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

PROYECTO

TRABAJO FINAL DE MAESTRÍA

La formación de las personas como factor crítico en la ciberseguridad.

AUTOR: ESP. LIC. ALINA SILVIA DI LERNIA

DIRECTOR: MG. ING. ALEJANDRO ECHAZÚ

Noviembre 2021

Índice

i. Resumen.

El presente trabajo final de Maestría analizará el nivel de formación general de las personas en materia de Ciberseguridad en Argentina, como uno de los ejes principales para el posicionamiento de nuestro país en el ranking de Ciberseguridad en la región y en el mundo. El análisis del estado del arte[1] en España y el estudio de nuestra realidad nos darán indicios que nos guiarán en la generación de propuestas de formación académica para profesionales de las áreas informáticas y no informáticas.

En los comienzos del siglo XXI, estamos transitando la cuarta revolución industrial, las tecnologías exponenciales van penetrando en nuestras vidas. Personas de todas las edades, desde niños hasta adultos mayores forman parte de este nuevo paradigma. Por eso, debemos estar preparados para los nuevos desafíos.

Nuevos campos de investigación en las ciencias como son la biotecnología, la nanotecnología o la neurotecnología y nuevas formas de obtener información, a través de Internet, Internet de las Cosas o la Inteligencia Artificial, enfrentan a los profesionales de todas las ramas a la necesidad de actualización para utilizar las nuevas herramientas tecnológicas en el desarrollo de sus actividades de manera segura.

En una primera instancia se definirán los perfiles de profesionales que surgen de la investigación para la formación en ciberseguridad. Luego, se definirán lineamientos para la formación en Ciberseguridad orientándonos hacia un enfoque multidisciplinario. De este modo, todos los profesionales tendrán la posibilidad de contar con herramientas, conocimientos y preparación para acompañar la evolución tecnológica.

ii. Abstract.

This final Master's work will analyze the level of general training of people in Cybersecurity in Argentina, as one of the main axes for the positioning of our country in the Cybersecurity ranking in the region and in the world. The analysis of the state of the art in Spain and the study of our reality will give us clues that will guide us in the generation of academic training proposals for professionals in the IT and non-IT areas.

At the beginning of the 21st century, we are going through the fourth industrial revolution, exponential technologies are penetrating our lives. People of all ages, from children to older adults are part of this new paradigm. Therefore, we must be prepared for new challenges.

[1] Estado del arte es un tipo de investigación documental acerca de la forma en que diferentes autores han tratado un tema específico. En otras palabras, es la búsqueda, lectura y análisis de la bibliografía encontrada en relación con un tema que se quiere investigar. (https://leo.uniandes.edu.co/images/Guias/Estadodelarte.pdf)

New fields of research in science such as biotechnology, nanotechnology or neurotechnology and new ways of obtaining information, through the Internet, Internet of Things or artificial intelligence, confront professionals of all branches with the need to update to use new technological tools in the development of their activities safely.

In the first instance, the profiles of professionals emerging from research for cybersecurity training will be defined. Then, guidelines for training in Cybersecurity will be defined, guiding us towards a multidisciplinary approach. In this way, all professionals will have the possibility of having the tools, knowledge and preparation to accompany technological evolution.

iii. Dedicatorias.

A mi hijo que siempre me acompaña, me alienta y me apoya en todos mis proyectos.

iv. Agradecimientos.

A mi Director de Tesis, Mg. Ing. Alejandro Echazú por su guía, su dedicación, por incentivarme durante el desarrollo del trabajo, por compartir conmigo sus experiencias y conocimientos y por su tiempo dedicado.

A los profesores y directivos que me acompañaron durante la maestría y el desarrollo del presente trabajo, Dr. Roberto Uzal, Ing. Carlos Amaya y Lic. Adriana Baravalle.

A todos mis compañeros de la cohorte 2018 de la Maestría en Ciberdefensa y Ciberseguridad; a todos los que participaron en la encuesta, y en especial al Sr. Subsecretarío de Ciberdefensa del Ministerio de Defensa Oscar Niss, al Sr. Comandante Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas General de Brigada Aníbal Intini, al Mg. Lic. Daniel Perles y al Sr. Juan Bosoms, que me brindaron su tiempo y permitieron que los entrevistara.

v. Abreviaturas y Acrónimos.

APT: Amenaza Persistente Avanzada

BIOS: Basic Input Output System o Sistema Básico de Entrada/Salida

CE: Consejo de la Unión Europea

CRU-IUA: Centro Regional Universitario – Instituto Universitario Aeronáutico

CSI: Computer Science Institute o Instituto de Ciencias de la Computación

CSIC: Consejo Superior de Investigaciones Científicas

CSIRT: Computer Security Incident Response Team o Equipo de Respuesta ante Incidencias de Seguridad Informáticas

CTFs: Capture The Flags o Captura las Banderas

DDOS: Distributed Denial of Service o denegación de servicio distribuido

ENISA: European Union Agency for Network and Information Security o Agencia Europea de Seguridad de las Redes y de la Información

FIE: Facultad de Ingeniería del Ejército

IDS: Intrusion Detection System o Sistema de detección de intrusiones

IEEE: Instituto Español de Estudios Estratégicos

INAP: Instituto Nacional de la Administración Pública

INCIBAR: Instituto de Ciberseguridad Argentino

INCIBE: Instituto de Nacional Ciberseguridad de España

IoT: Internet of Things o Internet de las Cosas

IP: Internet Protocol o Protocolo de Internet

IPS: Intrusion Prevention System o Sistema de Prevención de Intrusiones

ITU: International Telecommunication Union o Unión Internacional de Telecomunicaciones

LAN: Local Area Network o Red de Área Local

MAC: Media Access Control

MOOCs: Massive Open Online Courses o Cursos en línea abiertos y masivos

RDP: Remote Desktop Protocol o Protocolo de Escritorio Remoto

SDN: Software-defined Networking o Redes Definidas por Software

SOC: Security Operations Center o Centro de Operaciones de Seguridad

SQL: Structured Query Language

TI: Tecnologías de la Información

TIC: Tecnologías de la Información y la Comunicación

UE: Unión Europea

UIT: Unión Internacional de Telecomunicaciones

UNDEF: Universidad de la Defensa Nacional

VLAN: Virtual Local Area Network

VPN: Virtual Private Network o Red Privada Virtual

vi. Listado de Figuras.

1. Introducción.

A partir de los conocimientos adquiridos en las materias cursadas en la Maestría, se observó que el factor humano resulta fundamental en los aspectos relacionados con la ciberseguridad. En particular, centrándonos en los ciberataques, vimos que muchos de los casos estudiados fueron exitosos como consecuencia del accionar de las personas. Estas acciones, en muchos casos, no se llevan adelante a propósito sino por falta de conciencia o desconocimiento sobre los riesgos asociados. Además, no todas las actividades conllevan las mismas responsabilidades. Del mismo modo sucede con los conocimientos en ciberseguridad. La formación que necesitan las personas no es la misma para los que ocupan un liderazgo político/militar, mandos medios, especialistas o usuarios comunes.

Otro aspecto importante a tener en cuenta a partir del análisis de casos estudiados es la poca formación en ciberseguridad por parte de los decisores que, entre otras cosas, por ejemplo, participan en la elaboración de políticas de seguridad. Además, se observó la necesidad de formar en esta materia a un gran número de personas y brindarles los conocimientos básicos para tomar decisiones sobre qué corresponde hacer ante determinadas situaciones o cuáles son las mejores prácticas a seguir para garantizar las condiciones de integridad, confidencialidad y disponibilidad de la información de la empresa u organismo.

La necesidad de comprender el impacto de las tecnologías, sus riesgos y amenazas son temas inherentes a los profesionales de todas las ramas. Esto incluye, la necesidad de conocer hacia dónde vamos, es decir qué capacitación es necesaria ante el futuro de las tecnologías, las tendencias que imponen el Internet de las Cosas, la Inteligencia Artificial y la Robótica, entre otras.

Para ello, se analizaron detalladamente los planes de estudio de reconocidas universidades de España, como país referente en ciberseguridad, y de nuestro país poniendo el foco en la formación de las personas en la materia. Al respecto, no se observaron materias afines en carreras tradicionales o de otras áreas de conocimiento. La mayoría de las materias relacionadas con la temática sólo se dictan en carreras de Informática o Computación. Además, incluso en estos últimos casos, las materias que incluyen temáticas de ciberseguridad suelen ser optativas dentro de los planes de estudio de las carreras de grado con lo cual no todos los profesionales cuentan con esos conocimientos. De manera complementaria, se realizaron encuestas sobre la formación de las personas en ciberseguridad y entrevistas a gerentes/responsables de áereas afines para conocer sus realidades y percepciones en la temática.

A partir de los estudios realizados se establecieron los lineamientos para la actualización de los planes de estudio basados en la experiencia adquirida durante la Maestría. Como indica el informe de la Unión Internacional de Telecomunicaciones:

> La creación de capacidad humana e institucional es esencial para aumentar la conciencia, el conocimiento y el *know-how*[2] en todos los sectores, para soluciones sistemáticas y apropiadas, y para promover el desarrollo de profesionales calificados. (Global Cybersecurity Index 2018, 2019, p.9)

Entre los antecedentes sobre la formación de las personas en ciberseguridad nos encontramos con el reporte de la Unión Internacional de Telecomunicaciones sobre el estado de la ciberseguridad en la región y en el mundo, en los que se puede observar la necesidad de formación en ciberseguridad. También, destacamos algunas noticias recientes que se desencadenaron producto de fallas o debilidades humanas.

En el marco teórico, se hizo un repaso de las revoluciones industriales hasta el día de hoy, con las implicancias en la ciberseguridad de la cuarta revolución industrial, que hoy estamos atravesando. Luego, se definieron conceptos que se utilizaron durante el desarrollo del trabajo, tales como: Ciberseguridad, ciberespacio, Estrategia Nacional de Ciberseguridad, infraestructuras críticas, vulnerabilidades, amenazas, riesgos, malware, disponibilidad, integridad, confidencialidad, no repudio, autenticación, control de acceso, virus, entre otros. Después, se vieron las amenazas y vulnerabilidades a la ciberseguridad como consecuencia del accionar de las personas. Finalmente, al ser la educación un arma fundamental con la cual contar para mejorar los niveles de ciberseguridad, se revisó la importancia del papel que desempeñan las entidades educativas en ese sentido y los nuevos roles emergentes en esta nueva era.

Como parte de la educación y, de la mano del incesante avance de las tecnologías, surge la necesidad de formación continua y actualización permanente en temas de ciberseguridad. Estos aspectos se tomaron en cuenta en las propuestas realizadas y en la definición de los perfiles profesionales a los cuales esa capacitación debe ser dirigida para la gestión de la mejora continua.

En resumen, el desarrollo de este trabajo se organizó en cinco partes. En primer lugar, analizamos las ofertas de estudios de diez (10) universidades de España en relación a la ciberseguridad; en segundo lugar, hicimos lo mismo, en Argentina, analizamos las ofertas

[2] *Know-how* Proviene del inglés “Saber cómo”. Conjunto de capacidades y conocimientos que le permiten a una empresa o a una persona desarrollar una actividad o un proyecto con experiencia. (https://www.economiasimple.net/glosario/know-how)

académicas de diez (10) universidades, en relación a carreras informáticas y no informáticas; en tercer lugar, realizamos el análisis comparativo de las situaciones encontradas de España y Argentina; en cuarto lugar, a través de encuestas al público en general analizamos la situación de las personas respecto de su formación en ciberseguridad; en quinto y último lugar, por medio de entrevistas a destacados funcionarios y gerentes de áreas hicimos un repaso de la perspectiva actual en las organizaciones respecto de la formación del personal en ciberseguridad.

