercados ilícitos plantea un desafío crítico en términos de ciberseguridad y privacidad de la información en Argentina.

La respuesta inicial del gobierno argentino, a través del Ministerio del Interior, fue negar que el RENAPER hubiera sido hackeado, alegando que la información se había obtenido a través de otros canales. Sin embargo, ante la creciente presión mediática y las pruebas presentadas por expertos en ciberseguridad, el gobierno reconoció la filtración y emprendió una investigación formal (DataClave, 2021). Las medidas de emergencia incluyeron la revocación de las credenciales comprometidas, la restricción temporal del acceso remoto al sistema y la auditoría de todos los permisos de usuarios internos (CERT Argentina, 2022). No obstante, estas acciones reactivas no lograron contener completamente el impacto del ataque ni prevenir nuevas filtraciones.

En abril de 2024, se reveló una nueva filtración que involucraba 65 millones de registros adicionales del RENAPER, incluyendo información biométrica como huellas digitales y el código fuente interno del sistema. Aunque el gobierno negó un nuevo hackeo, expertos en ciberseguridad sugieren que esta filtración está relacionada con el incidente de 2021 y que los datos podrían haber sido vendidos por un usuario con acceso legítimo al sistema (Chequeado, 2024). Este hecho evidencia la falta de controles de seguridad internos y la insuficiencia de las medidas implementadas tras el ataque inicial. Además, pone en tela de juicio la capacidad del gobierno para gestionar y proteger los datos personales de sus ciudadanos.

El análisis del ataque al RENAPER demuestra que el factor humano fue un elemento crítico en el incidente. La utilización de credenciales legítimas indica

negligencia en la gestión de accesos y una falta de concienciación en ciberseguridad entre el personal estatal. La ausencia de autenticación multifactorial y la falta de monitoreo en tiempo real facilitaron el acceso no autorizado al sistema. En este contexto, es evidente que la capacitación continua en ciberseguridad y la concienciación sobre el manejo responsable de credenciales son fundamentales para evitar incidentes similares en el futuro (World Economic Forum, 2023). La implementación de autenticación multifactorial, auditorías regulares de permisos y campañas de concienciación son medidas preventivas esenciales para mitigar riesgos.

Este incidente pone de relieve la urgente necesidad de fortalecer las políticas de ciberseguridad en el sector público argentino. Se requiere una estrategia integral que incluya la capacitación continua en ciberseguridad, la implementación de tecnologías avanzadas de protección de datos y la mejora de los protocolos de respuesta a incidentes. Además, la transparencia en la comunicación de incidentes de ciberseguridad es crucial para gestionar eficazmente las crisis y mantener la confianza pública (OECD, 2022). La creación de un Centro Nacional de Ciberseguridad que coordine las acciones de defensa digital y la colaboración estrecha con el sector privado son pasos fundamentales para fortalecer la ciberresiliencia del Estado argentino

El ciberataque al RENAPER no solo expuso las debilidades de la infraestructura digital del gobierno argentino, sino que también reveló la necesidad de una transformación cultural en la gestión de la ciberseguridad. La protección de los datos personales y la preservación de la privacidad de los ciudadanos requieren un enfoque preventivo y proactivo en ciberseguridad. Este incidente debe servir como un llamado de atención para implementar políticas integrales de protección digital que prioricen la formación continua, la concienciación en ciberseguridad y la adopción de tecnologías avanzadas de protección de datos. La ciberseguridad es un desafío global, y Argentina debe adaptarse a las amenazas emergentes fortaleciendo su infraestructura digital y promoviendo una cultura de seguridad en todos los niveles de la administración pública.

Intrusión en el Poder Judicial de la Provincia del Chaco

En diciembre de 2021, el Poder Judicial de la Provincia del Chaco en Argentina fue víctima de un ciberataque masivo que paralizó sus sistemas informáticos durante más de dos semanas. Este incidente, uno de los más graves en términos de ciberseguridad en el ámbito judicial argentino, expuso la vulnerabilidad de las infraestructuras digitales del sector público y reveló la falta de preparación ante

incidentes cibernéticos críticos. El ataque afectó no solo a la operatividad del sistema judicial, sino también a la seguridad de la información sensible, incluidas sentencias judiciales, expedientes digitales y datos personales de empleados y ciudadanos (Página 12, 2021).

El ciberataque fue identificado como un ransomware de tipo “Dharma”, un programa maligno conocido por cifrar archivos en sistemas Windows y exigir un rescate en criptomonedas a cambio de la clave de descifrado (Bleeping Computer, 2021). La intrusión comenzó cuando un empleado del Poder Judicial abrió un correo electrónico fraudulento que contenía un enlace malicioso. Este correo electrónico, diseñado como un ataque de phishing, aprovechó la ingeniería social para engañar al usuario y hacerle descargar un archivo adjunto infectado. Este incidente pone de manifiesto una vez más el factor humano como el eslabón más débil en la cadena de ciberseguridad (ENISA, 2023). La falta de concienciación sobre la detección de correos electrónicos fraudulentos y la ausencia de capacitación en ciberseguridad facilitó el ingreso inicial del ransomware al sistema judicial.

El ataque afectó a más de 500 computadoras y servidores del Poder Judicial, dejando fuera de servicio el sistema de gestión judicial y el portal web de acceso a expedientes, lo que provocó la interrupción de las actividades judiciales en toda la provincia durante más de 15 días. Los operadores judiciales no pudieron acceder a las causas en trámite ni gestionar expedientes digitales, lo que generó un importante atraso en los procedimientos judiciales y afectó el acceso a la justicia de miles de ciudadanos chaqueños (Página/12, 2021). La interrupción de servicios críticos puso de relieve la importancia de la disponibilidad de los sistemas digitales y su impacto directo en la continuidad operativa de las funciones estatales.

El ransomware utilizado en este ataque, “Dharma”, es conocido por encriptar archivos con extensiones específicas y modificar las configuraciones del sistema para bloquear el acceso a los usuarios afectados. Al cifrar datos críticos, como expedientes judiciales y archivos administrativos, los atacantes demandaron un rescate en criptomonedas para restaurar el acceso a la información secuestrada. El monto del rescate no fue revelado oficialmente, pero se estima que podría haber superado los 100.000 dólares en Bitcoin, lo que pone de manifiesto el componente económico de estos ataques (Bleeping Computer, 2021).

A pesar de la magnitud del ataque, el Poder Judicial del Chaco no contaba con un plan de contingencia ni con sistemas de respaldo adecuados para restaurar los datos afectados. La falta de copias de seguridad actualizadas y la inexistencia de un protocolo de respuesta ante incidentes de ciberseguridad hicieron que la recuperación de la información fuera extremadamente complicada y prolongada. La ausencia de un sistema de respaldo eficiente refleja la falta de políticas preventivas de ciberseguridad en el sector público argentino (Forbes Argentina, 2022). Además, el hecho de que los sistemas afectados no contaran con parches de seguridad actualizados ni con herramientas avanzadas de detección de programas malignos evidencia la falta de inversión en tecnologías de protección digital y la insuficiencia de medidas proactivas de ciberseguridad.

La respuesta de las autoridades provinciales fue inicialmente reactiva y limitada. Se contrató a un equipo de expertos en ciberseguridad para investigar el ataque y se solicitó apoyo al Centro de Operaciones de Ciberseguridad (COCS) de la Nación para analizar el alcance del daño. No obstante, la falta de un plan de contingencia y la dependencia de sistemas obsoletos dificultaron la recuperación de los datos cifrados y la restauración de los servicios digitales (DataClave, 2022). Este incidente evidencia la necesidad urgente de implementar protocolos de respuesta ante incidentes cibernéticos en el sector público argentino.

La investigación forense reveló que el ataque podría haber sido prevenido si el Poder Judicial del Chaco hubiera implementado una autenticación multifactorial y medidas de monitoreo de accesos inusuales. La falta de concienciación y capacitación en ciberseguridad por parte del personal del Poder Judicial fue un factor determinante en el éxito del ataque. La ausencia de programas educativos regulares y la falta de simulaciones de phishing para sensibilizar a los empleados sobre las amenazas cibernéticas crearon un entorno vulnerable y propicio para el acceso no autorizado a través de técnicas de ingeniería social (ENISA, 2023).

Este incidente expone la necesidad de fortalecer las políticas de ciberseguridad en el ámbito judicial argentino. La implementación de una estrategia integral de ciberseguridad que incluya la autenticación multifactorial, la actualización continua de parches de seguridad, el monitoreo de accesos y la capacitación regular en ciberseguridad para el personal judicial es crucial para prevenir futuros incidentes. Además, la adopción de programas de concienciación continua, simulaciones de

phishing y ejercicios prácticos de respuesta a incidentes permitirían sensibilizar a los empleados y reducir las brechas de seguridad relacionadas con el factor humano (World Economic Forum, 2023).

La creación de un plan de contingencia con sistemas de respaldo actualizados y la implementación de políticas de recuperación de desastres son esenciales para garantizar la continuidad operativa en caso de futuros incidentes de ransomware. La colaboración con el Centro de Operaciones de Ciberseguridad (COCS) de la Nación y la cooperación con el sector privado son estrategias clave para mejorar la defensa cibernética en el sector judicial argentino (OECD, 2022). La transparencia en la comunicación de incidentes de ciberseguridad también es fundamental para gestionar las crisis y mantener la confianza pública.

El ataque al Poder Judicial del Chaco revela la necesidad de un cambio cultural en la gestión de la ciberseguridad, enfatizando la concienciación y la responsabilidad compartida entre todos los empleados. Además, destaca la importancia de integrar la ciberseguridad en la planificación estratégica y operativa de las instituciones judiciales. La ciberseguridad no debe considerarse únicamente como una cuestión técnica, sino como una prioridad organizacional y cultural en la era digital.

Ciberataque a la Legislatura de la Ciudad de Buenos Aires

En septiembre de 2022, la Legislatura de la Ciudad de Buenos Aires fue víctima de un ciberataque que afectó gravemente sus sistemas informáticos y expuso datos sensibles de funcionarios y ciudadanos. El incidente evidenció una vez más la vulnerabilidad de las infraestructuras digitales del sector público argentino y la necesidad urgente de fortalecer las políticas de ciberseguridad en el ámbito gubernamental. El ataque, identificado como ransomware del tipo “Conti”, paralizó el funcionamiento administrativo y legislativo, interrumpiendo el acceso a documentos y correos electrónicos institucionales durante varias semanas (La Nación, 2022).

El ransomware “Conti” es conocido por ser altamente sofisticado y peligroso, ya que no solo cifra archivos críticos, sino que también exfiltra datos confidenciales antes de encriptarlos, lo que permite a los atacantes amenazar con divulgar información sensible si no se paga el rescate. En este caso, los cibercriminales exigieron un rescate de más de un millón de dólares en criptomonedas para proporcionar la clave de descifrado y evitar la publicación de los datos robados. La negociación con los atacantes

se realizó a través de canales de comunicación cifrados en la darknet, lo que dificultó el seguimiento y la identificación de los responsables (Bleeping Computer, 2022).

El ataque se originó cuando un empleado de la Legislatura abrió un archivo adjunto malicioso en un correo electrónico de phishing diseñado para parecer una comunicación interna. Este archivo contenía macros maliciosas que instalaron el ransomware en el sistema de la víctima, permitiendo a los atacantes acceder a la red interna y propagarse lateralmente a través de los servidores de la Legislatura. La falta de capacitación en ciberseguridad y la ausencia de una política de protección contra correos electrónicos fraudulentos facilitaron el éxito de este ataque de ingeniería social (ENISA, 2023). Este incidente destaca nuevamente el papel crucial del factor humano en la ciberseguridad y subraya la importancia de la concienciación y formación continua para evitar errores humanos que comprometan la seguridad de las infraestructuras digitales.

El ransomware "Conti" aprovechó vulnerabilidades no parcheadas en los servidores de la Legislatura y utilizó técnicas de movimiento lateral para infectar múltiples sistemas críticos. Al cifrar archivos esenciales, incluidos documentos legislativos, correos electrónicos oficiales y bases de datos administrativas, el ataque paralizó las actividades legislativas, impidiendo la realización de sesiones virtuales y el acceso a expedientes digitales. La interrupción de los servicios legislativos afectó la toma de decisiones políticas y generó un atraso significativo en la gestión de proyectos de ley y otros trámites administrativos (Infobae, 2022).