Con este trabajo, se espera contribuir a la mejora de los niveles de Ciberseguridad en la región y a realizar aportes para mejorar el posicionamiento de nuestro país a nivel global, y en consecuencia la mirada que tienen las demás naciones sobre nosotros.

2. Planteamiento del Problema de Investigación.

2.1 Antecedentes.

Muy a menudo leemos noticias sobre distintos ataques que afectan a la ciberseguridad en empresas, organismos de Estado o a particulares. Algunos dados a conocer en los últimos años se resumen a continuación.

Hacia mediados de 2020, la red social Twitter fue atacada producto de la ingeniería social de la que fueron víctimas algunos empleados con acceso a sistemas y herramientas internas. Se secuestraron cuentas tales como la del ex presidente Barack Obama, el candidato por entonces, Joe Biden, entre otros famosos. Desde esas cuentas se prometía regalar criptomonedas a quienes donaran dinero para paliar las consecuencias del Covid-19. Antes de frenar la emisión de esos mensajes falsos, ya se habían robado más de $100.000 dólares. (Ochoa, 2020)

Según informó el diario La Nación a fines de agosto de 2020, el Ministerio del Interior sufrió un ciberataque del ransomware llamado Netwalker, que afectó el funcionamiento del Sistema Integral de Captura Migratoria, que opera en los pasos internacionales durante 3 horas. Se ocasionaron demoras en los ingresos y egresos al país. Los delincuentes pedían 4 millones de dólares por la obtención de las claves de acceso para el rescate de la información encriptada. El Ministerio del Interior optó por no pagar y denunció el incidente ante la Justicia. Cuando el plazo venció, los atacantes subieron un total de 1.8 GB de información a la Deep Web.

En marzo de 2021, se dio a conocer una noticia sobre un caso de phishing que suplantaba la identidad de la Dirección General de Tráfico de España. Se enviaba un correo electrónico con una multa al usuario, supuestamente pendiente de pago. Con la notificación llegaba un link con un acceso a una sede electrónica falsa. Si la persona hacía clic en ese

acceso, se iniciaba la descarga de un archivo con malware cuya intención era recopilar datos personales de todo tipo. (Higuera, 2021)

En abril de 2021 la compañía Apple fue afectada por un ataque de *ransomware*. Los atacantes se robaron imágenes de diseños de computadoras y otros dispositivos que produce la empresa y pedían USD 50 millones por el rescate de la información robada. Aunque en este caso, la empresa no especificó cómo lograron insertar el malware, se conoce que "más del 80% de los ataques de ransomware exitosos se llevaron adelante logrando vulnerar la red mediante ataques de fuerza bruta a las credenciales del RDP". El *Remote Desktop Protocol* (RDP), es el protocolo de escritorio remoto en auge en estos tiempos utilizado para el trabajo remoto. (Jaimovich, 2021)

Como vimos, parte de los ataques informáticos logran su cometido porque se aprovechan de la confianza y el desconocimiento o desacierto de las personas, por tal motivo se deben tomar diversas medidas preventivas. Sin embargo, el elemento fundamental en esta cadena es la capacitación constante de las personas. De aquí surge el eje central de este trabajo: La formación de las personas como factor crítico en la ciberseguridad.

La ciberseguridad tiene un campo de aplicación transversal a todas las industrias y sectores. Para ello, todos deben trabajar en incrementar el desarrollo de capacidades. La policía, los departamentos de justicia, las instituciones educativas, los ministerios, los operadores del sector privado, los desarrolladores de tecnología y las asociaciones público-privadas, deben visibilizar el mismo el objetivo y aumentar los esfuerzos en la adopción e integración de la ciberseguridad a nivel global. La Unión Internacional de Telecomunicaciones publica un informe periódicamente sobre el posicionamiento de los países en materia de ciberseguridad. El listado de los países se encuentra ordenado en base al índice global de ciberseguridad, el cual mide el nivel de preparación y compromiso de los países con la ciberseguridad a nivel global. No es objetivo de este índice medir el detalle de sus capacidades ni sus posibles vulnerabilidades. La obtención del índice se basa en cinco pilares o medidas: legales, técnicas, organizacionales, de desarrollo de capacidades y cooperación. En particular, vamos a centrarnos en uno de los pilares que son nuestra materia de investigación: las medidas de desarrollo de capacidades. Las mismas se construyen a partir de indicadores sobre la existencia de proyectos de investigación y desarrollo en ciberseguridad; programas de educación o capacitación académica en ciberseguridad; campañas públicas de concientización; marco para la certificación de profesionales en ciberseguridad; cursos de capacitación profesional en Ciberseguridad; mecanismos de incentivos; y agencias del sector público que fomenten el desarrollo de capacidades. En el

último informe, publicado en Ginebra, Suiza en 2021, Argentina ocupa el puesto número 91 a nivel global y 13 en la región de América, como se puede observar en las figuras 1 y 2 respectivamente. Cabe señalar, que Argentina ascendió tres posiciones desde el último informe de la ITU en 2018 a nivel global, sin embargo, descendió dos posiciones a nivel regional.

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

Country Name	Score	Rank
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

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

Figura 1. Ranking Índice Global de Ciberseguridad
Fuente: Índice Global de Ciberseguridad 2020 – ITU

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 – ITU

2.2 Problema de Investigación.

Al analizar las ofertas académicas notamos que la capacitación en temas atinentes a la ciberseguridad está acotada a profesionales, la mayoría pertenecientes a ramas informáticas y se brinda a través de algún tipo de formación de grado o posgrado especializado en estos temas. Además, los contenidos de los planes de estudio vigentes en carreras de grado en Argentina son insuficientes en lo relativo a la ciberseguridad.

La concientización y la formación en ciberseguridad no están orientadas hacia el resto de la población. Los conocimientos de las personas no especializadas en las ramas informáticas e incluso las de las no especializadas en ciberdefensa o ciberseguridad resultan escasos en el tema. No son concientes de los riesgos y amenazas a los que pueden estar expuestas en su accionar diario en el uso de las tecnologías y el tratamiento a seguir sobre los mismos.

Como resultante, la formación académica disponible en nuestro país en materia de ciberseguridad resulta inadecuada para las necesidades de la revolución tecnológica que nos atraviesa.

2.3 Justificación de la Importancia.

Una formación académica de calidad en nuestro país en materia de ciberseguridad permitirá reforzar los conocimientos de los profesionales de todas las ramas, adecuarlos y actualizarlos para atravesar con solvencia las disparidades a las que los enfrente la industria 4.0.

La investigación contribuye a nivel local mediante la realización de aportes para la actualización de los planes de estudio de las carreras de grado vigentes en nuestro país. Por otro lado, atento a la relevancia que se da a la capacitación en materia de ciberseguridad, en la medición de los niveles de ciberseguridad de los países en el mundo, esta investigación realizará aportes para un mejor posicionamiento a nivel global dentro de la escala de ciberseguridad.

De manera, adyacente, los profesionales de todas las áreas del conocimiento que formen parte de esta nueva propuesta y reciban esta capacitación actualizada se verán beneficiados al momento de tomar decisiones e incluso a nivel operativo. De este modo, podrán contar con las herramientas adecuadas para enfrentar los problemas de ciberseguridad que puedan surgirles en la realización de sus actividades diarias, las que hoy en día se gestionan a través de medios electrónicos, desde aquellas en el campo de las finanzas hasta las relacionadas con la salud, todas pueden verse afectadas por temas de ciberseguridad.

2.4 Objetivo General.

El objetivo general es realizar aportes en la capacitación de las personas que incluyan a la ciberseguridad dentro de la oferta educativa, para tener organizaciones más seguras a fin de mejorar el posicionamiento del país sobre el tema.

2.5 Objetivos Específicos.

Los objetivos específicos a cumplir son:

- 2.5.1 Investigar las ofertas de formación en España en materia de ciberseguridad para contar con un marco de referencia a seguir;
- 2.5.2 Explorar las ofertas de formación en materia de ciberseguridad para evaluar el estado de situación actual en nuestro país;
- 2.5.3 Definir perfiles de profesionales que surjan a partir del análisis de los conocimientos que se posee en materia de ciber para presentar propuestas que mejoren la situación;
- 2.5.4 Proponer lineamientos en la formación de ciberseguridad con un enfoque multidisciplinario para que los nuevos profesionales cuenten con los conocimientos necesarios a fin de generar un entorno ciberseguro.

2.6 Metodología Empleada.

El trabajo constará de un diseño metodológico descriptivo y explorativo. Se investigará sobre ataques informáticos resultantes de la falta de capacitación de los individuos. Se analizarán los datos del informe elaborado por la ITU sobre el índice global de ciberseguridad. También incluye un análisis de la capacitación en ciberseguridad en Argentina y en España.

Se utilizará el método cuantitativo. Se realizarán encuestas para la recopilación de datos y entrevistas a personas referentes en materia de ciberseguridad. Posteriormente, a partir de un diagnóstico se conformarán los perfiles profesionales a formar en ciberseguridad y las propuestas de adecuación de los planes de estudio para las carreras universitarias.

3. Marco Teórico.

3.1 Conceptos de Ciberseguridad.

Comenzamos por el eje central del trabajo, la ciberseguridad, sobre la que encontramos varias definiciones. Vamos a tomar en consideración la expresada por la Unión Internacional de Telecomunicaciones:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de

> riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad. (Recomendación UIT-T X.1205 (04/2008), 2009)

En el mes de mayo de 2019, mediante Resolución 829 de 2019 [Secretaría de Gobierno de Modernización] en el ámbito de la Jefatura de Gabinete de Ministros se aprobó la Estrategia Nacional de Ciberseguridad de la República Argentina. Uno de los principios rectores de la ciberseguridad hace referencia a la cultura de ciberseguridad y la responsabilidad compartida en donde se expresa que "El Estado Nacional debe promover la generación de una cultura de ciberseguridad". (Anexo I, p.5)

El presente trabajo realizará aportes para el cumplimiento del segundo objetivo planteado en la Estrategia Nacional de Ciberseguridad que trata sobre la capacitación y educación en el uso seguro del ciberespacio, lo que se entiende como "El proceso de formación y adquisición de conocimientos, aptitudes y habilidades necesarias para un uso seguro del Ciberespacio". (Resolución 829 de 2019 [Secretaría de Gobierno de Modernización], Anexo I, p.5).

El ciberespacio es el lugar virtual en donde se desarrollan nuestras actividades cibernéticas, en la Estrategia Nacional de Ciberseguridad (2019) se define como:

> El dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones, tiene entre otras, como características esenciales, su dimensión global y transfronteriza, su naturaleza dual, su masividad y su vertiginosa y constante evolución. (Resolución 829 de 2019 [Secretaría de Gobierno de Modernización], Anexo I, p.2).

A diario utilizamos servicios a los cuales accedemos de manera automatizada en nuestras vidas como son la luz, el gas, el agua e incluso la televisión o internet sin darnos

cuenta que provienen de medios tales como centrales eléctricas o nucleares, sistema de aguas, tecnologías satelitales, o sistemas de telecomunicaciones. Estas son las denominadas infraestructuras críticas, Dentro del ámbito de la Ciberseguridad, la Directiva del Consejo de la Unión Europea 2008/114/CE del 8 de diciembre de 2008, las define como:

> El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones.

Entre los conceptos que se desarrollan en el estudio de la ciberseguridad encontramos las vulnerabilidades y las amenazas. Una vulnerabiliad es una debilidad de software o hardware a través de la cual un intruso puede ganar acceso y escalar dentro de un sistema o red. Esta debilidad también puede provocarse por la ausencia de procedimientos de seguridad, o controles que permitan explotar una amenaza. Una amenaza es una acción dirigida sobre objetos tangibles o intangibles como servidores, clientes, canales de comunicación, archivos o información. (Kizza, 2017)

En conjunción con las vulnerabilidades y las amenazas encontramos a los riesgos, es decir, la "combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto" (Resolución 781 de 2015 [Ministerio de Defensa], Anexo I, p.14).

Otro término a conocer cuando hablamos de ciberseguridad, es el malware. Este proviene de la combinación de las palabras en inglés *malicious software*. Se trata de un programa con código que puede resultar dañino para el sistema o para un usuario. Diariamente crece el número de amenazas, al mismo tiempo, las herramientas con las que cuentan los hackers se vuelven más sofisticadas. El tiempo desde que se anuncia una vulnerabilidad hasta que es desplegada es cada vez más corto. Tradicionalmente se define a la seguridad como al proceso de prevenir accesos no autorizados, uso, alteración, robo, o daño físico a un objeto al mantener alta confidencialidad, integridad y disponibilidad de la información sobre el mismo. Un objeto puede ser tangible, como un servidor o intangible como la información que se transporta a través de los canales de comunicación. Más allá de su condición, es decir si es o no tangible, un objeto se encuentra en un estado seguro si el proceso logra mantener su valor intrínseco elevado bajo cualquier tipo de condiciones, sean producidas por factores internos o externos. (Kizza, 2017).

El estado de la ciberseguridad lo vamos a medir en función de las condiciones presentes en los principios básicos tales como disponibilidad, integridad, confidencialidad, no repudio, autenticación y control de acceso.

La disponibilidad "indica la característica o propiedad mediante la cual la información o cualquier recurso relacionado, permanece accesible y disponible para su uso cuando una entidad autorizada así lo requiera". (Resolución 781 de 2015 [Ministerio de Defensa], Anexo I, p.12).

La integridad es la propiedad a través de la cual se asegura que los datos en tránsito no son alterados. Mediante encriptación y algoritmos de hashing podemos asegurar la información de posibles amenazas cuando es enviada del emisor al receptor. Las funciones hash se utilizan para firmar los mensajes, de manera similar a una huella dactilar y permiten proveer integridad y autenticidad a los mismos. (Kizza, 2017)

La confidencialidad es la propiedad a través de la cual se asegura la no exposición o divulgación no autorizada de datos o información. A través de algoritmos de encriptación podemos proteger la información cuando viaja de un extremo a otro en la red, a través de canales no confiables. De este modo, la protegeremos de ataques como man in de middle o sniffers. Man in the middle es un tipo de ataque en donde se intercepta la información que está viajando de un extremo a otro con la capacidad de leerla y modificarla a voluntad. Sniffers son programas instalados en el canal de comunicación que se encargan de examinar todo lo que pasa a través de él, son fáciles de escribir y difíciles de detectar. (Kizza, 2017)

No repudio es la propiedad a través de la cual se prueba el origen y entrega de un servicio o información. Muchas veces en el mundo digital, el destinatario puede negar haber recibido información, sin embargo, hay mecanismos como la firma digital y algoritmos de encriptación para asegurar el no repudio. Se trata de mecanismos criptográficos equivalentes a la firma ológrafa, la cual puede ser verificada por una tercera parte en cualquier momento. (Kizza, 2017)

La autenticación es la capacidad de identificación de los usuarios legítimos. Se basa en algo que la persona sabe o tiene. Para verificar que una persona es quien dice ser, se suelen utilizar nombre de usuario, password, imagen de retina, huellas dactilares, tarjetas de identificación y ubicación física, como puede ser la dirección IP[3] del cliente. Además, las distintas modalidades se pueden usar de forma combinada. (Kizza, 2017)

[3] Dirección IP significa dirección del Protocolo de Internet. Este protocolo es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de video o la conexión a un sitio web. Una dirección IP identifica una red o dispositivo en Internet. (https://www.avast.com/es-es/c-what-is-an-ip-address)

El control de acceso permite determinar quién usa cada uno de los servicios. Puede realizarse a través de herramientas de hardware o software. Entre las primeras encontramos terminales de acceso, monitoreo visual de eventos, tarjetas de identificación, identificación biométrica y video vigilancia. Entre las de software, monitoreo de puntos de acceso y monitoreo remoto. Muchos de ellos se utilizan en forma combinada con alguna información que el usuario conoce o posee tal como una password. (Kizza, 2017)

Las amenazas pueden materializarse principalmente a través de virus o gusanos. Un virus es un programa de computación con código malicioso que tiene la capacidad de propagarse en el sistema y aún más allá de él. Hoy en día, son cada vez más fáciles de codificar, dadas las facilidades que ofrecen los nuevos lenguajes de programación, incluso muchos de ellos se pueden encontrar disponibles para su uso en Internet. Además, el grado de interconexión global de computadoras, hace que la velocidad de propagación sea realmente muy rápida. Al ejecutarse un virus, ataca los recursos del sistema, como pueden ser software, datos o hardware, debilitando la capacidad para realizar funciones hasta poder llegar a dejar el sistema fuera de uso. (Kizza, 2017)

Existen diversos tipos de virus, entre los que encontramos a los residentes en memoria, generadores de errores, destructores de programas, destructores de sistemas, destructores de hardware, ladrones de tiempo, troyanos, bombas de tiempo, trampas (del inglés, *trapdoors*) y engaños (del inglés, *hoaxes*). Los virus residentes en memoria son los más difíciles de detectar y se suelen utilizar para atacar la parte central del almacenamiento de un sistema. Los generadores de errores se alojan en código ejecutable, entonces cada vez que el software se ejecuta generan un error que puede variar desde lo más simple hasta el apagado del sistema. En el caso de los destructores de programas, se trata de virus que se adjuntan a un software y lo utilizan como conductor para propagarse pudiendo dañar, es decir, alterar, borrar o destruir, todo lo que esté en contacto con ese software, ya sean datos u otro software. Los destructores de sistemas pueden afectar sistemas operativos, compiladores, o software similar que se utiliza en programación. Los ladrones de tiempo, "roban" el tiempo del sistema, de este modo logran obtiener control total como si fueran un superusuario con acceso a todos los recursos del sistema. Los destructores de hardware son virus embebidos dentro del bios[4] o controladores de dispositivos[5], pueden producir

[4] El bios (Sistema Básico de Entrada/Salida) es un software almacenado en el chip en la placa madre de una computadora cuya función es inicializar y comprobar todos los componentes de hardware durante el arranque de la máquina. También prepara el equipo para que el Sistema Operativo se cargue y se ejecute.

[5] Controladores de dispositivos son los programas que se instalan en una computadora para poder utilizar un cierto dispositivo e interactuar con él a través de una interfaz.

alteraciones que resulten en daños físicos, como por ejemplo bloquear teclados o mouses, o roturas de discos rígidos. Los troyanos, son virus basados en la leyenda del Caballo de Troya, en donde programas confiables esconden algún tipo de virus. Las bombas de tiempo son virus cronometrados que se encuentran inactivos y se disparan cuando sucede un evento, generalmente determinado por una fecha, como por ejemplo el día de San Valentín. Los *trapdoors,* también conocidos como puertas trampa o puertas traseras, son en realidad una herramienta utilizada por hackers para introducir virus en el sistema. Se trata de puntos secretos que permiten el acceso al sistema, muchas veces producidos intencionalmente por los desarrolladores del software para permitirles el ingreso en futuras actualizaciones, sin embargo, pueden ser aprovechados por personas malintencionadas para producir daño. Por último, los *hoaxes* son virus a modo de broma que pueden producir algún disturbio, pero no suelen ser dañinos. (Kizza, 2017)

Los gusanos son muy similares a los virus respecto de sus propiedades, ambos pueden realizar ataques automatizados, autoreplicarse en nuevas copias a medida que se propagan, y ambos pueden dañar cualquier recurso que ataquen. La principal diferencia es que los virus se encuentran escondidos, embebidos dentro de otros programas, en cambio los gusanos son programas que están solos. (Kizza, 2017)

Los spywares o keyloggers son programas maliciosos o incluso en algunos casos puede tratarse de hardware que de algún modo fue instalado sin el consentimiento del usuario. Se ocupa de robar información confidencial como claves o números de tarjetas de crédito, para luego enviarlas a otro sitio remoto. (Arano Chávez, Beltrán y Escudero Macluf, 2016)

Un adware es un tipo de programa publicitario. Su nombre surge de la combinación de las palabras en inglés *ad*, proveniente de advertising, que en castellano significa publicidad, y *ware*, en relación a software. Puede utilizarse para mostrar publicidades o para recopilar información personal. Pueden ser maliciosos o cumplir funciones espías. En estos casos, se instalan en la computadora o celular sin el consentimiento de la persona cuando se instalan aplicaciones gratuitas, al ingresar a sitios web infectados o al instalar extensiones en el navegador (https://www.argentina.gob.ar/justicia).

Venganza, logros personales, odio, diversión, pueden ser algunas de las motivaciones que provocan las amenazas a la ciberseguridad. Más alla de cuáles sean los objetivos, los hackers cuentan con una diversidad de técnicas para tratar de alcanzarlos. Entre ellas podemos destacar: Ingeniería social, impersonalización, *exploits*, *scripts* de ataque de datos,

debilidades en la infraestructura, denegación de servicios distribuído, fuerza bruta, escuchas activas, web defacement, inyección SQL.