Además del impacto operativo, el ataque comprometió datos sensibles, incluidos correos electrónicos confidenciales, documentos internos y datos personales de legisladores, empleados y ciudadanos que interactuaron con la Legislatura. La exfiltración de datos antes del cifrado agregó una dimensión crítica al incidente, ya que los atacantes utilizaron esta información como medio de extorsión. La amenaza de divulgar estos datos en foros de la darknet generó preocupaciones de privacidad y aumentó la presión sobre las autoridades para negociar el rescate. Sin embargo, la Legislatura optó por no pagar el rescate y recurrió a expertos en ciberseguridad para tratar de recuperar la información utilizando copias de seguridad y herramientas de descifrado (Forbes Argentina, 2022).

La respuesta inicial al ataque fue lenta e ineficiente debido a la falta de un plan de respuesta a incidentes de ciberseguridad y la ausencia de protocolos de contingencia.

La Legislatura carecía de una política de gestión de crisis cibernéticas y no contaba con un equipo especializado en ciberseguridad para gestionar la recuperación de sistemas. Esto provocó una prolongada interrupción de los servicios legislativos y una recuperación parcial que se extendió durante más de un mes (La Nación, 2022). La falta de una estrategia proactiva y la dependencia de sistemas desactualizados complicaron aún más el proceso de recuperación.

La investigación posterior reveló que la Legislatura de la Ciudad de Buenos Aires no contaba con medidas de seguridad básicas, como la autenticación multifactorial y el monitoreo de accesos sospechosos. La ausencia de un programa de formación continua en ciberseguridad y la falta de campañas de concienciación sobre phishing contribuyeron al éxito del ataque. Además, la infraestructura tecnológica utilizada en la Legislatura no había sido actualizada con parches de seguridad recientes, lo que facilitó la explotación de vulnerabilidades conocidas por el ransomware "Conti" (ENISA, 2023). Estos factores expusieron una grave deficiencia en las políticas de ciberseguridad de la institución y reflejaron la falta de preparación para enfrentar ciberataques sofisticados.

El incidente generó un fuerte impacto mediático y afectó la imagen pública de la Legislatura de la Ciudad de Buenos Aires. La transparencia en la comunicación fue limitada, y la falta de información oportuna generó incertidumbre entre los ciudadanos y empleados afectados. Este episodio subraya la necesidad de implementar políticas de comunicación de crisis en casos de ciberataques, garantizando una gestión transparente de la información y manteniendo la confianza pública en las instituciones gubernamentales (Página/12, 2022).

El ciberataque a la Legislatura de la Ciudad de Buenos Aires demuestra la necesidad de adoptar un enfoque proactivo y preventivo en ciberseguridad, en lugar de depender de respuestas reactivas tras un incidente. La implementación de políticas integrales de ciberseguridad que incluyan la autenticación multifactorial, la actualización continua de parches de seguridad y el monitoreo de accesos inusuales es esencial para proteger las infraestructuras críticas del sector público. Además, la formación continua en ciberseguridad y las simulaciones de phishing son fundamentales para reducir la vulnerabilidad del factor humano y aumentar la conciencia sobre las amenazas cibernéticas (World Economic Forum, 2023).

Asimismo, la Legislatura de la Ciudad de Buenos Aires debería establecer un plan de respuesta a incidentes de ciberseguridad, incluyendo protocolos claros de gestión de crisis y procedimientos de recuperación ante desastres digitales. La creación de un equipo especializado en ciberseguridad y la cooperación con el Centro de Operaciones de Ciberseguridad (COCS) de la Nación permitirían una respuesta más rápida y efectiva ante futuros incidentes (OECD, 2022). Además, se recomienda la adopción de políticas de comunicación de crisis que garanticen la transparencia y la información oportuna para mitigar el impacto en la imagen pública y mantener la confianza de los ciudadanos.

Este caso subraya la importancia de considerar la ciberseguridad como una prioridad estratégica en la administración pública y de integrar la protección digital en todos los niveles organizacionales. La inversión en infraestructuras seguras, la actualización continua de sistemas y la formación regular del personal en ciberseguridad son elementos clave para fortalecer la ciber resiliencia de las instituciones gubernamentales en Argentina.

En conclusión, los ciberataques al Registro Nacional de las Personas (RENAPER), al Poder Judicial de la Provincia del Chaco y a la Legislatura de la Ciudad de Buenos Aires revelan profundas debilidades en las infraestructuras digitales del sector público argentino. Estos incidentes no solo evidencian la falta de preparación y respuesta ante amenazas cibernéticas, sino también la ausencia de políticas integrales de ciberseguridad que incluyan formación continua y medidas de concienciación para el personal. La dependencia de sistemas obsoletos y la escasa implementación de protocolos de protección, como la autenticación multifactorial y la actualización continua de parches de seguridad, han facilitado el acceso no autorizado a datos sensibles y la interrupción de servicios críticos.

Además, el factor humano ha demostrado ser una de las mayores vulnerabilidades, ya que los ataques de phishing y ransomware han aprovechado la falta de conocimiento y concienciación en ciberseguridad de los empleados públicos. La ausencia de programas educativos adecuados y la falta de simulaciones prácticas han dejado expuesto al personal a técnicas de ingeniería social, aumentando la probabilidad de errores humanos que facilitan el acceso de los atacantes. La carencia de una cultura organizacional de ciberseguridad y la insuficiente comunicación de crisis han agravado

las consecuencias de estos incidentes, afectando la confianza pública y generando un impacto negativo en la imagen de las instituciones afectadas.

Estos casos también han demostrado cómo los ciberataques pueden paralizar instituciones clave del país, afectando tanto la operatividad de los servicios gubernamentales como la seguridad de la información. La interrupción de los sistemas legislativos, judiciales y administrativos ha evidenciado la dependencia crítica de las infraestructuras digitales para el funcionamiento del Estado y la continuidad de sus servicios. Esto pone de manifiesto la necesidad urgente de implementar políticas de ciberseguridad más robustas y de adoptar un enfoque proactivo en lugar de reactivo ante las amenazas cibernéticas.

Para enfrentar estos desafíos, es fundamental que el gobierno argentino invierta en la modernización de sus sistemas digitales, la implementación de protocolos de seguridad avanzados y la creación de un Centro Nacional de Ciberseguridad que coordine la respuesta ante incidentes a nivel nacional. Asimismo, es imprescindible adoptar un enfoque integral de formación y concienciación en ciberseguridad que abarque no solo aspectos técnicos, sino también el desarrollo de competencias en gestión de riesgos y la promoción de una cultura organizacional de seguridad digital. La cooperación público-privada y la colaboración internacional también son esenciales para compartir información sobre ciberamenazas y adoptar buenas prácticas en ciberseguridad.

En definitiva, estos incidentes deben servir como una llamada de atención para fortalecer la ciber resiliencia del Estado argentino y garantizar la seguridad digital de sus infraestructuras críticas. La implementación de políticas proactivas y la creación de un entorno educativo continuo son pasos fundamentales para reducir las vulnerabilidades asociadas al factor humano y proteger la información sensible del país. Solo a través de un enfoque integral y coordinado se podrá enfrentar el creciente número de ciberamenazas y garantizar la continuidad de los servicios públicos en un mundo cada vez más digitalizado.

3.5. Desafíos y oportunidades en el fortalecimiento de la ciberseguridad

Argentina enfrenta una serie de desafíos significativos en su esfuerzo por fortalecer la ciberseguridad en el sector público. Uno de los mayores obstáculos radica en la fragmentación en la gestión de la protección digital. Actualmente, diversas agencias gubernamentales se encargan de la seguridad cibernética, pero carecen de una estrategia unificada que permita coordinar de manera efectiva las respuestas ante ciberincidentes. La división de responsabilidades entre distintos niveles de gobierno y organismos crea dificultades para implementar políticas nacionales coherentes, lo que debilita la capacidad de respuesta del país ante amenazas cibernéticas complejas (Taverna & Rutz, 2022). Esta falta de cohesión no solo limita la eficiencia en la utilización de recursos, sino que también incrementa la vulnerabilidad de las infraestructuras digitales críticas del Estado.

Además, otro desafío fundamental es la escasez de recursos financieros y tecnológicos. La implementación de tecnologías avanzadas de protección, como la detección de intrusos en tiempo real, la autenticación multifactorial y el uso de criptografía avanzada, requiere inversiones significativas. Sin embargo, el sector público argentino enfrenta restricciones presupuestarias que han impedido la adquisición de estas soluciones de vanguardia. A esta limitación se suma la falta de personal capacitado en ciberseguridad, un problema crítico en un contexto global en el que la demanda de expertos en seguridad digital supera con creces la oferta. La falta de talento especializado no solo ralentiza la modernización de las infraestructuras de seguridad, sino que también dificulta la optimización y gestión efectiva de las herramientas existentes (SANS Institute, 2022).

El factor humano sigue siendo una de las mayores vulnerabilidades en el ámbito de la ciberseguridad. Los errores humanos, como el uso de contraseñas débiles, la apertura de correos electrónicos maliciosos y la falta de actualización de software, representan una puerta de entrada común para los ciberataques. A pesar de los avances tecnológicos, los empleados públicos a menudo no están adecuadamente capacitados para identificar y mitigar estos riesgos. De acuerdo con un informe de ENISA (2023), el 95% de los incidentes de ciberseguridad pueden atribuirse a errores humanos, lo que subraya la necesidad de programas de formación y concienciación en ciberseguridad en el sector público argentino.

A pesar de estos desafíos, existen diversas oportunidades para fortalecer la ciberseguridad en Argentina. Una de las más relevantes es la creación de un Centro Nacional de Ciberseguridad que coordine las acciones gubernamentales y privadas en torno a la defensa cibernética. Este centro permitiría monitorear de manera centralizada las amenazas, gestionar las políticas de protección de infraestructuras críticas y coordinar la respuesta ante incidentes a nivel nacional. Además, facilitaría la cooperación internacional y el intercambio de información sobre ciberamenazas con otros países, fortaleciendo la ciberresiliencia del Estado argentino. La experiencia de países como Estonia y España, que han implementado estrategias de cooperación público-privada y formación continua, ofrece valiosas lecciones que podrían adaptarse al contexto argentino (World Economic Forum, 2023).

Asimismo, la cooperación público-privada representa una oportunidad clave para mejorar la protección de las infraestructuras críticas. En Argentina, muchas de estas infraestructuras, como las telecomunicaciones, la energía y el transporte, son operadas por empresas privadas. Por lo tanto, es fundamental fomentar una colaboración más estrecha entre el sector público y privado para compartir información sobre amenazas cibernéticas y coordinar la defensa colectiva del país. La implementación de plataformas de intercambio de información y la realización de ejercicios conjuntos de simulación de ciberataques ayudarían a mejorar la preparación y la respuesta ante incidentes de seguridad cibernética. Según un informe de la OECD (2022), los países que han adoptado modelos de cooperación público-privada han logrado reducir significativamente el tiempo de respuesta ante ciberincidentes.

Otro aspecto crucial es el fortalecimiento de la formación y concienciación en ciberseguridad. Los resultados de la encuesta realizada a empleados del sector público argentino revelaron que el 59% de los encuestados no ha recibido ninguna formación o información relacionada con la ciberseguridad en su trabajo, lo que pone de manifiesto la necesidad de programas educativos adaptados a las necesidades del sector público. La implementación de campañas de concienciación, simulaciones de ciberataques y programas educativos interactivos podría fortalecer la cultura de seguridad digital y reducir las vulnerabilidades asociadas al factor humano. La Universidad de Palermo, por ejemplo, ofrece una Licenciatura en Ciberseguridad diseñada para formar expertos en la gestión de la seguridad en empresas y en la implementación efectiva de medidas de protección tanto en infraestructuras de hardware como en la nube, lo que demuestra

el creciente interés en capacitar profesionales en este campo (Universidad de Palermo, s.f.).