La ingeniería social es una técnica mediante la cual, a través de manejos psicológicos, se consigue información confidencial como ser claves de acceso a algún sistema, de usuarios reales. Se puede ejecutar de manera indirecta o directa. Indirecta es por búsqueda de información tirada en contenedores de basura o por correo postal a través de la intercepción de la dirección de la víctima. De manera directa, puede ser a través de distintos medios: Vía telefónica, online, en persona, o mediante la suplantación de identidad. Cualquiera de estas modalidades, el atacante logra engañar a la víctima, haciéndose pasar por otra persona, por una autoridad, o ganándose su confianza para sonsacar información confidencial. (Kizza, 2017)

La impersonalización es el robo de derechos de acceso de usuarios autorizados. Los atacantes pueden, por ejemplo, capturar las credenciales de una sesión de usuario, y luego loguearse como un usuario legítimo, y realizar acciones en nombre de la víctima. (Kizza, 2017)

Cuando un software se pone en producción, es probable que por falta de testeos o por las corridas de los desarrolladores y administradores para lanzar el producto, se produzcan descuidos y queden expuestos agujeros de seguridad, a través de los cuales los hackers puedan ingresar. De esto se tratan los exploits. Pueden darse en cualquier tipo de software, incluso en sistemas operativos. (Kizza, 2017)

Los scripts son porciones de código de programación, que se ejecutan de forma secuencial. Generalmente se utilizan para controlar el comportamiento de un programa o interactuar con el sistema operativo. Pueden ejecutarse en servidores o en los equipos clientes, lugar por donde permitiría introducir código malicioso en el sistema. (Kizza, 2017)

Un tipo de script malicioso es el conocido como cross-site-scripting, tiene la habilidad de moverse entre computadoras de Internet visitando servidores en donde alojan esos scripts. Pueden aparecer a través del uso de formularios web interactivos de sitios desconocidos, posteos de grupos o foros, links de páginas web o mensajes de mails. (Kizza, 2017)

Las debilidades en la infraestructura suelen encontrarse en los protocolos de comunicación. Cuando se encuentra un agujero de seguridad, seguramente el fabricante lanza al mercado inmediatamente un parche, es decir una actualización del software que corrije el problema. Sin embargo, muchas veces sucede que los administradores no lo instalan inmediatamente. Esto da lugar a los hackers, que se ocupan de husmear las redes en

búsqueda de estas fallas, a conseguir ingresar a un sistema, incluso aprovechándose de una vulnerabilidad ya conocida. (Kizza, 2017)

En relación a esto, se encuentra el concepto de vulnerabilidad de día cero o zero day. Cuando se desarrolla un software, muchas veces presenta debilidades de seguridad producto de fallas en el diseño, omisión de los requisitos mínimos de seguridad de la información o construcción de la aplicación a través del uso de funciones, métodos y procedimientos débiles del lenguaje de programación elegido en el proyecto. Además, suele suceder que el desarrollo de aplicaciones es una carrera contra el tiempo para sacar nuevos productos o versiones al mercado. Todo esto más la falta de entrenamiento en desarrollo seguro garantiza la presencia de *bugs* o fallos en el código de programación de las aplicaciones. Estas vulnerabilidades posibles de ser explotadas por malintencionados son las conocidas como vulnerabilidades de día cero, es decir, cuando son recién descubiertas y no existe ninguna contramedida para reducir el riesgo que representan. En este momento es cuando los hackers se aprovechan para comercializarlas. Luego se desarrolla y publica el parche, entonces pasa a ser una vulnerabilidad común. (Santiago y Allende, 2017)

El ataque de denegación de servicios distribuido (DDOS) tiene como objetivo dejar un recurso o servidor inoperativo. Para ello, se requiere de varios equipos que trabajan en forma coordinada enviando peticiones masivas a un servidor. De este modo, logran saturar ese servicio y colapsarlo. Los equipos utilizados para lanzar la DDoS forman parte de una botnet o red de zombies que el atacante controla de manera remota sin que los propietarios lo sepan. (Ciberseguridad en la identidad digital y la reputación online: Una guía de aproximación para el empresario, 2016)

Los ataques de fuerza bruta, son aquellos que utilizan esta técnica para ejecutar el robo de contraseñas en Internet. No se requiere de grandes conocimientos, dado que, generalmente, se realiza de forma automatizada a través de programas, muchos de los cuales ya existen. (Arano Chávez, Beltrán y Escudero Macluf, 2016)

Finalmente, las escuchas activas son un riesgo directo para la confidencialidad de los datos. Se producen al interceptar paquetes de datos las redes de comunicaciones. Puede suceder de dos formas, que se modifique el contenido de ese paquete como por ejemplo la IP de destino o el número de secuencia o que, simplemente se copie su contenido para luego utilizarlo para el escaneo de la red. (Kizza, 2017)

Una de las formas de hacktivismo es el web *defacement*. Los hacktivistas ganan el acceso, penetran el servidor web y reemplazan el contenido y los vínculos del sitio seleccionado con lo que quieran que vean los espectadores. Suelen dar mensajes políticos,

sociales o económicos. Algo similar sucede cuando los piratas logran cambiar el servidor de nombres de dominio para que se resuelva en una dirección IP cuidadosamente seleccionada de un sitio donde tienen el contenido que quieren que los espectadores vean. (Kizza, 2017)

Un ataque de inyección SQL[6] es la utilización de una técnica mediante la cual se inserta código SQL en un campo de entrada de datos para que se ejecute. Esta sentencia se ejecutará directamente contra la base de datos permitiendo robar, modificar, o hasta destruir datos sensibles; elevar los privilegios para llegar a la aplicación, base de datos o incluso sistema operativo o; actuar como pivote desde una base de datos comprometida para atacar otro sistema dentro de la misma red. Estos problemas pueden evitarse mediante una apropiada codificación de las aplicaciones web. (https://security.berkeley.edu)

Gracias al uso abusivo de las redes, actualmente podemos observar otro tipo de amenazas o malos tratos.

El ciberbullying es el maltrato que se le realiza a un menor de edad a través de Internet u otros medios electrónicos como telefonía móvil, correo electrónico, mensajería instantánea, redes sociales, juegos online, etc. Las amenazas o humillaciones las realiza otro menor de edad mediante la publicación de textos, imágenes, videos o audios (https://www.argentina.gob.ar/justicia).

Dentro de las amenazas a través de medios electrónicos también están las conductas llamadas sextorsiones, la que se dan cuando se chantajea a una persona con divulgar y hacer públicas imágenes o videos de su intimidad sexual a través de redes sociales, mail o whatsapp (https://www.argentina.gob.ar/noticias).

El grooming es el acoso sexual hecho por un adulto a un niño, niña o adolescente por medio de internet o u otros medios electrónicos (https://www.argentina.gob.ar/justicia).

A continuación, se definen otros términos específicos relacionados a la ciberseguridad: Hacking ético; internet de las cosas; inteligencia artificial; VPN; algoritmos criptográficos; firma digital; blockchain; IDS; IPS y sistemas de gestión de identidades.

El hacking ético se trata de realizar pruebas de intrusión o pentest para comprobar la existencia de vulnerabilidades en un sistema o infraestructura. A partir del informe resultante se podrá tomar una determinación sobre qué hacer con cada uno de los fallos encontrados a fin de mitigarlos y evitar fugas de información y ataques informáticos. (Rodriguez Llerena, 2020)

[6] SQL es un lenguaje de alto nivel utilizado para la administración de bases de datos. (https://www.universidadviu.com/es/actualidad/nuestros-expertos/programacion-sql-para-que-sirve-y-quien-la-necesita)

El Internet de las cosas (IoT) se trata de un entorno inteligente que se construye a partir de la conectividad con la que cuentan una variedad de objetos grandes y pequeños que les permite lograr una red de comunicación interconectada. Estos objetos son dispositivos o nodos cotidianos como pueden ser dispositivos móviles, heladeras, televisores, lavavajillas, lavarropas, abre-puertas, entre una gran variedad. Estos cuentan con sensores que permiten compartir información a través de plataformas y frameworks[7] unificados. (Kizza, 2017)

La inteligencia artificial "es la ciencia de construir máquinas para que hagan cosas que requerirían inteligencia si las hicieran los humanos" (Marvin Minsky, s.f.). Sus áreas de aplicación son muchas. Entre ellas se destacan el aprendizaje, la modelización de conductas para luego la implantación en computadoras, como es el caso de filtrado de contenidos, por ejemplo. Se utiliza también en robótica, en aplicaciones que realizan traducciones de idiomas, y en sistemas expertos, en donde la experiencia del personal calificado se incorpora a los sistemas para permitir alcanzar deducciones más cercanas a la realidad. (Alfonso Galipienso, Cazorla Quevedo, Colomina Pardo, Escolano Ruiz y Lozano Ortega, 2003)

Una VPN es una red privada virtual que hace uso de la infraestructura pública de comunicaciones, como es Internet, y le agrega seguridad al canal de comunicación. Los procedimientos de seguridad incluyen encripción los que se logran a través del protocolo de tunelización. Este permite crear un túnel entre dos puntos y transmitir datos de forma segura por un canal inseguro. Adicionalmente, como una variación al concepto de VPN, se encuentran las VLANs o virtual LAN, se trata de un grupo de dispositivos conectados lógicamente en una red o más configuradas para que pueden comunicarse como si estuvieran conectados a un mismo cable. (Kizza, 2017)

Los algoritmos criptográficos son algoritmos matemáticos combinados con claves que permiten convertir un determinado conjunto de códigos o caracteres comprensibles en otro de difícil interpretación. Las características del algoritmo en conjunción con la longitud de la clave determinarán el nivel de dificultad con las que se encontrará un intruso para poder descifrar o interpretar el mensaje resultante. (Corletti Estrada, 2011)

La firma digital es la técnica utilizada para establecer la autenticidad e integridad de los mensajes y asegurar el no repudio por parte de los usuarios. Se trata de un digesto encriptado por una clave privada que se adosa a un documento, lo que resulta análogo a la firma ológrafa. Un certificado digital es un mensaje firmado digitalmente que se utiliza para

[7] Framework es un entorno de trabajo que ofrece una estructura para el desarrollo cuyo objetivo es facilitar la labor de programación ofreciendo una serie de características y funciones que aceleran el proceso, reducen los errores y favorecen el trabajo colaborativo. (https://www.seoestudios.es/blog/que-es-un-framework/)

dar fe de la validez de la clave pública de un elemento comunicante. En las comunicaciones, los certificados se utilizan para brindar seguridad a las mismas. El cliente envía peticiones, el servidor envía al cliente la clave pública en un certificado digital firmado por una autoridad certificante, entonces el cliente puede validar la firma digital. (Kizza, 2017)

Blockchain es una tecnología diseñada para administrar un registro de datos online, en donde, en lugar de tener información centralizada en una sola computadora y con unos pocos usuarios con capacidad de modificarla, una cadena de bloques está replicada a lo largo de toda una serie de computadoras bajo un modelo de red de pares, que agregan datos solo a partir del acuerdo entre las partes. En una red centralizada, un ataque a un nodo podría poner en riesgo a toda la estructura, en cambio, en una plataforma distribuida la estructura es más confiable y podría no verse afectada si una de las partes se comprometiera (https://bfa.ar).