Finalmente, Argentina tiene la oportunidad de desarrollar una legislación más robusta en torno a la protección de datos personales y la gestión de ciberincidentes. La implementación de un marco normativo integral no solo brindaría mayores garantías a los ciudadanos en términos de privacidad y protección de datos, sino que también permitiría una mejor coordinación en la respuesta ante incidentes de seguridad cibernética. La adopción de estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, podría servir como modelo para fortalecer la protección de datos en el contexto argentino.

En conclusión, aunque el sector público argentino enfrenta desafíos significativos en el fortalecimiento de su ciberseguridad, también existen oportunidades estratégicas para mejorar su capacidad de defensa ante amenazas digitales. La creación de un Centro Nacional de Ciberseguridad, la cooperación público-privada y el fortalecimiento de la formación continua son pasos fundamentales para reducir las vulnerabilidades asociadas al factor humano y garantizar la protección de las infraestructuras críticas del Estado. La implementación de políticas integrales y coordinadas, junto con la adopción de una cultura organizacional de ciberseguridad, permitirá a Argentina enfrentar de manera efectiva el creciente número de ciberamenazas y asegurar la continuidad de sus servicios públicos en un entorno digital cada vez más complejo.

Capítulo 4: Propuesta de Formación y Concienciación en Ciberseguridad para el Sector Público

En el contexto actual, donde las amenazas cibernéticas evolucionan constantemente y afectan tanto a infraestructuras críticas como a datos sensibles, la ciberseguridad se ha convertido en una prioridad para los gobiernos de todo el mundo. En Argentina, el sector público enfrenta desafíos significativos en términos de protección digital, como se evidenció en los incidentes de seguridad en el RENAPER y la Legislatura de la Ciudad de Buenos Aires. Estos eventos han revelado no solo la vulnerabilidad de las infraestructuras digitales, sino también la necesidad urgente de mejorar la formación y concienciación en ciberseguridad entre los empleados públicos (Forbes Argentina, 2024; Clarín, 2022).

El factor humano sigue siendo una de las principales vulnerabilidades en ciberseguridad. La falta de conocimientos adecuados, combinada con una baja concienciación sobre los riesgos digitales, incrementa la probabilidad de errores humanos, que a su vez pueden conducir a incidentes de seguridad significativos. A pesar de los avances en tecnologías de protección digital, muchos ciberataques explotan precisamente las debilidades humanas mediante técnicas de ingeniería social, como el phishing o el spear-phishing (ENISA, 2023). Por lo tanto, la formación y concienciación continua de los empleados públicos se ha vuelto esencial para fortalecer la ciber resiliencia del Estado argentino y proteger la integridad de sus infraestructuras críticas.

Este capítulo presenta una propuesta integral de formación y concienciación en ciberseguridad diseñada específicamente para el sector público argentino. La propuesta se basa en un enfoque continuo y cíclico, adaptado a las necesidades identificadas en los análisis realizados en capítulos anteriores. Se busca no solo educar a los empleados en temas técnicos de ciberseguridad, sino también crear una cultura organizacional de seguridad digital que fomente una actitud proactiva y responsable ante las amenazas cibernéticas.

La propuesta incluye actividades formativas distribuidas estratégicamente a lo largo del año, con un enfoque en la concienciación continua y la evaluación constante del nivel de conocimientos. Estas actividades abarcan desde campañas de phishing y noticias de ciberseguridad hasta cursos interactivos y seminarios informativos. La estrategia se enfoca en reforzar tanto las competencias técnicas como las habilidades conductuales necesarias para identificar, prevenir y gestionar incidentes de seguridad.

A continuación, se detallan los objetivos específicos, las estrategias de formación continua, los contenidos formativos y metodologías recomendadas, y los mecanismos de evaluación y seguimiento que permitirán medir la efectividad de la propuesta formativa y ajustarla según las necesidades detectadas. La implementación de este plan no solo fortalecerá la ciber resiliencia del Estado argentino, sino que también contribuirá a crear un entorno laboral más seguro y consciente de los riesgos digitales.

4.1 Objetivos de la propuesta formativa

El objetivo principal de esta propuesta es incrementar el nivel de concienciación y formación en ciberseguridad de los empleados del sector público argentino, reduciendo así la incidencia de errores humanos y mejorando la ciber resiliencia de las infraestructuras digitales del Estado. Se busca capacitar a los empleados para que puedan identificar, prevenir y gestionar ciberamenazas de manera efectiva, promoviendo una cultura organizacional de seguridad digital que abarque tanto las competencias técnicas como las habilidades comportamentales necesarias en el contexto actual.

Mejorar la concienciación en ciberseguridad en todos los niveles del sector público es una prioridad fundamental. Es esencial que los empleados comprendan la importancia de implementar buenas prácticas de seguridad digital en sus actividades laborales diarias, tales como la gestión segura de contraseñas, la identificación de correos electrónicos fraudulentos y la protección de datos personales. La creación de una cultura de ciberseguridad no solo fortalecerá la capacidad de respuesta ante ciberamenazas, sino que también fomentará una actitud preventiva y responsable frente a los riesgos digitales.

Otro de los objetivos de esta propuesta es fortalecer las competencias técnicas y comportamentales necesarias para identificar y responder de manera efectiva a ciberamenazas. Para ello, se implementarán actividades formativas prácticas y simulaciones de ciberataques, como campañas de phishing, que permitirán a los empleados aplicar los conocimientos adquiridos en situaciones reales. Este enfoque basado en experiencias prácticas y desafíos interactivos no solo mejora la retención del conocimiento, sino que también fortalece la capacidad de respuesta ante incidentes de seguridad (SANS Institute, 2022).

Reducir la incidencia de errores humanos es un componente crítico de esta propuesta formativa. Los errores humanos, como el uso de contraseñas débiles o la interacción con correos electrónicos maliciosos, siguen siendo una de las principales causas de incidentes de ciberseguridad. La formación continua y la evaluación periódica ayudarán a los empleados a estar mejor preparados para identificar y gestionar riesgos digitales, minimizando así las vulnerabilidades asociadas al factor humano (ENISA, 2023). La propuesta no solo se enfocará en la enseñanza de habilidades técnicas, sino también en la concienciación sobre el impacto de los errores humanos en la seguridad

digital, fomentando una cultura organizacional de ciberseguridad basada en la responsabilidad compartida y la proactividad ante riesgos digitales.

La creación de una cultura organizacional de ciberseguridad es otro de los pilares fundamentales de esta propuesta. Se busca fomentar un enfoque integral que abarque tanto los aspectos técnicos como los comportamentales de la ciberseguridad. Esto implica no solo educar a los empleados en el uso de herramientas de protección digital, sino también promover una actitud proactiva y colaborativa en el entorno laboral. La concienciación continua y la participación activa de todos los empleados son elementos clave para fortalecer la ciber resiliencia del Estado argentino y garantizar la protección de sus infraestructuras críticas.

Además, esta propuesta tiene como objetivo promover la formación continua y la actualización constante de conocimientos en ciberseguridad. En un entorno digital en constante cambio, donde las amenazas cibernéticas evolucionan rápidamente, es esencial que los empleados se mantengan informados sobre las últimas tendencias en ciberseguridad y adquieran habilidades adaptativas para enfrentar nuevos desafíos digitales. Para lograrlo, se implementarán actividades formativas periódicas, como campañas de phishing, cursos interactivos y seminarios informativos, que garantizarán una actualización constante del conocimiento y permitirán a los empleados enfrentar con éxito las amenazas emergentes.

En resumen, la propuesta formativa no solo busca fortalecer las competencias técnicas y comportamentales de los empleados del sector público argentino, sino también crear una cultura organizacional de ciberseguridad basada en la concienciación continua, la responsabilidad compartida y la proactividad ante riesgos digitales. La implementación de este enfoque integral contribuirá significativamente a mejorar la ciberresiliencia del Estado argentino y a proteger la integridad de sus infraestructuras digitales.

4.2. Estrategias de formación continua para los empleados del sector público

Para lograr los objetivos planteados, se ha diseñado un plan anual de formación y concienciación en ciberseguridad, estructurado en actividades periódicas distribuidas estratégicamente a lo largo del año. Este enfoque continuo y cíclico garantiza que los empleados del sector público argentino reciban formación constante, manteniendo sus conocimientos actualizados y mejorando su capacidad de respuesta ante ciberamenazas. La propuesta formativa se basa en la premisa de que la concienciación y el entrenamiento continuo son fundamentales para mitigar los riesgos asociados al factor humano, que sigue siendo la principal vulnerabilidad en la ciberseguridad (ENISA, 2023). A través de un enfoque integral y adaptativo, la estrategia formativa no solo mejora las competencias técnicas, sino que también fomenta una cultura organizacional de ciberseguridad basada en la responsabilidad compartida y la vigilancia constante ante amenazas digitales emergentes.

El plan anual contempla la implementación de cinco actividades clave: Noticias de Ciberseguridad, Cursos de Ciberseguridad, Seminarios Informativos, Campañas de Phishing y un Curso Obligatorio de Ciberseguridad para Nuevas Incorporaciones. Estas actividades han sido diseñadas de manera complementaria para abordar las necesidades específicas de formación en el sector público, fomentando un enfoque proactivo y preventivo en la protección de datos y sistemas críticos. La combinación de actividades teóricas y prácticas garantiza que los empleados no solo adquieran conocimientos, sino que también desarrollen habilidades prácticas para identificar y gestionar ciberamenazas en tiempo real (KnowBe4, 2023).

Las Noticias de Ciberseguridad consisten en el envío periódico de boletines informativos a través de correo electrónico, los cuales incluirán actualizaciones sobre incidentes cibernéticos, tendencias en amenazas digitales como phishing y ransomware, y mejores prácticas en protección de datos. Este enfoque busca mantener a los empleados informados sobre los riesgos emergentes y fomentar una actitud preventiva y de vigilancia continua. Los boletines informativos también incluirán casos reales de ciberincidentes y recomendaciones prácticas, lo que permitirá a los empleados aprender de situaciones concretas y aplicar el conocimiento adquirido en su entorno laboral (ENISA, 2023). La inclusión de este componente en el plan anual responde a la necesidad de mantener una conciencia situacional constante, especialmente en un entorno digital dinámico donde las amenazas evolucionan rápidamente.

Los Cursos de Ciberseguridad se desarrollarán utilizando plataformas de aprendizaje en línea, con módulos interactivos y desafíos gamificados que evalúan el conocimiento de manera lúdica y efectiva. Estos cursos cubrirán temas críticos como la identificación de correos electrónicos fraudulentos (phishing), el manejo seguro de contraseñas, la protección de datos personales y la respuesta ante incidentes de seguridad. Al adoptar un enfoque interactivo y basado en desafíos, se espera no solo aumentar la retención del conocimiento, sino también motivar a los empleados a aprender de manera continua y proactiva (SANS Institute, 2022). Además, los contenidos formativos se personalizarán según las funciones y responsabilidades de cada área de trabajo, garantizando que los empleados adquieran competencias específicas y relevantes para sus roles en la administración pública. La implementación de cursos gamificados ha demostrado ser una metodología efectiva para mejorar el compromiso y la participación en programas de formación en ciberseguridad (KnowBe4, 2023).

Los Seminarios Informativos se llevarán a cabo de manera trimestral y contarán con la participación de expertos en ciberseguridad, quienes compartirán experiencias reales y ofrecerán recomendaciones prácticas. Estos seminarios estarán diseñados para generar conciencia sobre la importancia de la ciberseguridad en el entorno laboral y su impacto en la continuidad de los servicios públicos. Además, se promoverá un enfoque colaborativo en el que los empleados puedan interactuar con los expertos, hacer preguntas y participar en debates sobre ciberamenazas emergentes y estrategias de mitigación. La inclusión de seminarios informativos en la estrategia formativa responde a la necesidad de ofrecer una perspectiva práctica y actualizada sobre los desafíos en ciberseguridad, fomentando una cultura organizacional de seguridad digital basada en el conocimiento compartido y la colaboración (World Economic Forum, 2023).

Por otro lado, las Campañas de Phishing se llevarán a cabo de manera periódica a lo largo del año, con el objetivo de medir la preparación de los empleados y su capacidad de respuesta ante intentos de suplantación de identidad y otras tácticas de ingeniería social. Estas simulaciones permitirán evaluar el comportamiento de los empleados en situaciones reales y proporcionar retroalimentación personalizada para corregir errores y reforzar buenas prácticas en seguridad digital. Además, los resultados de estas simulaciones se utilizarán para identificar brechas en el conocimiento y ajustar los contenidos formativos en consecuencia. La realización de campañas de phishing ha demostrado ser una de las estrategias más efectivas para aumentar la concienciación

sobre ciberamenazas, ya que permite a los empleados aprender de manera práctica y aplicar sus conocimientos en situaciones controladas (KnowBe4, 2023).

Finalmente, se implementará un Curso Obligatorio de Ciberseguridad para Nuevas Incorporaciones, con el objetivo de garantizar que todos los empleados que ingresen a la administración pública tengan un conocimiento básico sobre ciberseguridad y buenas prácticas en seguridad digital. Este curso abordará temas fundamentales como la gestión segura de contraseñas, la identificación de correos fraudulentos y la protección de datos personales. Al hacer que este curso sea obligatorio para todas las nuevas incorporaciones, se busca fomentar una cultura de seguridad digital desde el inicio de sus actividades laborales, garantizando que los empleados adopten una actitud proactiva y responsable ante los riesgos cibernéticos (OECD, 2022).

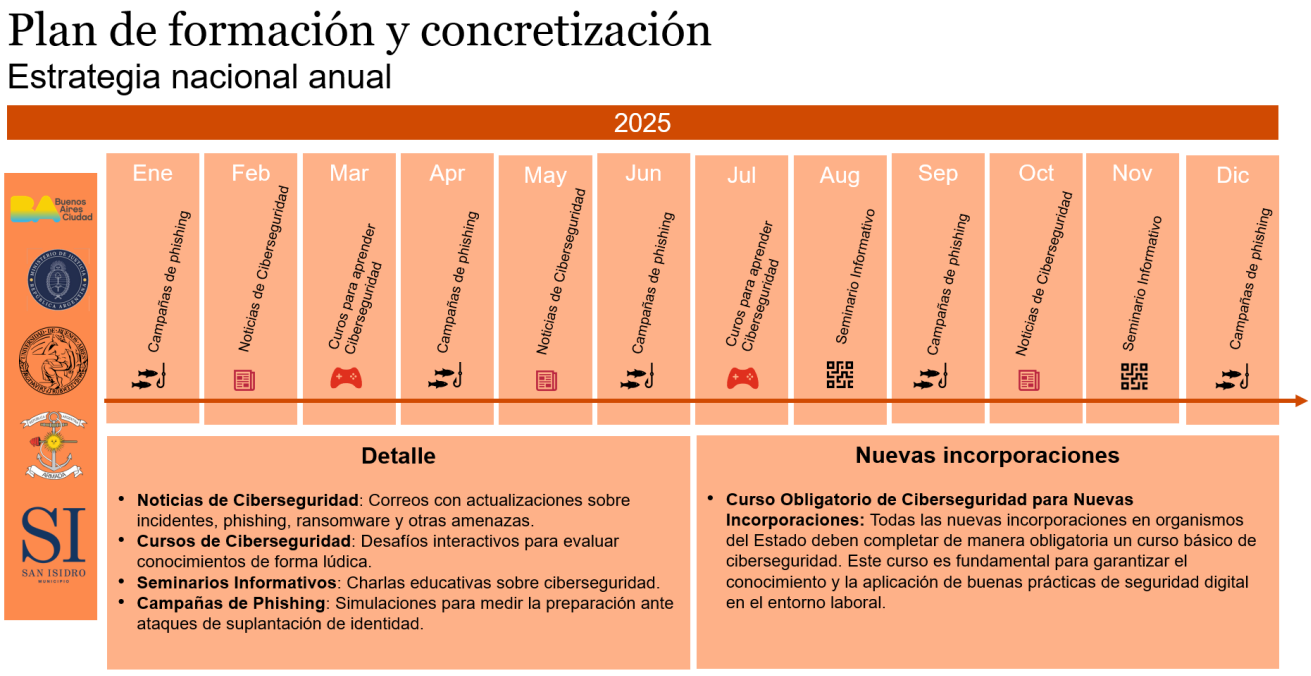

Figura 12:Plan anual de seguridad

En conclusión, la estrategia de formación continua para los empleados del sector público argentino se basa en un enfoque integral y adaptativo que combina simulaciones prácticas, cursos interactivos, seminarios informativos y noticias de ciberseguridad. Este enfoque continuo y cíclico no solo mejorará las competencias técnicas de los empleados, sino que también fomentará una cultura organizacional de ciberseguridad basada en la concienciación, la responsabilidad compartida y la vigilancia constante. La implementación de esta estrategia contribuirá significativamente a fortalecer la ciber

resiliencia del Estado argentino y a garantizar la protección de sus infraestructuras digitales, minimizando así las vulnerabilidades asociadas al factor humano.

4.3. Contenidos formativos y metodologías recomendadas

En la propuesta formativa de ciberseguridad para el sector público argentino, es esencial definir con precisión los contenidos formativos y las metodologías que se utilizarán para transmitirlos de manera efectiva. La elección adecuada de los contenidos garantizará que los empleados adquieran no solo conocimientos teóricos, sino también habilidades prácticas para identificar, prevenir y responder a ciberamenazas en tiempo real. Además, las metodologías deben adaptarse a las diversas necesidades de aprendizaje de los empleados, fomentando una cultura de ciberseguridad basada en la concienciación, la proactividad y la responsabilidad compartida.

En cuanto a los contenidos formativos, se abordarán cinco áreas fundamentales:

1) Conocimientos básicos de ciberseguridad: Este módulo proporcionará una visión general de los conceptos fundamentales de ciberseguridad, incluyendo la tríada de la CIA (Confidencialidad, Integridad y Disponibilidad) y las principales amenazas digitales, como phishing, ransomware, malware, ataques DDoS y técnicas de ingeniería social. Se enfatizará en la identificación temprana de estas amenazas y en las mejores prácticas para protegerse de ellas (Stallings & Brown, 2020). Además, se incluirán estudios de casos reales, como el ciberataque al RENAPER en 2020, para ilustrar cómo las amenazas pueden afectar a las infraestructuras críticas del Estado (Forbes Argentina, 2024). La incorporación de ejemplos locales aumentará la relevancia del contenido y permitirá a los empleados comprender el impacto directo de los ciberataques en su entorno de trabajo.

2) Gestión segura de contraseñas y autenticación: Este módulo abordará la importancia de utilizar contraseñas seguras, únicas y difíciles de adivinar, así como la implementación de autenticación multifactorial para proteger cuentas y sistemas críticos. Se enseñarán mejores prácticas en la creación y gestión de contraseñas, incluyendo el uso de gestores de contraseñas y la actualización periódica de credenciales. Además, se abordarán las vulnerabilidades comunes asociadas al uso inadecuado de contraseñas, como el reciclaje de contraseñas o el uso de combinaciones sencillas (Schneier, 2022). Se espera que, al final de este módulo, los empleados sean capaces de crear contraseñas seguras y administrar sus credenciales de manera eficaz para reducir el riesgo de accesos no autorizados.

3) Identificación de correos electrónicos fraudulentos (phishing): Se enseñará a los empleados a reconocer correos electrónicos maliciosos diseñados para obtener información confidencial o instalar malware en sus dispositivos. El contenido incluirá ejemplos prácticos de correos de phishing, destacando señales de alerta como errores ortográficos, enlaces sospechosos y solicitudes de información personal. Además, se realizarán simulaciones de phishing en un entorno controlado, permitiendo a los empleados practicar la identificación y el reporte de correos fraudulentos sin poner en riesgo la seguridad de los sistemas (KnowBe4, 2023). Este enfoque práctico no solo mejorará las habilidades de detección, sino que también aumentará la confianza de los empleados en su capacidad para identificar intentos de phishing.

4) Protección de datos personales y confidenciales: Este módulo cubrirá las mejores prácticas para proteger la información personal y confidencial de los ciudadanos y empleados del sector público. Se abordarán temas como la clasificación de datos, el cifrado de información sensible y la eliminación segura de datos confidenciales. Además, se explicará la importancia de cumplir con las normativas de protección de datos, como la Ley de Protección de Datos Personales de Argentina (Ley N.º 25.326), para garantizar la privacidad y seguridad de la información almacenada en sistemas gubernamentales. La inclusión de este módulo responde a la necesidad de fortalecer la protección de datos sensibles, especialmente considerando el incremento de ataques dirigidos a la obtención de información personal a través de técnicas de ingeniería social (ENISA, 2023).

5) Respuesta ante incidentes de ciberseguridad: Se enseñará a los empleados a seguir un protocolo adecuado para responder a incidentes de ciberseguridad, minimizando el impacto y acelerando la recuperación. Este módulo incluirá instrucciones sobre cómo informar incidentes, cómo aislar dispositivos comprometidos y cómo colaborar con el equipo de seguridad de la información para mitigar daños. Además, se simularán ciberincidentes en un entorno controlado, permitiendo a los empleados practicar la respuesta ante situaciones de crisis digital. La inclusión de simulaciones prácticas es esencial para mejorar la capacidad de reacción y garantizar que los empleados puedan actuar con rapidez y eficacia ante ciberamenazas reales (SANS Institute, 2022).

En cuanto a las metodologías de formación, se adoptará un enfoque mixto que combine aprendizaje en línea, simulaciones prácticas y sesiones presenciales. El aprendizaje en línea permitirá a los empleados acceder a contenidos formativos de

manera flexible, desde cualquier dispositivo con conexión a internet. Los módulos en línea incluirán videos educativos, cuestionarios interactivos y desafíos gamificados para evaluar el conocimiento de manera lúdica y efectiva. Además, se utilizarán plataformas de e-learning con sistemas de seguimiento y evaluación automática, lo que permitirá monitorear el progreso de cada empleado y adaptar el contenido según sus necesidades específicas.

Por otro lado, las simulaciones prácticas serán una herramienta clave para poner en práctica los conocimientos adquiridos en un entorno controlado y seguro. Se llevarán a cabo simulaciones de phishing, ejercicios de respuesta ante incidentes y pruebas de habilidades técnicas en laboratorios virtuales. Estas simulaciones no solo evaluarán el comportamiento de los empleados en situaciones reales, sino que también proporcionarán retroalimentación personalizada para corregir errores y reforzar buenas prácticas en seguridad digital (KnowBe4, 2023).

Finalmente, se llevarán a cabo sesiones presenciales y seminarios informativos, en los que expertos en ciberseguridad compartirán experiencias reales y ofrecerán recomendaciones prácticas. Estas sesiones promoverán un enfoque colaborativo en el que los empleados podrán interactuar con los expertos, plantear preguntas y participar en debates sobre ciberamenazas emergentes y estrategias de mitigación. La combinación de metodologías interactivas y colaborativas garantizará que los empleados no solo adquieran conocimientos teóricos, sino que también desarrollen habilidades prácticas y adopten una actitud proactiva ante los riesgos digitales.

En conclusión, la selección de contenidos formativos y metodologías para el plan de formación en ciberseguridad en el sector público argentino responde a la necesidad de abordar las vulnerabilidades asociadas al factor humano y fomentar una cultura de ciberseguridad basada en la concienciación, la responsabilidad compartida y la vigilancia constante. Al implementar un enfoque integral y adaptativo, se espera mejorar significativamente las competencias técnicas de los empleados y reducir las vulnerabilidades de las infraestructuras digitales del Estado argentino.

4.4. Mecanismos de evaluación y seguimiento

Para garantizar la efectividad de la propuesta formativa en ciberseguridad en el sector público argentino, es fundamental establecer mecanismos sólidos de evaluación y seguimiento. La evaluación no solo permite medir el nivel de conocimiento adquirido por los empleados, sino que también proporciona información valiosa para ajustar y mejorar continuamente el programa formativo. El seguimiento, por otro lado, asegura que los aprendizajes sean aplicados de manera efectiva en el entorno laboral, fortaleciendo así la cultura de ciberseguridad en las instituciones públicas.