Las redes de computadoras están hechas bajo tres principios: prevención, detección y respuesta. Sin embargo, la mayoría de los recursos de seguridad están dedicados a la detección y prevención ya que si estamos en capacidad de detectar y prevenir todas las amenazas no hará falta dar respuestas. En este sentido, encontramos los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS). El primero se encarga de detectar accesos no autorizados a un sistema o a una red, mientras que el segundo, se ocupa de prevenir los accesos no autorizados, es decir que, además, los filtra. (Kizza, 2017)

Un sistema de gestión de identidades se utiliza para garantizar que sólo los usuarios autenticados y autorizados tengan acceso a los recursos de red o sistemas particulares. Este proceso se puede automatizar y ser auto-gestionable por parte de los usuarios, cuando, por ejemplo, pueden restablecer sus propias contraseñas. En la gestión de identidades se pueden utilizar uno o múltiples factores de autenticación. Estos factores pueden ser: algo que uno sabe, como puede ser una contraseña; algo que uno tiene, como es el caso de un token; algo que uno es, en el caso de utilizar biometría; el lugar donde uno está (dirección IP o MAC[8]); o algo que uno hace (comportamiento). (Palomares, 2017)

3.2 La Ciberseguridad en la Cuarta Revolución Industrial.

A partir de la segunda mitad del siglo XVIII comenzaron a darse una serie de transformaciones en los aspectos económicos y sociales, sobre todo en las actividades

[8] Una dirección MAC es la identificación única que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, sean computadoras, routers, impresoras u otros dispositivos. (https://www.xataka.com/basics/que-es-la-direccion-mac-de-tu-ordenador-del-movil-o-de-cualquier-dispositivo)

industriales. De allí surge el concepto de revolución industrial. El cambio de la energía muscular a la mecánica desencadena la primera revolución industrial, la que abarcó desde aproximadamente 1760 hasta más o menos 1840, con la construcción del ferrocarril y la invención del motor de vapor entre los grandes hitos. Luego, hacia finales de siglo XIX y principios de siglo XX, nuevos hallazgos dan cuenta de una nueva y segunda revolución industrial. A partir de la electricidad como gran innovación, surgen otros descubrimientos para la industria, el transporte, las comunicaciones y el ocio: la cadena de montaje, la lamparita, el telégrafo, el automóvil, el teléfono, la radio, el aeroplano, el ferrocarril eléctrico y el cinematógrafo. Hacia la década de 1960, con el desarrollo de los semiconductores y el surgimiento de los primeros ordenadores, comienza una transformación digital, conocida como tercera revolución industrial. Estos cambios continúan en las siguientes décadas, hacia 1970 y 1980 aparecen las primeras computadoras personales y hacia 1990, surge Internet. (Schwab, 2016)

Desde comienzos del siglo XXI estamos transitando una nueva transformación, que nos lleva a un mundo globalizado, sin fronteras: La cuarta revolución industrial. Con la transformación digital los cambios comenzaron a aumentar de manera exponencial. Hacia 1985, Internet tenía menos de 2000 computadoras conectadas, para saltar a 109 billones hacia 2001, con una tasa estimada de 51% anual. Cada vez son más los usuarios conectados a Internet y con ellos, crecen los servicios, las amenazas y las responsabilidades. Desde los comienzos del nuevo siglo, la interdependencia entre las personas y las computadoras ha crecido enormemente, incluso para las naciones enteras que se encuentran con la necesidad de proteger la información almacenada en esa red, de nuevas amenazas, hasta ahora inexistentes, con las que tendrán que lidiar. (Kizza, 2017)

En la cuarta revolución industrial está cambiando la magnitud y la índole de los conflictos. Antes se distinguía claramente la diferencia entre la guerra y la paz y los combatientes usaban técnicas bélicas en los ataques. Ahora los conflictos se tornan cada vez más híbridos y los actores dejan de ser sólo estatales y pueden pasar a ser individuos con ganas de dañar a otros, lo cual les puede resultar mucho más fácil con la tecnología al alcance de las manos. Como afirma Schwab (2016) “El ciberespacio se está convirtiendo en un sitio de enfrentamiento tanto como la tierra, el mar y el aire lo eran en el pasado”.

Los conflictos en el ciberespacio pueden producirse a partir de ataques a infraestructuras críticas, espionaje o actos delictivos. Cualquier red o dispositivo conectado a Internet, es plausible de ciberataques. También podemos hablar de una guerra autónoma o

automatizada, con el despliegue de robots, vehículos autónomos, satélites, submarinos no tripulados capaces de actuar en el mar o en el espacio. (Schwab, 2016)

Entre las tecnologías emergentes en la cuarta revolución industrial que están transformando la seguridad internacional podemos distinguir: drones; armas autónomas, dirigidas por medio de la inteligencia artificial; satélites y armas planeadoras hipersónicas utilizados para la militarización del espacio; wearables o dispositivos portátiles, electrónicos e inteligentes utilizados por ejemplo para optimizar la salud, lo que podría mejorar el rendimiento de los soldados; manufactura aditiva de piezas a partir de diseños digitales como en el caso de la impresión 3D; energía renovable, que permite contar con capacidades aún en lugares remotos; nanotecnología, a partir de materiales inteligentes permite generar armas más ligeras, móviles y precisas; redes sociales, con canales digitales a través de los cuales se difunde información de buenas causas pero también de contenido malicioso para reclutar seguidores; armas biológicas y bioquímicas, desarrolladas a partir de las innovaciones tecnológicas. "Resulta claro que la cuarta revolución industrial trae consigo grandes oportunidades al tiempo que plantea riesgos significativos". (Schwab, 2016, p.78)

Varios son los factores que amenazan a la seguridad, sin embargo, uno de los más importantes es el crecimiento de la comunidad de hackers. En tal sentido, según estadísticas publicadas por Symantec[9], las actividades maliciosas de ataques en Internet crecen un 64% anualmente. A través de distintas modalidades, como virus, gusanos, ataques de denegación de servicios, u otros, los hackers ponen en riesgo sistemas, computadoras, redes de telecomunicaciones. Sin embargo, hoy en día, los hackers no son considerados tan malos como lo eran antes, por el contrario, son utilizados por el gobierno y organizaciones para la defensa nacional, o defensa de las redes y sistemas o infraestructuras críticas, inclusive son utilizados de forma clandestina para atacar a otras naciones. (Kizza, 2017)

Hoy en día realizamos muchas actividades de manera virtual que antes hacíamos de manera física y pueden representar una fuente de ingreso de amenazas cibernéticas. Correo electrónico, redes sociales, banca electrónica[10], comercio electrónico[11] y juegos en línea, son algunas de ellas. (Reyna Ramos y Olivera Gómez, 2016)

[9] Symantec era una compañía dedicada al desarrollo de productos y soluciones de seguridad para pequeñas, medianas y grandes empresas; transferida a Broadcom hacia finales de 2019. Pasó a llamarse NortonLyfeLock. (https://www.itreseller.es/seguridad/2019/11/symantec-transfiere-su-marca-a-broadcom-y-pasa-a-llamarse-nortonlifelock)

[10] La banca electrónica es una modalidad a través de la cual se pueden realizar pagos de servicios, traspasos de efectivo, realizar inversiones y otras diversas operaciones bancarias sin la necesidad de trasladarse hasta la institución. (Reyna Ramos y Olivera Gómez, 2016)

[11] El comercio electrónico brinda la posibilidad de realizar compras y pagarlas online con tarjetas de débito o crédito, desde una computadora, smartphone, tablet u otro dispositivo móvil y, además, se pueden realizar en sitios ubicados dentro del país o en el exterior. (Reyna Ramos y Olivera Gómez, 2016)

Las empresas también han incorporado las tecnologías de la información y las comunicaciones para el desarrollo de sus actividades. Las herramientas más utilizadas son internet en la nube[12] o cloud computing, comercio electrónico, negocio electrónico, mercadotecnia electrónica o marketing digital y big data. (Arano Chávez, Beltrán y Escudero Macluf, 2016)

La infinidad de datos que se generan a través de aplicaciones, redes sociales, páginas web, entre otras fuentes, no pueden ser almacenados en bases de datos convencionales. Big Data se refiere a la manipulación, procesamiento y visualización de estos grandes volúmenes de datos. La explotación de ellos se aplica, por ejemplo, a la detección de perfiles de personas para la personalización de campañas publicitarias o la construcción de patrones de usuarios para ventas de productos o servicios en distintos ámbitos. (Arano Chávez, Beltrán y Escudero Macluf, 2016)

Todas las herramientas que ofrecen las tecnologías de la información y las comunicaciones en la era de la cuarta revolución industrial, cuyas bondades son aprovechadas por las personas particulares y empresas, tienen un lado no tan bueno, tras ser víctimas constantes de ciberamenazas. (Arano Chávez, Beltrán y Escudero Macluf, 2016).

Al mismo tiempo en que se desarrolla la revolución tecnológica de los últimos años, evolucionan las técnicas y herramientas utilizadas en ciberdelitos, es por ello que las políticas públicas y la legislación nacional deben considerar el tema como prioritario. En este sentido, se establecen entre los retos en materia de ciberseguridad, las iniciativas que impulsen la investigación, la formación y desarrollo de capacidades en ciberseguridad; la especialización de los profesionales; el despliegue de campañas de sensibilización y concientización; la prevención como mecanismo de combate al cibercrimen; la cooperación nacional e internacional entre sectores públicos, privados y académicos para aunar esfuerzos en la lucha contra el cibercrimen; y el impulso de proyectos legislativos en materia de ciberdelitos. (González Barrales, 2016)

Para enfrentar todos estos desafíos tenemos que desarrollar la ciberresiliencia, es decir, la "capacidad de respuesta y recuperación ante incidentes de seguridad". (Corletti, Estrada, 2017, p.31) Para ello, además de contar con la infraestructura, arquitectura de red y políticas de seguridad apropiadas, hay aspectos que resultan fundamentales, como son la adopción de una cultura de ciberseguridad y la sensibilización.

[12] Internet en la nube se trata de servicios instalados en servidores de los cuales no se conoce realmente la ubicación física, pudiendo estar en cualquier lugar del mundo. (Arano Chávez, Beltrán y Escudero Macluf, 2016)

3.3 Vulnerabilidades Relacionadas con el Hombre.

Día tras día, el mundo se inunda con noticias sobre la ciberseguridad. Aplicaciones, redes de comunicaciones, infraestructura y demás componentes del ciberespacio se ven afectados a diario. Muchas de las vulnerabilidades son producto de fallas de hardware o software, en cambio otras se producen a partir de fallas o debilidades humanas. En este sentido, investigaremos los distintos tipos de amenazas y/o vulnerabilidades, especialmente aquellas en los que la acción del hombre impacta en los riesgos asociados al uso de las tecnologías.

Las amenazas a la seguridad de los sistemas de información provienen de diversos factores, entre ellos se incluyen: debilidades en la infraestructura de redes y los protocolos de comunicaciones; rápido crecimiento del ciberespacio convirtiéndose en una red de comunicaciones y negocios vital, en donde se expande el comercio internacional y se conectan diversas infraestructuras; crecimiento de la comunidad de hackers expertos en accesos no autorizados a sistemas de gobierno, empresas e infraestructuras críticas; vulnerabilidades en protocolos de sistemas operativos en donde se ejecutan servicios de las redes de comunicaciones; trabajadores de la organización que se dedican a robar y vender bases de datos, listados de casillas de correo o documentos confidenciales; robo físico en las organizaciones tales como computadoras con información sensible. (Kizza, 2017)

La filosofía de diseño de la infraestructura de las redes de computadoras y los protocolos de comunicaciones basados en una arquitectura abierta han incrementado el desarrollo y crecimiento del ciberespacio y el uso de internet. Además, los desarrolladores de esta infraestructura y de los protocolos también siguieron una política para crear una interfaz fácil de usar, lo más eficiente y transparente posible para que todos los usuarios de todos los niveles educativos puedan usarlo sin tener conocimiento del funcionamiento de las redes y, por lo tanto, no se preocupen por los detalles. Sin embargo, esto trae algunos inconvenientes dado que los usuarios prestan poca atención a la seguridad de los sistemas. Lamentablemente, esto atrae otro tipo de personas que tratan de explotar los puntos débiles y vulnerabilidades de la red como forma de desafío, aventurerismo, diversión o gratificación personal. (Kizza, 2017)

Los datos de investigación de muchas agencias de renombre muestran constantemente que la mayor amenaza para la seguridad en cualquier empresa son las personas que trabajan dentro de ella, conocidos como *insiders*. La amenaza interna a la seguridad de una organización proviene de su interior, es decir, de los propios miembros. Se trata de una persona con privilegios de acceso a documentación clasificada, confidencial o

sensible que hace uso de esos privilegios para borrar o transferir información afuera de la organización o a usuarios no autorizados, quizás sin saberlo producto de la ingeniería social. Dentro de los errores más comunes, se observa el cifrado de información sensible en computadoras portátiles y la no revocación de privilegios de acceso cuando un empleado se desvincula de la empresa. (Kizza, 2017)

Numerosos incidentes también ocurren a partir del robo de computadoras portátiles o cualquier otro tipo de dispositivo móvil, muchos de los cuales encierran secretos de compañías o información muy valiosa de uso personal. Un caso conocido fue lo que le ocurrió a Bono el cantante de la banda de música U2, en diciembre de 1999, cuando alguien robó su laptop del auto, en donde contenía canciones que representaban meses de trabajo. (Kizza, 2017)

No todas las empresas conocen los riesgos asociados a su identidad digital y cómo gestionarlos. Para ello, el INCIBE publicó una guía sobre Ciberseguridad en la identidad digital y reputación online, en donde da cuenta sobre esos riesgos, las técnicas utilizadas por los atacantes y brinda recomendaciones al respecto.