La evaluación de los programas de formación en ciberseguridad debe realizarse en varias etapas para obtener una visión integral de su efectividad. La primera etapa corresponde a la evaluación inicial, que se llevará a cabo antes de que los empleados participen en los cursos o actividades formativas. Esta evaluación inicial medirá el nivel de conocimiento previo y las actitudes hacia la ciberseguridad. A través de cuestionarios y encuestas en línea, se evaluará el grado de familiaridad con conceptos clave, como phishing, ransomware, autenticación multifactorial y protección de datos personales. Esta línea de base permitirá identificar brechas de conocimiento y diseñar contenidos adaptados a las necesidades específicas del personal público (ENISA, 2023).

Después de completar los cursos y actividades formativas, se realizará una evaluación intermedia para medir el progreso de los empleados y su comprensión de los conceptos enseñados. Esta etapa incluye evaluaciones prácticas, como simulaciones de ataques de phishing y ejercicios de identificación de amenazas digitales. Las simulaciones de phishing se utilizarán para medir la capacidad de los empleados para identificar correos electrónicos maliciosos y tomar decisiones seguras en situaciones reales. Los resultados de estas simulaciones se analizarán para identificar posibles brechas de conocimiento y ajustar el contenido formativo en consecuencia (KnowBe4, 2023).

Asimismo, se utilizarán evaluaciones de seguimiento continuo para asegurar que los conocimientos adquiridos sean aplicados de manera efectiva en el entorno laboral. Estas evaluaciones incluyen cuestionarios periódicos, encuestas de retroalimentación y análisis de incidentes de seguridad en las instituciones públicas. El seguimiento continuo permitirá evaluar la transferencia del conocimiento teórico a la práctica diaria y detectar si los empleados aplican de manera efectiva las buenas prácticas de

ciberseguridad, como el uso de contraseñas seguras, la verificación de correos electrónicos y la protección de datos sensibles (SANS Institute, 2022).

Otro componente esencial del seguimiento es la medición de la efectividad de las campañas de phishing. Las simulaciones periódicas de phishing ayudarán a evaluar la capacidad de respuesta de los empleados ante intentos de suplantación de identidad. Los resultados se analizarán para identificar patrones de comportamiento, determinar la tasa de clics en enlaces maliciosos y evaluar la efectividad de las contramedidas implementadas. Este enfoque basado en datos permitirá ajustar las campañas de concienciación y reforzar las áreas donde se detecten debilidades (ENISA, 2023).

La retroalimentación cualitativa también desempeña un papel importante en el seguimiento. Se realizarán encuestas de satisfacción y grupos focales para recopilar opiniones de los empleados sobre la calidad de los contenidos formativos, la claridad de los temas abordados y la relevancia de las actividades prácticas. La retroalimentación cualitativa proporcionará información valiosa sobre la percepción de los empleados respecto a la importancia de la ciberseguridad en su trabajo diario y ayudará a identificar áreas de mejora en el diseño del programa formativo (Stallings & Brown, 2020).

Para asegurar una evaluación integral del programa formativo, se utilizarán métricas cuantitativas y cualitativas que permitan medir el impacto en la organización. Entre las métricas cuantitativas se incluyen la tasa de finalización de los cursos, el porcentaje de empleados que aprueban las evaluaciones, la tasa de clics en simulaciones de phishing y la reducción de incidentes de seguridad relacionados con errores humanos. Por otro lado, las métricas cualitativas evaluarán la percepción de los empleados sobre su preparación ante ciberamenazas y su nivel de confianza para manejar situaciones de seguridad cibernética (SANS Institute, 2022).

Para garantizar la transparencia y la mejora continua, se elaborarán informes trimestrales y anuales con los resultados de las evaluaciones y el seguimiento del programa formativo. Estos informes se presentarán a los responsables de ciberseguridad de las instituciones públicas, quienes utilizarán esta información para tomar decisiones informadas sobre la mejora continua de la formación en ciberseguridad. Además, se realizarán auditorías internas y externas para garantizar la calidad del programa y verificar que se cumplen los objetivos de formación y concienciación establecidos (ENISA, 2023).

En conclusión, la implementación de mecanismos sólidos de evaluación y seguimiento es fundamental para el éxito de la propuesta formativa en ciberseguridad en el sector público argentino. Estos mecanismos permitirán medir el impacto de la formación en el conocimiento y las prácticas de ciberseguridad de los empleados, identificar áreas de mejora y ajustar continuamente el contenido formativo para enfrentar las amenazas cibernéticas en constante evolución. Al utilizar un enfoque basado en datos y retroalimentación cualitativa, se fortalecerá la cultura de ciberseguridad en las instituciones públicas, mejorando así la ciber resiliencia del Estado.

Capítulo 5: Evaluación de la Eficacia de los Programas de Formación en Ciberseguridad

5.1. Métricas de evaluación y desempeño en ciberseguridad

En el contexto actual de creciente dependencia digital, la evaluación efectiva de los programas de formación en ciberseguridad es fundamental para garantizar la protección de las infraestructuras críticas y la seguridad de la información en el sector público. La medición del impacto de estos programas requiere el establecimiento de un conjunto diverso de métricas de desempeño que permitan evaluar tanto el conocimiento adquirido como la capacidad de respuesta ante incidentes cibernéticos (SANS Institute, 2022). Estas métricas deben ser específicas y alineadas con los objetivos generales de las instituciones públicas, y deben ir más allá de los resultados de las pruebas teóricas para incluir aspectos más profundos que midan la aplicabilidad práctica de lo aprendido y el impacto organizacional de la formación (Pfleeger, Pfleeger, & Margulies, 2023).

Una de las principales métricas es la medición del conocimiento adquirido y la mejora en las competencias técnicas. Para ello, se utilizan tanto evaluaciones teóricas como prácticas que miden no solo la comprensión conceptual, sino también la capacidad de aplicar esos conocimientos en situaciones reales. Las evaluaciones teóricas pueden centrarse en conceptos básicos de ciberseguridad, como la gestión de contraseñas, la identificación de correos electrónicos fraudulentos y las normas de protección de datos. Según Whitman y Mattord (2022), “la evaluación del conocimiento teórico proporciona una base sólida para medir la comprensión de los principios fundamentales de la ciberseguridad” (pág. 115). Sin embargo, las evaluaciones prácticas son esenciales para reflejar la capacidad de los empleados para aplicar estos conocimientos en situaciones cotidianas. Estas evaluaciones incluyen simulaciones de incidentes cibernéticos, como ataques de phishing, ransomware o denegación de servicio distribuida (DDoS), en las que los empleados deben demostrar su habilidad para identificar, mitigar y recuperarse de los ataques (Stallings & Brown, 2020).

Las pruebas prácticas son especialmente relevantes para evaluar la efectividad de la formación, ya que permiten medir la reacción real de los empleados en situaciones de presión. Según el SANS Institute (2022), las simulaciones prácticas proporcionan una comprensión más profunda de cómo los empleados aplican sus habilidades en situaciones del mundo real. Un enfoque recomendado es la utilización de plataformas de simulación interactivas que permitan recrear escenarios realistas de ciberataques. Estas

plataformas no solo miden el tiempo de respuesta, sino también la precisión en la identificación de amenazas y la aplicación de protocolos de seguridad. La integración de estas herramientas en el sector público argentino podría mejorar significativamente la preparación ante ciberincidentes, alineándose con las mejores prácticas internacionales en ciberseguridad (OECD, 2022).

Otra métrica fundamental es la evaluación del impacto en la reducción de errores humanos, dado que el factor humano sigue siendo la mayor vulnerabilidad en los sistemas de ciberseguridad (Anderson, 2021). Los errores humanos, como contraseñas débiles, clics en enlaces maliciosos o la falta de actualización de software, continúan siendo una puerta de entrada para los atacantes. Para medir la reducción de estos errores, se pueden analizar los incidentes de seguridad ocurridos antes y después de la formación. De acuerdo con ENISA (2023), "la reducción de errores humanos es una métrica directa de la efectividad de los programas de formación en ciberseguridad, ya que refleja una mejora tangible en las prácticas diarias de los empleados" (pág. 78). Además, las encuestas de autoevaluación y los análisis de comportamiento digital permiten medir el cambio en las actitudes y percepciones de los empleados sobre la ciberseguridad. Estos instrumentos pueden revelar si la formación ha aumentado la conciencia de los riesgos digitales y ha fomentado prácticas más seguras, como el uso de autenticación multifactorial o la verificación de correos electrónicos sospechosos (Bishop, 2019).

La evaluación de la mejora en la respuesta ante incidentes cibernéticos es otro aspecto crucial en la medición del desempeño. La rapidez y efectividad de la respuesta ante un ciberataque pueden marcar la diferencia entre un incidente controlado y una catástrofe de seguridad (Schneier, 2022). En este sentido, las simulaciones de ciberincidentes y los ejercicios de mesa son herramientas útiles para medir la capacidad de los empleados para identificar amenazas, coordinar respuestas y aplicar protocolos de recuperación. Estas simulaciones permiten evaluar tanto el tiempo de detección como el tiempo de respuesta, así como la calidad de las decisiones tomadas durante el incidente. Según un estudio de Zhang-Kennedy y Chiasson (2022), "las simulaciones de ciberincidentes mejoran significativamente la capacidad de respuesta de los empleados, ya que proporcionan un entorno controlado para practicar la gestión de crisis cibernéticas" (pág. 53).

Asimismo, se deben considerar indicadores cualitativos, como las entrevistas con empleados y supervisores, que proporcionan información sobre la percepción de la formación y su aplicabilidad en el trabajo diario. Este enfoque permite identificar las áreas de mejora en el diseño de los programas de formación y ajustar los contenidos para abordar las necesidades específicas del sector público argentino (World Economic Forum, 2023). Además, la retroalimentación constante de los empleados ayuda a evaluar la motivación y el compromiso con la ciberseguridad, lo que es fundamental para crear una cultura organizacional de seguridad digital.

En conclusión, la implementación de métricas de evaluación y desempeño en ciberseguridad en el sector público argentino es esencial para garantizar la efectividad de los programas de formación y mejorar la capacidad de respuesta ante ciberamenazas. La integración de evaluaciones teóricas, simulaciones prácticas, análisis de comportamiento digital y encuestas de autoevaluación proporciona un enfoque integral para medir el conocimiento adquirido, la reducción de errores humanos y la mejora en la respuesta ante incidentes. Estas métricas deben estar alineadas con las mejores prácticas internacionales y adaptadas a las necesidades específicas del sector público argentino, garantizando una formación continua y efectiva en ciberseguridad (OECD, 2022).

5.2. Análisis de la mejora en la respuesta ante ciberincidentes

El análisis de la mejora en la respuesta ante ciberincidentes es un componente esencial para evaluar la efectividad de los programas de formación en ciberseguridad en el sector público argentino. La capacidad de respuesta ante incidentes no solo determina la rapidez con la que se mitigan los daños, sino también la capacidad de una organización para aprender de los ataques y adaptarse a nuevas amenazas. En el contexto actual, donde los ciberataques se han vuelto más sofisticados y frecuentes, la formación en ciberseguridad debe ir más allá de la mera concienciación teórica e involucrar la aplicación práctica de conocimientos y habilidades en escenarios reales o simulados.

En el sector público argentino, la respuesta ante ciberincidentes se ve obstaculizada por una serie de desafíos. En primer lugar, la falta de formación continua y especializada impide que los empleados desarrollen una comprensión profunda de las tácticas, técnicas y procedimientos (TTPs) utilizados por los atacantes cibernéticos. De acuerdo con el World Economic Forum (2023), la velocidad y complejidad de los ciberataques han aumentado significativamente, lo que requiere que los empleados sean capaces de identificar y responder a amenazas en tiempo real. Sin embargo, la encuesta realizada a 157 empleados del sector público argentino reveló que solo el 41% ha recibido algún tipo de formación en ciberseguridad, mientras que el 59% no ha recibido ninguna capacitación (World Economic Forum, 2023). Esto sugiere que una gran parte de la fuerza laboral no está preparada para identificar o gestionar ciberincidentes de manera efectiva, aumentando la vulnerabilidad de las infraestructuras críticas del Estado.