El primero de los riesgos, es la suplantación de identidad. Se trata del robo de la identidad y se produce cuando una persona utiliza los datos personales de otra en nombre de ella. Esto puede incluir la creación o el acceso no autorizado al perfil de una empresa o entidad en un medio social y la utilizacíon del mismo. Los atacantes logran contar con información sensible como credenciales de acceso o números de tarjetas de crédito a través de la utilización de distintas técnicas, como el phishing y el pharming. En el phishing el estafador se hace pasar por la empresa, generalmente a través de correos electrónicos, creando un ambiente que le da credibilidad, utiliza imágenes o nombres de sitios web similares a las originales, logra, de este modo, confundir a la víctima, la que no se da cuenta de que se trata de un fraude y brinda información privada. En el caso de pharming, el atacante redirige, de algún modo, los accesos a páginas web de la víctima a sitios falsos que suplantan la identidad del original. (Ciberseguridad en la identidad digital y la reputación online: Una guía de aproximación para el empresario, 2016)

El segundo de los riesgos es el registro abusivo de nombres de dominio, también conocido como cibersquatting. Se da cuando terceros malintencionados registran uno o varios nombres de dominio que coinciden con la marca de los productos o servicios o nombre comercial de una empresa e impiden el uso por parte de la misma. Se puede producir durante el registro, si aparece una nueva extensión, tal como el caso de .eu o .ar, o al no renovar el nombre de dominio a tiempo, antes de la fecha de vencimiento. Una variante del

cibersquatting es el typosquatting. Este consiste en el registro de nombres de dominio muy similares a los originales u oficiales, los cuales pueden producir confusión y cuya única intencionalidad es el fraude. Por ejemplo, si el nombre de dominio original es Facebook y se observa que el sitio se llama Facebok, se trataría de un riesgo de este tipo. (Ciberseguridad en la identidad digital y la reputación online: Una guía de aproximación para el empresario, 2016)

El tercer tipo de riesgos es el ataque de denegación de servicios. Se produce cuando un atacante a través una red de computadoras a las cuales controla de manera remota, sin que lo propietarios sean concientes de ello, realiza peticiones masivas a un servidor determinado al mismo tiempo provocando su caída. Puede provocar, por ejemplo, la caída de un servidor web, lo que afecta a una pérdida en la imagen institucional, su reputación e identidad digital. (Ciberseguridad en la identidad digital y la reputación online: Una guía de aproximación para el empresario, 2016)

El cuarto de los riesgos es la fuga de información. En estos casos el objetivo suele ser el lucro, por ejemplo, al obtener información bancaria de la empresa y sus clientes, o al extorsionar al propietario de los datos a cambio de un rescate, aunque también se distinguen otros motivos, como el espionaje industrial o el desprestigio a la organización. (Ciberseguridad en la identidad digital y la reputación online: Una guía de aproximación para el empresario, 2016)

Otros de los riesgos son las publicaciones por terceros de informaciones negativas. Hoy en día, el uso de las redes sociales brinda los medios para interactuar con los usuarios o clientes, quienes pueden dar opiniones o devoluciones, y, a veces las usan de forma negativa, hasta incluso con insultos o burlas. El problema es que la información sigue apareciendo aún con el paso del tiempo en los buscadores de internet, y el descrédito realizado a la organización puede resultar perjudicial más allá de las acciones legales o medidas reactivas que se tomen oportunamente. (Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario, 2016)

El último de los riesgos a mencionar es la utilización no consentida de derechos de propiedad industrial. Entre estos derechos están las invenciones, los diseños industriales y los signos distintivos tales como marcas o nombres comerciales. Su utilización por parte de terceros puede implicar un valor positivo o negativo para la organización. (Ciberseguridad en la identidad digital y la reputación online: una guía de aproximación para el empresario, 2016)

Hemos visto que las amenazas a la seguridad de la información pueden originarse en actividades humanas voluntarias o involuntarias, realizadas por *insiders* o personas de afuera de la organización llamadas *outsiders*; sin embargo, la mayoría de ellos se originan en actos ilegales o criminales. (Kizza, 2017)

Hasta aquí vimos los distintos tipos de amenazas y riesgos que enfrentan las tecnologías de la información y las comunicaciones, ahora nos centraremos en las posibles fuentes de vulnerabilidades que las afectan. Entre las más frecuentes se destacan defectos de diseño, mala gestión de la seguridad, implementación incorrecta, vulnerabilidad de la tecnología de internet, la naturaleza de la actividad del intruso, la dificultad de la fijación de sistemas vulnerables y los límites de eficacia de las soluciones reactivas. (Kizza, 2017)

Los defectos en el diseño de un sistema de computación pueden provenir del hardware o del software. Las vulnerabilidades asociadas al software son las más susceptibles de suceder. Estas pueden desencadenarse por factores humanos. Tal puede ser el caso de lapsus de memoria o fallas de atención; la prisa para terminar, sea por lanzar un producto al mercado o cumplir tiempos pautados con los clientes; el exceso de confianza y uso de algoritmos no estándares, poco testeados; y la malicia. (Kizza, 2017)

Otra de las fallas desencadenadas por factores humanos es la complejidad del software. Con los lenguajes de programación actuales es muy difícil encontrar un juego de datos para testear todas las posibles salidas y errores, incluso para un mismo set de datos de entrada puede haber distintas salidas posibles. El malentendimiento de las especificaciones de diseño básicas también pueden derivar en fallas de todos los componentes del software. (Kizza, 2017)

Generalmente cuando necesitamos un software, no reparamos en quien lo desarrolló o en su calidad, sólo nos interesa que haga lo que necesitamos. Al utilizar un código expuesto para su uso en internet, se puede correr el riesgo de que contenga un troyano, por eso los expertos aconsejan utilizar fuentes confiables de software. (Kizza, 2017)

La administración de la seguridad involucra un análisis de riesgos, en donde se puedan identificar los activos a proteger, las amenazas y los riesgos que corren, para luego determinar los controles de acuerdo al nivel de protección deseado y estimar el posible daño y la pérdida potencial si algunas de estas amenazas se materializan. Todo esto debe estar organizado y delineado en las políticas de seguridad y en los procedimientos e instructivos que surgen de ellas, los cuales deben ser monitoreados y evaluados. Además, no puede quedar de lado la importancia de la educación en seguridad a todo el personal de la organización para que aprendan sus responsabilidades individuales. Si alguna parte de todo

este proceso falla o no se realiza de manera eficiente, podemos caer en la vulnerabilidad provocada por una administración de seguridad pobre. (Kizza, 2017)

Otra fuente de vulnerabilidades son las tecnologías de Internet. Constantemente, se reportan agujeros o brechas de seguridad en tecnologías de hardware o de software. Sin embargo, estas últimas son mucho más comunes, y las podemos clasificar en cuatro categorías: Vulnerabilidades en sistemas operativos; vulnerabilidades basadas en puertos; errores basados en aplicaciones de software; y protocolos del sistema, tales como el navegador de cliente y servidor. (Kizza, 2017)

Hoy en día está cambiando la naturaleza de la actividad de los hackers. Cada vez resulta más fácil para cualquier persona convertirse en uno de ellos. La fácil disponibilidad de las herramientas tecnológicas, la facilidad para ocultar las identidades y las ubicaciones de los atacantes, la automatización de la tecnología de ataque, permiten que no sean necesarios conocimientos muy avanzados para perpetrar un ataque. (Kizza, 2017)

3.4 La ciberseguridad y la Educación.

Con la creciente evolución de las tecnologías y, por consiguiente, de los riesgos a los que nos enfrentamos, no basta sólo con incrementar las medidas e inversiones en seguridad. También es necesario contar con las capacidades para poder brindar los conocimientos a todas las personas que desde distintos ámbitos realizan aportes para la construcción de la ciberseguridad. En este sentido, las universidades desde sus funciones sustantivas como son la docencia, la investigación, la difusión de la cultura y extensión de los servicios que brindan a través de las distintas facultades, juegan un rol importante relacionado con la Ciberseguridad. De este modo, podrán ser los principales concientizadores y formadores de personas en esta área del conocimiento para hacer frente a las amenazas cibernéticas. La universidad debería promover una dimensión integral en la formación de los universitarios, ir más allá de los lineamientos establecidos dentro de la currícula formal, y sembrar valores respecto de la seguridad pública. (Hernández Rodríguez, Cano Flores y García López, 2016)

Una de las herramientas viables para prevenir y frenar actividades ilegales en el ciberespacio es la educación. A través de ella, las personas podrán aprender el valor de la ciberseguridad, podrán contar con recursos y técnicas para usar las tecnologías de manera responsable, conocer cómo manejarse ante incidentes de seguridad y su tratamiento, entre otras cosas. La educación la podemos abordar de distintas formas, la educación dirigida y la educación masiva. Por un lado, la educación dirigida se ofrece a ciertos sectores o grupos de población como pueden ser los niños en la escuela, profesionales o ciertos grupos de interés. En este sentido, varias compañías privadas como Microsoft, Cisco y CSI, entre otras, brindan

cursos de diversas certificaciones en seguridad. A su vez, la podemos subdividir en educación formal y en ocasional. La educación formal abarca desde el jardín de infantes hasta la universidad y se personaliza según el nivel de madurez en cada uno de los ámbitos. En cambio, la educación ocasional, es aquella que obtienen los profesionales como parte de la formación continua, de este modo se deberían canalizar también las actualizaciones en materia de seguridad de la información. Por otro lado, la educación masiva, involucra a un gran número de personas a través de métodos de participación comunitaria para tratar de lograr una rápida conciencia efectiva. Este último caso, es un enfoque similar al de las campañas que se llevaron adelante para enfermedades tales como el cáncer o el SIDA. (Kizza, 2017)

A partir de los incidentes de seguridad producidos en los últimos años, se reconoce ampliamente la importancia de la ciberseguridad. Desde esta perspectiva, se observa la falta de habilidades, conocimientos y experiencia en ciberseguridad entre la fuerza laboral, la que se estimaba en alrededor de 3 millones de trabajadores a nivel global, según estudios de la fuerza laboral de ciberseguridad para los años 2018 y 2019. Una de las dificultades que se presentan es la falta de formadores con los conocimientos y experiencia necesaria en el ámbito. La comprensión de los temas que abarca la ciberseguridad, con su corta edad, debería utilizarse para dar forma al currículo de los nuevos programas educativos. La rápida evolución de los ciberataques, en contraste con la naturaleza estática de la academia, provocan un aumento en la brecha de profesionales con conocimientos en ciberseguridad. (Blažič, 2021)

En este sentido, los gobiernos comenzaron a desarrollar estrategias. Tal es el caso del Programa de Garantía y Seguridad de la Información, una iniciativa nacional de EE.UU. para la educación en ciberseguridad y de la Agencia Europea para la Seguridad de las Redes y de la Información (ENISA) creados para recopilar datos sobre ofertas educativas en ciberseguridad y proponer cambios apropiados. En la Unión Europea, desde la publicación de la primera estrategia de ciberseguridad en 2013, se han aumentado el interés y los esfuerzos por la educación y formación en torno a la seguridad. Al respecto, se ha planificado un programa de certificación voluntaria para mejorar las habilidades y competencias de los profesionales de las TIC y del personal de ciberseguridad. Además, se crearon dos centros para el desarrollo de la educación en ciberseguridad: El centro de competencia de Concordia en donde se está desarrollando un nuevo ecosistema educativo en ciberseguridad que ofrece formación por industria y el centro *Cybersecurity4Europe* en donde se ocupan de los programas de instituciones de educación superior de la Unión Europea. (Blažič, 2021)

El centro Concordia confeccionó una cartera de cursos de ciberseguridad, dirigida a profesionales de distintas categorías de la industria, tales como tecnólogos, gerentes de nivel medio y ejecutivos. El objetivo final fue crear una metodología para la creación de cursos con una amplia gama de contenidos que den respuesta a la diversidad de industrias existentes con contenidos de módulos específicos de ciberseguridad dirigido a distintos tipos de empleados. Algunos trabajadores necesitarán contar con los conocimientos básicos como para distinguir un incidente de seguridad y saber actuar ante él; otros, como pueden ser técnicos de TI necesitarán conocer las últimas herramientas y técnicas de prevención de ataques y recuperación de desastres, por ejemplo; y altos gerentes deberán tener conocimientos básicos de ciberseguridad y su impacto en el negocio. (Blažič, 2021)

Como parte del proyecto "Educación Universitaria", el centro *Cybersecurity4Europe* y ENISA, en el año 2019, llevaron a cabo una investigación sobre el nivel de educación en ciberseguridad que otorga títulos de master, para lo cual se inspeccionaron las currículas del 100% de las maestrías en casi todos los países de la Unión Europea. Se pudo observar, una disparidad de cobertura de temas en los distintos países en la currícula obligaroria. Hay temas como criptografía y seguridad que resultan comunes a la mayoría de los programas, sin embargo, hay otros que no son tran frecuentes, como es el caso de Seguridad Social, Seguridad Organizacional, Seguridad de Componentes y Seguridad de Conexiones. Como resultado del trabajo, ENISA publicó un mapa de Educación en Ciberseguridad de la UE, con el objetivo de ser la primera fuente de consulta para los ciudadanos que buscan actualizar sus conocimientos y habilidades en ciberseguridad. (Blažič, 2021)

Hay algunas opiniones encontradas en cuanto al manejo de la educación, algunos autores afirman que para mitigar los problemas de ciberseguridad actuales se deberían adoptar sistemas educativos más interdisciplinarios para una mejor integración de habilidades. Otros proclaman que los aspectos sociales juegan un rol fundamental en la educación en ciberseguridad y el desarrollo de las fuerzas de trabajo. En cambio, otros afirman que la ciberseguridad es un tema netamente técnico que lleva años de estudio y entrenamiento. (Blažič, 2021)

Joyanes Aguilar (2017), por su parte, observa la formación en ciberseguridad en España, América Latina y El Caribe. En estos lugares hay amplitud de ofertas de másteres, especializaciones, diplomaturas, cursos profesionales y de posgrado impartidos por universidades y escuelas de negocios.

Por un lado, tenemos las agencias estatales que se dedican a la ciberseguridad y por otro las universidades y centros de formación con carreras, programas, certificaciones y

especialidades afines a la ciberseguridad. En Argentina, entre los organismos del estatales cuyas funciones principales están relacionados a la ciberseguridad, encontramos a la Jefatura de Gabinete de Ministros, el Ministerio de Seguridad y el Ministerio de Defensa.

La Dirección Nacional de Ciberseguridad dependiente de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros desarrolla estrategias y mecanismos para la protección de la información y los servicios del estado nacional y sus ciudadanos y coordina la gestión de incidentes a nivel nacional. Además, coordina la realización de cursos de capacitación orientados a concientizar sobre la protección de la información, la toma de conciencia en relación al uso de las Tecnologías de la Información y las Comunicaciones, la protección de las infraestructuras y a elevar el nivel de seguridad de los organismos a partir de promover prácticas responsables y de buen uso de las herramientas informáticas de uso habitual en el ámbito laboral.

La Jefatura de Gabinete de Ministros cuenta además con el Instituto Nacional de la Administración Pública que ofrece cursos de capacitación, programas de formación, actualización y becas para carreras de grado y posgrado para todas las personas que prestan servicios en la Administración Pública Nacional.

En el Ministerio de Seguridad, la Subsecretaría de Formación y Carrera dependiente de la Secretaría de Seguridad y Política Criminal se encarga de desarrollar y coordinar la implementación de la formación, capacitación y entrenamiento del personal de las Fuerzas Policiales y de Seguridad, federales y jurisdiccionales, en todos los niveles, desde cursos de actualización hasta las carreras de pregrado, grado y posgrado.

En el Ministerio de Defensa encontramos la Subsecretaría de Ciberdefensa. Entre sus objetivos se incluyen fomentar e incentivar la formación de recursos humanos para la Ciberdefensa; promover las actividades de difusión y concientización dentro y fuera de la Jurisdicción en la materia, así como también extender y ampliar los programas de capacitación en Ciberdefensa en cooperación con Universidades, centros especializados y otros organismos públicos y privados.

Bajo la dependencia orgánica, funcional y operacional del Estado Mayor Conjunto de las Fuerzas Armadas, se encuentra el Comando Conjunto de Ciberdefensa, organismo coordinador de las acciones de los Centros de Ciberdefensa de las Fuerzas Armadas. Además, desarrolla ejercicios de entrenamientos y capacitaciones y atiende a la concientización en temas de ciberdefensa del personal de las Fuerzas Armadas.

El Comité de Ciberseguridad creado por Decreto 577 de 2017 integrado por los Ministerios de Seguridad y Defensa y el ex Ministerio de Modernización, que luego pasó a

las manos de la Secretaría de Gobierno de Modernización, quien lo preside, tiene por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad, la cual se aprobó mediante la Resolución 829 de 2019 [Secretaría de Gobierno de Modernización]. Los dos primeros objetivos de la Estrategia están relacionados con la formación de las personas en materia de Ciberseguridad.

El primer objetivo es la concientización del uso seguro del Ciberespacio, que incluye:

- Crear un plan programático de concientización de alcance nacional sobre la seguridad en el Ciberespacio, abarcativo de la sociedad en su conjunto.
- Fortalecer y articular con los sectores privados y las organizaciones civiles la promoción de contenidos de concientización.
- Incrementar las actividades de concientización en el ámbito educativo.

El segundo objetivo es la capacitación y educación en el uso seguro del Ciberespacio, que abarca:

- Promover la formación de profesionales, técnicos e investigadores.
- Desarrollar talleres y ejercicios, tanto gubernamentales como con los sectores privados y el sector civil.
- Fortalecer la capacitación en técnicas de prevención, detección, respuesta y resiliencia ante incidentes.
- Incrementar las actividades transversales de formación en el sector académico.

Algunos meses más tarde, mediante Decreto 480 de 2019, se amplió la participación en el Comité de Ciberseguridad para integrar a los Ministerios de Relaciones Exteriores y Culto y de Justicia y Derechos Humanos y a la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros.

Dentro del marco de la Estrategia Nacional de Ciberseguridad, la senadora Carmen Lucila Crexell, presentó en mayo de 2019, ante el Senado de la Nación Argentina un proyecto de Ley para la creación del Instituto de Ciberseguridad Argentino (INCIBAR) en el ámbito de la Jefatura de Gabinete de Ministros. Actualmente, se encuentra tramitando un nuevo proyecto, superador al presentado en el año 2019 (expediente S-1616/19), ambos son de autoría de la Senadora. La iniciativa con validez parlamentaria tramita mediante el expediente S-30/21, el cual ha sido girado en primer orden a la comisión de Legislación General, en segundo orden a la Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión, y en tercer orden a la Comisión de Presupuesto y Hacienda; ahora aguarda su

tratamiento en las comisiones correspondientes a su trámite legislativo. La iniciativa tiende a proteger las Infraestructuras Críticas de la Información "con la finalidad de fortalecer la capacidad nacional en ciberseguridad para lograr un elevado nivel de seguridad de las redes y sistemas de información dentro del territorio nacional". (Proyecto de Ley, S-30/21, art. 1, p.2)

Como podemos observar, todos los organismos del estado nacional cuentan con iniciativas para la capacitación y formación de sus agentes en ciberseguridad. Cuentan con agencias especiales de formación para el personal propio y con carreras de grado y posgrado, como las que ofrece la Universidad de la Defensa Nacional, a la que también pueden acceder personas, que no sean trabajadores del estado.

Los expertos en ciberseguridad son requeridos por empresas de todo tipo y tamaño, sean pequeñas, medianas o multinacionales. Además, se pueden desenvolver en una gran variedad de campos: Ciberinteligencia, análisis forense, hacking ético, desarrollo de hardware y software seguro, ciberespionaje, encriptación o seguridad en la nube. También hay algunas ramas o perfiles más nuevos, cada vez más demandados que surgen a partir de la transformación digital, entre los que podemos mencionar: expertos en Big Data, desarrolladores de Internet de las Cosas y de Ciudades Inteligentes para gestión de objetos inteligentes, especialistas en computación en la nube o cloud computing tales como Diseñador de nubes o Gestores de seguridad en la nube, científicos de datos o Data Scientist, especialistas en Aprendizaje de Máquina o Machine Learning[13] y Aprendizaje Profundo o Deep Learning[14]. (Joyanes Aguilar, 2017).

De este modo, surgen nuevos roles profesionales para los cuales las personas se tienen que formar. Las empresas y la administración requieren de la concienciación de los riesgos y oportunidades de la ciberseguridad en todos los niveles profesionales sea a nivel de personal directivo o simple empleado. Las tecnologías de la información son transversales a todas las especialidades, para lo cual la formación de estos profesionales debe ampliarse a las áreas de marketing, recursos humanos o jurídicos. Seguramente, continuarán emergiendo nuevos perfiles o profesiones que aún ni imaginamos, todos "guardarán una estrecha relación con la nube, la ciberseguridad, Internet de las Cosas y Big Data, los cuatro pilares de la transformación digital de las organizaciones y empresas del final de esta década y de la próxima". (Joyanes Aguilar, 2017, p.57)

[13] Machine Learning es la ciencia que hace que las computadoras aprendan a partir de los datos. (Bobadilla, 2020)
[14] Deep Learning utiliza métodos de machine learning basándose en redes neuronales multi-capa (Bobadilla, 2020)

4. Investigación.

4.1 Tipo de Investigación.

El tipo de investigación a realizar es exploratoria y descriptiva con enfoque de análisis cualitativo y proceso deductivo.