Además, el análisis de la encuesta realizada por el autor a 157 empleados públicos en 2024 revela que el 44% ha sido víctima de un problema de seguridad informática en el pasado, evidenciando una exposición significativa a ciberamenazas en el sector público argentino. Un preocupante 20% de los encuestados respondió "No lo sé" cuando se les preguntó si habían sido víctimas de un ataque, lo que destaca una falta de concienciación sobre la naturaleza de los ciberataques, un hallazgo consistente con tendencias globales reportadas por ENISA (2023). Esta brecha subraya la vulnerabilidad de los empleados como eslabón crítico, justificando la necesidad de programas de formación propuestos en esta tesis.

En términos de preparación organizacional, el 55% de los empleados considera que su organización está "algo preparada" para enfrentar ciberataques, mientras que un 21% la percibe como "poco preparada" y un 5% como "nada preparada". Estos resultados reflejan una falta de confianza en las capacidades de respuesta ante incidentes de seguridad digital y sugieren que las instituciones públicas en Argentina no han desarrollado protocolos de respuesta claros y efectivos. La ausencia de simulacros regulares y evaluaciones de ciberincidentes contribuye a esta percepción de inseguridad y prepara un terreno vulnerable para futuros ataques (OECD, 2022).

En este contexto, la implementación de simulacros de ciberataques y ejercicios de respuesta ante incidentes es fundamental para mejorar la capacidad de respuesta de los empleados públicos argentinos. Según un estudio de SANS Institute (2022), los simulacros de ciberincidentes permiten a las organizaciones evaluar sus procedimientos de respuesta en un entorno controlado, identificar debilidades en sus estrategias y mejorar la coordinación interna entre departamentos. Al practicar escenarios realistas, como ataques de phishing, ransomware o denegación de servicio (DDoS), los empleados pueden desarrollar habilidades críticas, incluyendo la identificación temprana de amenazas, la toma de decisiones bajo presión y la comunicación efectiva durante una crisis.

El modelo de formación basado en simulacros ha demostrado ser eficaz en varios países con estrategias avanzadas de ciberseguridad. Por ejemplo, en Estonia, los simulacros de ciberataques son una práctica común tanto en el sector público como en el privado. Estos ejercicios son coordinados por el Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN (CCDCOE) y permiten evaluar la capacidad de respuesta ante incidentes a nivel nacional (CCDCOE, 2023). Asimismo, en España, el Instituto Nacional de Ciberseguridad (INCIBE) organiza simulacros anuales de ciberincidentes en colaboración con empresas del sector privado y organismos gubernamentales, lo que fortalece la cooperación y la respuesta coordinada ante amenazas cibernéticas (INCIBE, 2023). Estos ejemplos internacionales subrayan la importancia de implementar simulacros de ciberseguridad en el sector público argentino para mejorar la capacidad de respuesta y fortalecer la ciber resiliencia del Estado.

Además de los simulacros, es esencial implementar métricas de evaluación para medir la mejora en la respuesta ante incidentes. Esto incluye el tiempo de detección de un ataque, el tiempo de respuesta y la eficacia de las medidas de contención y

recuperación. La aplicación de indicadores clave de rendimiento (KPIs) permite evaluar de manera objetiva la efectividad de los programas de formación y la capacidad de los empleados para gestionar ciberincidentes. Asimismo, la retroalimentación continua es crucial para ajustar los contenidos formativos y los procedimientos de respuesta, garantizando así una mejora continua en la capacidad de respuesta organizacional (Whitman & Mattord, 2022).

En conclusión, el análisis de la mejora en la respuesta ante ciberincidentes en el sector público argentino revela importantes deficiencias en la formación continua y la capacidad de respuesta ante amenazas digitales. La falta de simulacros regulares, la ausencia de métricas de evaluación efectivas y la baja percepción de preparación organizacional destacan la necesidad de adoptar un enfoque integral para la formación en ciberseguridad. Implementar simulacros de ciberataques, establecer indicadores clave de rendimiento y fomentar una cultura de ciberseguridad mediante campañas de concienciación son pasos esenciales para fortalecer la ciberresiliencia del Estado. Además, aprender de las mejores prácticas internacionales, como las de Estonia y España, puede proporcionar un marco efectivo para desarrollar programas de formación adaptados a las necesidades del sector público argentino. La mejora en la respuesta ante ciberincidentes no solo protegerá las infraestructuras digitales del Estado, sino que también garantizará la continuidad de los servicios públicos y la confianza de los ciudadanos en las instituciones gubernamentales.

Capítulo 6: Conclusiones y Recomendaciones

6.1. Conclusiones Generales

El presente estudio ha permitido identificar tanto los avances como las debilidades en la ciberseguridad del sector público argentino, revelando la necesidad de adoptar una estrategia integral y coordinada para proteger las infraestructuras digitales gubernamentales. En un mundo cada vez más interconectado y vulnerable a las ciberamenazas, las instituciones públicas deben garantizar la protección de datos sensibles y servicios críticos. Sin embargo, la realidad argentina muestra múltiples obstáculos que dificultan una defensa efectiva y continua frente a las amenazas digitales emergentes.

Uno de los hallazgos más importantes de esta investigación es que la infraestructura digital del sector público argentino, aunque ha avanzado en términos de digitalización de servicios, sigue siendo vulnerable debido a la desactualización tecnológica y la falta de integración de protocolos de seguridad adecuados. La creciente dependencia de los servicios en línea, junto con la adopción de tecnologías como la nube y el big data, ha incrementado la exposición a ciberamenazas, dejando al descubierto vulnerabilidades críticas en infraestructuras tecnológicas que no cuentan con las capacidades de defensa necesarias (OECD, 2022). La fragmentación en la gestión de la ciberseguridad también contribuye a esta vulnerabilidad, ya que múltiples organismos son responsables de la protección digital sin una estrategia unificada, lo que dificulta una coordinación efectiva y reduce la capacidad de respuesta ante ciberincidentes.

En el ámbito de la formación y concienciación, la investigación revela una significativa insuficiencia en la capacitación de los empleados públicos. A pesar de algunos esfuerzos aislados en talleres de sensibilización, la formación en ciberseguridad no es una práctica estandarizada en las instituciones públicas argentinas, lo que representa una carencia de políticas educativas integrales. La encuesta realizada a 157 empleados del sector público mostró que el 59% no ha recibido ninguna formación en ciberseguridad y solo el 21% ha participado en capacitaciones obligatorias, mientras que el 27% ha asistido a cursos opcionales. Además, el 22% de los empleados desconoce términos críticos como phishing, ransomware y ataques DDoS, mientras que el 57% tiene un conocimiento limitado sobre estas amenazas. Este nivel de desconocimiento representa una vulnerabilidad crítica, ya que el factor humano sigue siendo la principal

puerta de entrada para los ciberataques, especialmente aquellos basados en ingeniería social (ENISA, 2023).

El análisis de casos recientes de ciberataques en Argentina, como el incidente en el RENAPER, la intrusión en el Poder Judicial de la Provincia del Chaco y el ataque a la Legislatura de la Ciudad de Buenos Aires, ha demostrado que los errores humanos y la falta de procedimientos de seguridad adecuados son factores determinantes en la materialización de estos incidentes. Estos casos no solo revelan fallas en la formación y concienciación en ciberseguridad, sino también la ausencia de protocolos estandarizados y la falta de simulaciones prácticas de ciberincidentes que preparen a los empleados para enfrentar ataques reales (Forbes Argentina, 2024). El modelo económico desarrollado en el Capítulo 3.3 confirma esta vulnerabilidad al demostrar que una inversión óptima de 12.42 horas/año por empleado en formación en ciberseguridad genera un beneficio neto de 425.75 USD por empleado y un ROI del 343%, validando la hipótesis principal de que la falta de concienciación representa un riesgo significativo para la ciberseguridad del Estado.

A pesar de estos desafíos, existen oportunidades significativas para mejorar la ciberseguridad en el sector público argentino. La cooperación internacional se presenta como un aspecto clave para fortalecer las capacidades de defensa cibernética. Argentina tiene la posibilidad de aprender de las mejores prácticas internacionales adoptadas en países como Estonia y España, que han demostrado que la formación continua, la concienciación pública y la colaboración público-privada son pilares fundamentales para una estrategia de ciberseguridad exitosa (World Economic Forum, 2023). La adopción de un enfoque integral y coordinado, inspirado en modelos exitosos como el de Estonia, permitiría a Argentina centralizar la gestión de riesgos digitales y promover la concienciación continua en todos los niveles del Estado, fortaleciendo así su ciber resiliencia.

Asimismo, la digitalización creciente de los servicios públicos representa una oportunidad para integrar la ciberseguridad desde el diseño, fomentando una cultura de seguridad digital en todos los niveles del gobierno. La implementación de programas de formación continua, basados en simulaciones prácticas de ciberincidentes y adaptados a las necesidades de cada región, es esencial para fortalecer la cultura de seguridad digital y reducir las vulnerabilidades asociadas al factor humano (SANS Institute, 2022). Además, la alta disposición de los empleados públicos a recibir formación adicional,

como se observó en la encuesta realizada, ofrece una oportunidad estratégica para implementar políticas efectivas de ciberseguridad que reduzcan significativamente los riesgos de ciberataques en el sector público argentino.

En conclusión, los hallazgos de esta investigación destacan la necesidad de adoptar un enfoque integral y coordinado en ciberseguridad en el sector público argentino. La creación de una Estrategia Nacional de Ciberseguridad, basada en modelos exitosos y adaptada al contexto local, permitiría no solo reducir las vulnerabilidades digitales, sino también fomentar una cultura de ciberseguridad que fortalezca la protección de los activos digitales del Estado y garantice la continuidad de los servicios públicos. Esta transformación requiere una inversión en recursos financieros y humanos, así como un compromiso político para priorizar la ciberseguridad como un pilar esencial de la gobernanza digital en Argentina.

6.2. Recomendaciones para la Implementación de Políticas Públicas

Para fortalecer la ciberseguridad en el sector público argentino, es fundamental implementar políticas públicas integrales que aborden tanto las vulnerabilidades tecnológicas como las debilidades humanas. Basándose en el análisis exhaustivo realizado a lo largo de esta investigación, se han identificado una serie de recomendaciones clave que pueden contribuir a mejorar la protección de las infraestructuras digitales del Estado y a elevar el nivel de concienciación en ciberseguridad de los empleados públicos. Estas recomendaciones se fundamentan en las mejores prácticas internacionales y en las lecciones aprendidas de países líderes en ciberseguridad, como Estonia y España, adaptadas al contexto específico de Argentina.

En primer lugar, se recomienda la creación de un Centro Nacional de Ciberseguridad que centralice la coordinación de políticas, la respuesta a incidentes y la protección de infraestructuras críticas. Este centro debería actuar como una entidad estratégica y operativa, responsable de monitorear las amenazas cibernéticas, coordinar las respuestas ante incidentes de seguridad y desarrollar políticas de protección de datos a nivel nacional. Además, el centro debería servir como un punto de contacto centralizado para la cooperación internacional en ciberseguridad, permitiendo a Argentina participar activamente en el intercambio de inteligencia cibernética y en iniciativas globales de defensa digital. Este modelo de centralización ha demostrado ser exitoso en Estonia, donde el Centro Nacional de Ciberseguridad ha mejorado significativamente la capacidad de respuesta ante ciberataques y ha permitido una coordinación más eficiente entre el sector público y privado (Vallance, 2022).

Otra recomendación clave es el desarrollo de una Estrategia Nacional de Ciberseguridad que defina claramente los objetivos, responsabilidades y recursos necesarios para proteger la infraestructura digital del Estado. Esta estrategia debe incluir un marco normativo actualizado que regule la protección de datos, la gestión de incidentes y la cooperación entre organismos públicos y privados. Asimismo, es necesario establecer estándares de seguridad obligatorios para todas las instituciones gubernamentales, asegurando la adopción de medidas de protección consistentes y efectivas. La estrategia también debe incluir un enfoque integral de formación continua y concienciación en ciberseguridad, basado en simulaciones de ciberincidentes, para preparar al personal público ante posibles amenazas digitales (Hernández & Rueda, 2023).

En el ámbito de la formación y concienciación en ciberseguridad, se recomienda la implementación de un Plan Anual de Formación obligatorio para todos los empleados públicos. Este plan debe incluir módulos educativos sobre buenas prácticas de seguridad digital, gestión de contraseñas, identificación de correos electrónicos fraudulentos (phishing) y protección de datos personales. La formación debe ser adaptativa y continua, utilizando metodologías interactivas, como desafíos gamificados y simulaciones de ciberataques, para mantener a los empleados involucrados y mejorar su capacidad de respuesta ante incidentes. Además, se deben implementar campañas de concienciación periódicas, distribuyendo boletines informativos sobre nuevas amenazas cibernéticas y organizando seminarios informativos con expertos en ciberseguridad (Fernández & Gómez, 2022). La experiencia de España demuestra que la educación y concienciación continua son fundamentales para mitigar el impacto del factor humano en los ciberataques (González, 2023). La viabilidad económica de este plan está respaldada por el modelo económico del Capítulo 3.3, que estima que una inversión de 12.42 horas/año por empleado en formación en ciberseguridad genera un beneficio neto de 425.75 USD por empleado y un ROI del 343%. Extrapolado a los aproximadamente 3 millones de empleados públicos, esto representa un beneficio neto agregado de 1,277.25 millones USD anuales, justificando la implementación de programas de formación a gran escala

En términos de cooperación internacional, Argentina debe fortalecer sus alianzas con organismos internacionales y países líderes en ciberseguridad. La cooperación transnacional es esencial para compartir inteligencia sobre amenazas globales, desarrollar capacidades conjuntas de defensa cibernética y participar en ejercicios internacionales de ciberseguridad. Argentina debería unirse a iniciativas globales, como la Alianza Global de Ciberseguridad y el Foro de Resiliencia Cibernética, para beneficiarse del intercambio de conocimientos y adoptar mejores prácticas de seguridad digital. Además, se recomienda la firma de acuerdos bilaterales de cooperación en ciberseguridad con países que lideran en la protección de infraestructuras críticas, como Estonia y España (Agencia de Ciberseguridad Europea, 2023).

La colaboración público-privada es otro componente esencial para fortalecer la ciberseguridad en Argentina. Se debe fomentar una cooperación más estrecha entre el gobierno y el sector privado, especialmente con empresas tecnológicas que gestionan infraestructuras críticas, como telecomunicaciones y energía. La creación de plataformas de intercambio de información sobre ciberamenazas, gestionadas por el

Centro Nacional de Ciberseguridad, permitiría una comunicación efectiva y una respuesta coordinada ante incidentes de seguridad. Asimismo, es necesario impulsar el desarrollo de tecnologías de ciberseguridad locales, promoviendo la innovación en startups y empresas tecnológicas argentinas (Salas, 2023).

Finalmente, es crucial fortalecer el marco normativo en ciberseguridad. Argentina debe actualizar su legislación en materia de protección de datos personales y ciberseguridad, alineándola con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esto no solo mejoraría la protección de la información personal de los ciudadanos, sino que también fortalecería la confianza pública en el manejo de datos gubernamentales. Además, se deben establecer protocolos de gestión de incidentes y auditorías de seguridad periódicas para garantizar el cumplimiento de las políticas de ciberseguridad en todas las instituciones públicas (Rodríguez, 2023).

En conclusión, la implementación de estas recomendaciones permitiría a Argentina no solo fortalecer su ciberseguridad en el sector público, sino también convertirse en un referente regional en protección digital. La creación de un Centro Nacional de Ciberseguridad, el desarrollo de una Estrategia Nacional de Ciberseguridad, la formación continua de empleados públicos y la cooperación internacional son pasos fundamentales hacia una infraestructura digital más segura y resiliente. Estas políticas públicas deben ser implementadas de manera integral y coordinada, asegurando un enfoque holístico que abarque la protección de datos, la concienciación en ciberseguridad y la respuesta eficaz ante incidentes cibernéticos.

6.3. Futuro de la Ciberseguridad en Argentina y en el Sector Público

El futuro de la ciberseguridad en Argentina dependerá de la capacidad del país para adaptarse rápidamente a los cambios tecnológicos y a las nuevas amenazas cibernéticas. En un entorno digital en constante evolución, la implementación de inteligencia artificial (IA) y machine learning jugará un papel fundamental en la detección de ataques avanzados y en el monitoreo proactivo de redes. Estas tecnologías permitirán identificar patrones anómalos y anticipar posibles ciberamenazas antes de que causen daños significativos. Para aprovechar al máximo estas herramientas, Argentina debe integrar IA y machine learning en sus estrategias de seguridad cibernética en el sector público, garantizando que los sistemas sean capaces de aprender y evolucionar con las amenazas emergentes (ENISA, 2023).

Además, la creciente dependencia de tecnologías emergentes, como el Internet de las Cosas (IoT) y los sistemas interconectados, representa un desafío significativo para la protección de infraestructuras críticas. La introducción de dispositivos IoT en servicios públicos, como el transporte, la energía y la salud, amplía la superficie de ataque y aumenta las posibilidades de compromisos de seguridad. En este contexto, Argentina deberá implementar estándares de seguridad IoT y adoptar una arquitectura Zero Trust, que garantice un enfoque de seguridad basado en la verificación continua de identidad y accesos (Kumar & Carthy, 2023).

La formación continua se convertirá en un pilar estratégico para la ciberseguridad en Argentina, ya que las amenazas cibernéticas evolucionan constantemente y las tácticas de ataque se vuelven más sofisticadas. La creación de plataformas de formación digital que ofrezcan contenidos actualizados y prácticos en tiempo real permitirá a los empleados públicos adaptarse a las nuevas amenazas de manera más efectiva. Además, es crucial que la educación cibernética se incorpore en la currícula educativa nacional, con el fin de preparar a las futuras generaciones para enfrentar los desafíos tecnológicos emergentes. Esta estrategia garantizará que Argentina no solo responda a las amenazas actuales, sino que también se anticipe a los riesgos futuros mediante una fuerza laboral capacitada y resiliente (OECD, 2024).

Otra dimensión clave para el futuro de la ciberseguridad en Argentina es la colaboración internacional. La cooperación con organismos internacionales de ciberseguridad, así como la participación en iniciativas globales como el Foro de Resiliencia Cibernética, permitirá al país acceder a conocimientos avanzados y recursos

compartidos en ciberseguridad. Argentina debe fortalecer sus alianzas internacionales para intercambiar mejores prácticas y participar activamente en ejercicios globales de simulación de ciberataques, lo que mejorará su capacidad de respuesta ante incidentes críticos (Vallance, 2022).

En cuanto a la protección de infraestructuras críticas, Argentina debe adoptar un enfoque integral que abarque todos los elementos tecnológicos en el ecosistema gubernamental. La seguridad en la nube será esencial, considerando la creciente adopción de servicios en la nube en el sector público. En este sentido, es fundamental implementar modelos de seguridad Zero Trust y políticas de seguridad en la nube que garanticen una protección robusta de los datos gubernamentales sensibles. Asimismo, se deben realizar auditorías de seguridad periódicas para evaluar y fortalecer las defensas cibernéticas (Rodríguez, 2023).

En definitiva, el futuro de la ciberseguridad en Argentina dependerá de su capacidad de adaptación, anticipación y colaboración en un entorno digital dinámico y en constante cambio. La integración de tecnologías avanzadas, la formación continua de los empleados públicos y la cooperación internacional son fundamentales para fortalecer la resiliencia digital del país. La adopción de estrategias proactivas y la implementación de políticas de ciberseguridad integrales permitirán a Argentina no solo proteger sus infraestructuras críticas, sino también consolidar la confianza en el gobierno digital y garantizar la continuidad de los servicios públicos en el futuro.

6.4 Conclusión Final

En conclusión, el sector público argentino enfrenta desafíos significativos en términos de ciberseguridad, pero también tiene grandes oportunidades para mejorar. La mejora de la infraestructura tecnológica, el fortalecimiento de la formación y concienciación, y el fomento de la cooperación internacional son pilares esenciales para garantizar la protección de los datos y la resiliencia de los servicios gubernamentales ante las crecientes amenazas cibernéticas.

El modelo económico aplicado en el Capítulo 3.3, basado en los datos de la encuesta, demuestra cuantitativamente que una inversión óptima en formación en ciberseguridad genera beneficios netos significativos, reduciendo riesgos y costos asociados a incidentes, y comprueba la hipótesis principal de la tesis.

El país debe adoptar un enfoque integral y adaptativo en ciberseguridad, implementando políticas que no solo refuercen la infraestructura tecnológica, sino que también fomenten una cultura de seguridad digital que involucre a todos los niveles del gobierno. Si Argentina sigue estas recomendaciones, estará mejor posicionada para enfrentar los desafíos del futuro digital y proteger a sus ciudadanos y a sus infraestructuras de las crecientes amenazas en el ciberespacio.

En última instancia, la ciberseguridad no se trata solo de proteger datos y sistemas; se trata de salvaguardar la confianza pública, la estabilidad social y el bienestar de las generaciones futuras. La oportunidad de construir un Estado resiliente y seguro está al alcance, y el momento de actuar es ahora. Con visión estratégica, compromiso institucional y una cultura de ciberseguridad arraigada, Argentina puede no solo enfrentar los desafíos digitales del presente, sino también liderar el camino hacia un futuro más seguro e innovador.

Bibliografía y Referencias

- Anderson, R. (2021). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
- Agencia de Ciberseguridad Europea. (2023). Informe Anual de Ciberamenazas en Europa. Bruselas: ECSA.
- Argentina.gob.ar. (2021). Se aprobó la Segunda Estrategia Nacional de Ciberseguridad.
  Disponible en: https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad
- Argentina.gob.ar. (2023). OPTIMICEMOS LA CIBERSEGURIDAD.
  Disponible en:
  https://www.argentina.gob.ar/sites/default/files/2023/04/optimicemos_la_ciberseguridad_cmm_argentina_2023_reporte.pdf
- BBC News. (2022). Ukraine hit by massive cyber-attack on government websites.
- Banco Interamericano de Desarrollo. (2018). e Estonia: la e gobernanza en la práctica.
  Disponible en: https://publications.iadb.org/publications/spanish/document/e-Estonia-la-e-gobernanza-en-la-practica.pdf
- Brodersen, J. (2023). 2023: Ciberataques, filtraciones y casos de ransomware en Argentina. Brodersen Dark News.
  Disponible en: https://www.brodersendarknews.com/p/2023-ciberataques-ransomware-argentina-resumen
- Bleeping Computer. (2022). Conti ransomware: Analysis and de cryption tools.
  Disponible en: https://www.bleepingcomputer.com
- Bishop, M. (2019). Computer Security: Art and Science. Addison Wesley.
- CERT Argentina. (2022). Informe de Gestión CERT.ar 2022. Buenos Aires: Ministerio de Seguridad.
  Disponible en: https://www.argentina.gob.ar/noticias/informe-de-gestion-certar-2022
- CERT Argentina. (2023). Informe de Incidentes Informáticos 2023.
  Disponible en:
  https://www.argentina.gob.ar/sites/default/files/2024/05/informe_2023_del_cert.ar_.pdf
- Cadena SER. (2025, 5 de febrero). Málaga acogerá en abril la nueva edición del Congreso de Ciberseguridad de Andalucía.
  Disponible en: https://cadenaser.com/andalucia/2025/02/05/malaga-acogera-en-abril-la-nueva-edicion-del-congreso-de-ciberseguridad-de-andalucia-ser-malaga/
- Cadena SER. (2025, 19 de febrero). Fuenlabrada pone en marcha su primer Comité de Seguridad y Privacidad.
  Disponible en: https://cadenaser.com/cmadrid/2025/02/19/fuenlabrada-pone-en-marcha-su-primer-comite-de-seguridad-y-privacidad-ser-madrid-sur/

- CISA. (2021). Alert (AA21 042A) Compromise of U.S. Water Treatment Facility.
  Disponible en: https://www.cisa.gov
- Centro Criptológico Nacional (CCN CERT). (s.f.). Estrategia Nacional de Ciberseguridad.
  Disponible en: https://www.ccn-cert.cni.es
- Centro de Ciberseguridad Industrial (CCI). (2022). Informe sobre la seguridad de infraestructuras críticas en Argentina.
- CCN CERT. (s.f.). Formación y Sensibilización.
  Disponible en: https://www.ccn-cert.cni.es/nuestros-servicios/formacion-y-sensibilizacion.html
- Check Point Research. (2023). Ransomware as a Service: The Business Model Fueling Cyber Attacks.
  Disponible en: https://checkpoint.com
- Chen, X., Sacré, M., Lenzini, G., Greiff, S., Distler, V., & Sergeeva, A. (2024). The Effects of Group Discussion and Role playing Training on Self efficacy, Support seeking, and Reporting Phishing Emails: Evidence from a Mixed design Experiment.
  Disponible en: https://arxiv.org/abs/2402.11862
- CCDCOE. (2023). About CCDCOE. NATO Cooperative Cyber Defence Centre of Excellence.
  Disponible en: https://ccdcoe.org
- Czosseck, C., Ottis, R., & Talihärm, A. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism.
- Consumer Choice Center. (2019). Cómo la estrategia de ciberseguridad de Estonia puede ayudar a la UE a hacer frente a China.
  Disponible en: https://consumerchoicecenter.org
- Chequeado. (2024). Filtración de datos personales en el RE NAPER: ¿qué es y qué consecuencias puede tener?
  Disponible en: https://chequeado.com
- DataClave. (2021). RENAPER denunció ingreso indebido a su base de datos.
  Disponible en: https://www.dataclave.com.ar
- ENISA. (2023). Threat Landscape Report 2023: Sectoral and Thematic Threat Analysis. European Union Agency for Cybersecurity.
  Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- Estrategia Nacional de Ciberseguridad de España (2019).
  Disponible en:
  https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/PlanesCalidad/EstrategiaNacionalCiberseguridad2019.htm
- e-Governance Academy. (2023). About eGA.
  Disponible en: https://ega.ee

- El País. (2025). El mayor riesgo de la Inteligencia Artificial es no utilizarla, porque el enemigo sí lo va a hacer.
  Disponible en: https://elpais.com
- ENISA. (2023). Ciberamenazas Emergentes y Estrategias de Resiliencia Digital. Bruselas: Agencia de Ciberseguridad Europea.
- Forbes Argentina. (2023). Argentina sufrió 2.000 millones de intentos de ciberataques en 2023. Forbes Argentina.
  Disponible en: https://www.forbesargentina.com/innovacion/argentina-sufrio-2000-millones-intentos-ciberataques-2023-informe-n50386
- Fortinet. (2024). La importancia de desarrollar un mejor programa de concienciación sobre ciberseguridad.
  Disponible en: https://www.fortinet.com/lat/blog/business-and-technology/la-importancia-de-desarrollar-un-mejor-programa-de-concienciacion-sobre-ciberseguridad
- FDRA. (2024). Ciberseguridad: La potencia cibernética de Estonia.
  Disponible en: https://fdra.blogspot.com
- Fundación Sadosky. (s.f.). Documentos.
  Disponible en: https://fundacionsadosky.org.ar
- Fortinet. (2024). Ciberamenazas en el sector salud en América Latina.
- Forbes Argentina. (2022). El ciberataque a la Legislatura de Buenos Aires y sus consecuencias en la ciberseguridad pública.
  Disponible en: https://www.forbesargentina.com
- Forbes Argentina. (2024). Ciberataque al RENAPER: ¿Qué falló en la seguridad digital de Argentina?
  Disponible en: https://www.forbesargentina.com
- Fernández, J., & Gómez, L. (2022). Ciberseguridad y Factor Humano: Estrategias de Formación Continua.
  Madrid: Ediciones Cibernéticas.
- Gallagher, S. (2022). The HSE Ransomware Attack and its Impact on Public Health Services in Ireland.
  Journal of Information Security, 18(4), 317–329.
- Gobierno de España. (2019). Estrategia Nacional de Ciberseguridad 2019.
- Gobierno de Argentina. (2021). Segunda Estrategia Nacional de Ciberseguridad.
- Gartner. (2024). Informe sobre inversión en ciberseguridad en América Latina.
- Gutiérrez, A. (2023). Desafíos regulatorios en la protección de datos personales en Argentina.
- González, M. (2023). Educación en Ciberseguridad: Experiencias y Lecciones de España.
  Barcelona: CiberEducación.
- Hultquist, J. (2016). Sandworm Team and the Ukrainian Power Grid Attack.
  ICS CERT Monitor.
- HuffPost. (2025). España como líder en ciberseguridad en Europa.
- Hultquist, J. (2016). Análisis del ataque a la red eléctrica de Ucrania.

- Hernández, P., & Rueda, C. (2023). Políticas Públicas en Ciberseguridad: Un Enfoque Integral para América Latina.
  Bogotá: Editorial Seguridad Digital.
- ISACA. (2017). Cybersecurity Fundamentals Study Guide. ISACA.
- INDEC. (2023). Informe sobre el Empleo Público en Argentina. Instituto Nacional de Estadística y Censos
- IBM Security. (2023). Cost of a Data Breach Report 2023.
  Disponible en: https://www.ibm.com
- INCIBE. (2021). Plan Estratégico INCIBE 2021–2025.
  Disponible en: https://www.incibe.es/sites/default/files/paginas/que-hacemos/plan-estrategico-21-25-incibe.pdf
- INCIBE. (s.f.). Catálogo de Formación en Ciberseguridad.
- Infobae. (2022). Ransomware en la Legislatura de Buenos Aires: Un ataque sin precedentes.
  Disponible en: https://www.infobae.com
- INCIBE. (2023). Instituto Nacional de Ciberseguridad de España.
  Disponible en: https://www.incibe.es
- Jouini, M., Rabai, L. B. A., & Azaiez, M. N. (2014). Classification of security threats in information systems.
  Procedia Computer Science.
- Kaspersky Lab. (2023). The Evolution of DDoS Attacks in the IoT Era.
  Disponible en: https://www.kaspersky.com
- Krebs, B. (2023). Phishing Trends and Countermeasures.
  Cybersecurity Journal, 25(2), 102–119.
- KnowBe4. (2023). Phishing Simulations and Security Awareness Training.
  Disponible en: https://www.knowbe4.com
- Kumar, R., & Carthy, J. (2023). Inteligencia Artificial en Ciberseguridad: Oportunidades y Desafíos.
  Nueva York: McGraw Hill.
- La Nación. (2022). Ciberataque a la Legislatura porteña: Consecuencias y repercusiones.
  Disponible en: https://www.lanacion.com.ar
- Langner, R. (2011). Stuxnet: Dissecting a cyber weapon.
- Ley N.º 25.326. (2000). Ley de Protección de Datos Personales de Argentina.
  Boletín Oficial de la República Argentina.
- Mayer Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think.
  Houghton Mifflin Harcourt.
- Marco teórico.
- Ministerio de Asuntos Económicos y Comunicaciones de Estonia (2019). Estrategia de Ciberseguridad de Estonia.
  Disponible en: https://www.mkm.ee/en/cyber-security
- McAfee. (2022). Human Error in Cybersecurity: The Overlooked Threat.
  Disponible en: https://www.mcafee.com

- Ministerio de Asuntos Económicos y Transformación Digital. (2020). Agenda España Digital 2025.
  Disponible en: https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/Esquema_Nacional_de_Seguridad.aspx
- Ministry of Economic Affairs and Communications of Estonia. (2023). Cyber Security Strategy.
  Disponible en: https://www.mkm.ee/en/cyber-security
- NordPass. (2022). Top 200 Most Common Passwords.
  Disponible en: https://nordpass.com
- NIST. (2022). Digital Identity Guidelines. National Institute of Standards and Technology.
- NATO Cooperative Cyber Defence Centre of Excellence. (2023). Locked Shields Exercise. CCDCOE.
- National Cyber Security Index. (s.f.). Ranking - National Cyber Security Index.
  Disponible en: https://ncsi.ega.ee/ncsi-index
- OECD. (2022). Digital Security in Critical Infrastructure: Managing the Risk. Organisation for Economic Co operation and Development.
  Disponible en: https://www.oecd.org/digital/digital-security-in-critical-infrastructure-managing-the-risk.htm
- Observatorio de Ciberseguridad. (2022). El ciberataque a Estonia de 2007.
  Disponible en: https://observatoriociber.org/el-ciberataque-a-estonia-de-2007/
- Observatorio de Ciberseguridad de la Universidad de Buenos Aires (UBA). (2023). Estado de la ciberseguridad en infraestructuras críticas argentinas.
- OECD. (2024). Digitalización y Ciberseguridad en América Latina.
  París: Organización para la Cooperación y el Desarrollo Económicos.
- Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2023). Security in Computing. Pearson.
- Proofpoint. (2023). State of the Phish Report 2023.
  Disponible en: https://www.proofpoint.com
- Página/12. (2022). Impacto del ciberataque en la Legislatura de Buenos Aires.
  Disponible en: https://www.pagina12.com.ar
- Rid, T. (2022). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
- Rodríguez, A. (2023). Marco Normativo y Ciberseguridad: Desafíos y Oportunidades en Argentina.
  Buenos Aires: Universidad de Palermo.
- SANS Institute. (2022). Security Awareness Report: Managing Human Risk. SANS Security Awareness.
  Disponible en: https://www.sans.org/security-awareness-training/reports/managing-human-risk-2022/
- Sanchez, J. (2015). Privacy and Confidentiality in Information Systems: A Practical Guide. Springer.

- Schneier, B. (2022). Secrets and Lies: Digital Security in a Networked World. Wiley.
- Schreier, F. (2012). On Cyberwarfare. National Defense University Press.
- Spafford, E. H. (1989). “The Internet Worm Incident.” Communications of the ACM.
- Symantec. (2018). Lessons Learned from WannaCry and NotPetya.
  Disponible en: https://www.symantec.com
- Smartfense. (2023). El papel fundamental de la concienciación en ciberseguridad.
  Disponible en: https://smartfense.com/blog/el-papel-fundamental-de-la-concienciacion-en-ciberseguridad/
- SANS Institute. (2022). Incident Response and Threat Intelligence Training.
  Disponible en: https://www.sans.org
- Schneier, B. (2022). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
- Stallings, W., & Brown, L. (2020). Computer Security: Principles and Practice (5ta ed.). Pearson.
- Zhang-Kennedy, L., & Chiasson, S. (2022). User-Centered Security: A Usability and Human Factors Perspective. Springer.
- Salas, E. (2023). Innovación y Ciberseguridad en América Latina: Oportunidades para el Desarrollo Local.
  Lima: Fondo de Innovación Digital.
- TalTech. (2023). Master's in Cyber Security. Universidad Tecnológica de Tallin.
- Taverna, A., & Rutz, G. (2022). Aportes a la ciberdefensa y ciberseguridad para la gestión de las infraestructuras críticas en Argentina.
  Universidad de la Defensa Nacional.
  Disponible en: https://www.undef.edu.ar/libros/wp-content/uploads/2022/02/6.-TAVERNA-RUTZ.pdf
- UIT. (2021). Global Cybersecurity Index (GCI) 2020. Unión Internacional de Telecomunicaciones.
  Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
- Universidad de Jaén. (2023). Máster en Seguridad Informática.
  Disponible en: https://www.ujaen.es/estudios/master-en-seguridad-informatica
- Unión Internacional de Telecomunicaciones (UIT). (2021). Índice Global de Ciberseguridad.
- Universidad de Palermo. (s.f.). Licenciatura en Ciberseguridad.
  Disponible en: https://www.palermo.edu/ingenieria/licenciatura-en-ciberseguridad/
- Verizon. (2023). Data Breach Investigations Report 2023.
  Disponible en: https://www.verizon.com
- Vallance, K. (2022). Ciberseguridad en Estonia: Un Modelo de Resiliencia Digital.
  Tallin: Instituto de Ciberseguridad de Estonia.

- World Economic Forum. (2023). Global Cybersecurity Outlook 2023. World Economic Forum.
  Disponible en: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/
- Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security. Cengage Learning.
- Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.