4.2 Hipótesis de la Investigación.

La formación académica disponible en nuestro país en materia de ciberseguridad resulta poco adecuada para las personas que se desempeñan en distintos ámbitos laborales en la Argentina, en línea con las necesidades actuales frente a la revolución tecnológica que vivimos.

Para evaluar la hipótesis presentada intentaremos responder las siguientes preguntas:

- ¿Cuáles son los riesgos y amenazas a las que pueden verse expuestas las personas con el uso de las tecnologías?
- ¿Por qué resulta necesaria la formación de las personas en materia de Ciberseguridad?
- ¿Cuáles son los distintos perfiles de profesionales que surgen de la investigación para la formación en Ciberseguridad?
- ¿Es adecuada la formación disponible en el país sobre Ciberseguridad?

4.3 Desarrollo de la Investigación.

4.3.1 Estudios en España.

De acuerdo con el Índice Global de Ciberseguridad obtenido por la Unión Internacional de Telecomunicaciones, podemos observar que España posee un alto nivel de compromiso con la ciberseguridad. Ocupa el primer lugar dentro de los países de habla hispana y empata en el cuarto lugar con Corea y Singapur, como se puede observar en la Figura 1 - Índice Global de Ciberseguridad.

Ahora, vamos a analizar las ofertas de las diez universidades de España mejores rankeadas, de acuerdo a la información existente en sus sitios web. Para ello nos basaremos en el ranking recientemente publicado por un grupo de investigación del Consejo Superior de Investigaciones Científicas (CSIC) de España, Webometrics[15] en julio de 2021, como se puede observar en la figura 3 a continuación:

[15] El CSIC está adscripto al Ministerio de Educación de España. Su principal objetivo es promover la investigación científica para mejorar el progreso del nivel científico y tecnológico del país. El "Ranking Webometrics de Universidades del Mundo" es realizado periódicamente por el grupo de investigación del Laboratorio de Cibermetría, perteneciente a CSIC. La confección del ranking se realiza a partir de un indicador que toma en cuenta varios factores basados en la visibilidad y presencia en línea, el número de documentos y las publicaciones y citaciones. (https://www.ovtt.org/webometrics-ranking-mundial-de-universidades/)

España

Ranking	Ranking Mundial	Universidad
1	131	Universitat de Barcelona
2	182	Universitat Autònoma de Barcelona
3	192	(1) Universitat de València
4	220	Universidad de Granada
5	258	Universidad Autónoma de Madrid
6	286	Universidad de Sevilla
7	288	Universitat Politècnica de Catalunya BarcelonaTech
8	299	Universitat Pompeu Fabra
9	323	Universidad Politécnica de Valencia
10	328	Universidad Politécnica de Madrid

Figura 3. Ranking de Universidades de España
Fuente: https://www.webometrics.info/es/Europe_es/España

Encontramos a la Universidad de Barcelona, la Universidad Autónoma de Barcelona, la Universidad de Valencia, la Universidad de Granada, la Universidad Autónoma de Madrid, la Universidad de Sevilla, la Universidad Politécnica de Catalunya BarcelonaTech, la Universidad de Pompeu Fabra, la Universidad Politécnica de Valencia y la Universidad Politécnica de Madrid. En el Anexo A se pueden observar las mencionadas universidades con sus sitios web.

Tomamos como referencia las carreras de grado de Derecho, Economía e Informática de cada una de las universidades seleccionadas. Analizamos los planes de estudio de las carreras de grado relacionadas a Derecho en todas las facultades respectivas (Anexo B). En todos los casos, observamos que no existen materias relacionadas a la ciberseguridad en modalidad obligatoria. Sólo el 10% de las carreras cuentan con una materia optativa.

Luego, analizamos los planes de estudio de las carreras relacionadas a Economía en las facultades correspondientes (Anexo C). En todos los casos, observamos que no existen materias relacionadas a la ciberseguridad ni en modalidad obligatoria ni optativa.

Por último, analizamos los planes de estudio de las carreras relacionadas al área Informática (Anexo D). En estos casos, observamos que, en general, las carreras relacionadas al área Informática no disponen de materias de carácter obligatorio relacionadas con la ciberseguridad. De las veintidós (22) carreras dictadas en las universidades tomadas como muestra, observamos que sólo el 55% dispone de materias de carácter obligatorio y también el 55% tiene materias de carácter optativo. Asimismo, un 13% no presenta dentro de sus planes de estudio ninguna materia atinente a la ciberseguridad. De la totalidad de carreras con materias obligatorias relacionadas a la ciberseguridad, el 50% cuenta con 2 o 3 materias y otro 50% sólo disponen de una materia. Respecto de la cantidad de materias

optativas, los planes disponen de 1, 2, 3 y 4 materias, una sola carrera cuenta con nueve (9) opciones de materias optativas.

4.3.2 Estudios en Argentina.

Actualmente, Argentina posee un nivel medio de compromiso con la ciberseguridad. De acuerdo al Índice de Ciberseguridad Global 2020, ocupa el puesto número 91 a nivel mundial y décimo tercero dentro de los países de la región como podemos observar en la Figura 2.

Ahora, vamos a analizar la oferta académica en las universidades de Argentina. En la actualidad, varias instituciones de educación superior ofrecen programas de grado, posgrado y certificaciones en una amplia variedad de aspectos relacionados con la ciberseguridad. La figura 4 muestra las diez (10) universidades mejores rankeadas en Argentina:

Argentina

Ranking	Ranking Mundial	Universidad
1	392	Universidad de Buenos Aires
2	489	Universidad Nacional de La Plata
3	1529	Universidad Nacional de Mar del Plata
4	1645	Universidad Nacional del Centro de la Provincia de Buenos Aires
5	1831	Universidad Nacional de Tucumán
6	1869	Universidad Tecnológica Nacional
7	1871	Universidad Nacional de Córdoba
8	1963	Universidad Nacional de Quilmes
9	2004	Universidad Nacional de San Juan
10	2294	Universidad Nacional de San Luis

Figura 4. Ranking de Universidades de Argentina
Fuente: https://www.webometrics.info/es/Latin_America_es/Argentina

Ocupan los primeros lugares la Universidad de Buenos Aires, la Universidad Nacional de La Plata, la Universidad Nacional de Mar del Plata, la Universidad Nacional del Centro de la Provincia de Buenos Aires, la Universidad Nacional de Tucumán, la Universidad Tecnológica Nacional, la Universidad Nacional de Córdoba, la Universidad Nacional de Quilmes, la Universidad Nacional de San Juan y la Universidad Nacional de San Luis. En el Anexo E se pueden observar las mencionadas universidades con sus sitios web.

Tomamos como referencia las carreras de grado de Derecho, Economía e Informática de cada una de las universidades seleccionadas. Analizamos los planes de estudio de las carreras de grado relacionadas a Derecho en todas las facultades de Derecho o similares respectivas. (Anexo F).

En este caso, observamos que, de la totalidad de las universidades y sus correspondientes facultades del área de Derecho consultadas, sólo una cuenta en su plan de estudios con una materia de carácter obligatorio relacionada a la ciberseguridad, lo que representa el 10% de la totalidad y sólo dos universidades, cuentan entre sus materias optativas con la opción de cursar alguna materia relativa a la ciberseguridad.

Luego, analizamos los planes de estudio de las carreras relacionadas a Economía en las facultades correspondientes (Anexo G). En el área de Economía, observamos que, sólo una de las diez universidades consultadas, posee una materia de carácter obligatorio relacionadas a la ciberseguridad, lo que representa el 10% y sólo una universidad, cuenta entre sus materias optativas con la opción de cursar una materia relativa a la ciberseguridad.

Por último, analizamos los planes de estudio de todas las ofertas de carreras relacionadas al área Informática (Anexo H). Se analizaron los planes de estudio de diez (10) universidades con sus catorce (14) facultades/escuelas correspondientes, las que contienen veintiún (21) carreras de la rama Informática. En estos casos, observamos que el 38% de las carreras poseen materias de carácter obligatorio relacionadas a la ciberseguridad. Sin embargo, el 10% solamente cuenta con más de una materia obligatoria, mientras que el 28% restante cuenta sólo con una materia obligatoria. El 19% de las carreras no dispone de materias de carácter obligatorio ni optativo relacionadas con la ciberseguridad. El 52% de la totalidad posee materias de carácter optativo; ésto significa que el alumno puede elegir no cursarlas. El 33% posee entre 1 y 3 materias optativas y el 19% entre 4 y 7 materias optativas.

Finalmente, en el cuadro adjunto en el Anexo I se pueden observar las ofertas de carreras de posgrado relacionadas a la ciberseguridad en Argentina. Tomamos en cuenta las ofertas académicas de las diez (10) universidades mejores rankeadas, e incorporamos la Universidad de la Defensa Nacional, por ser la institución en donde se forman muchos de los agentes que contribuirán en el futuro a la Defensa Nacional. En este caso observamos que, solamente tres de las universidades analizadas poseen estudios de posgrado atinentes a la ciberseguridad. En la mayoría de los casos, los requisitos para acceder a esas titulaciones son poseer título universitario atinente a la informática o alguna rama de ingeniería. Sin embargo, como comenta Mariana Leiva (2019) en su nota “Posgrados 2020: ¿Cuánto cuesta estudiar en Argentina?”, sólo el 1% de la población alcanza niveles de formación de posgrado en nuestro país, con lo cual podemos ver que son muy pocas las personas que alcanzan esos estudios. Además, podemos observar que las ofertas de posgrados están concentradas en Buenos Aires, lo que presenta una limitante para las personas que trabajan en el resto del país, cuando las cursadas son de manera presencial.

4.3.3 Comparación de los Estudios en España y Argentina.

En relación al análisis de los planes de estudio de carreras informáticas y no informáticas, se confeccionaron los siguientes cuatro cuadros que se muestran en las figuras a continuación para ayudar a la visualización de los resultados:

	España		Argentina	
	Materias Obligatorias	Materias Optativas	Materias Obligatorias	Materias Optativas
Derecho	0%	10%	10%	20%
Economía	0%	0%	10%	10%
Informática	55%	55%	38%	52%

Figura 5. Cuadro resumen de materias obligatorias y optativas relativas a ciberseguridad, en carreras de grado en España y Argentina

Oferta de materias	España			
	Ni obligatorias ni optativas	Sólo Obligatorias	Sólo Optativas	Obligatorias y Optativas
Derecho	90%	0%	10%	0%
Economía	100%	0%	0%	0%
Informática	13%	32%	32%	23%

Figura 6. Ofertas de materias relacionadas a la Ciberseguridad en España

Oferta de materias	Argentina			
	Ni obligatorias ni optativas	Sólo Obligatorias	Sólo Optativas	Obligatorias y Optativas
Derecho	70%	10%	20%	0%
Economía	90%	0%	0%	10%
Informática	19%	28%	42%	10%

Figura 7. Ofertas de materias relacionadas a la Ciberseguridad en Argentina

Cantidad de materias	España		Argentina	
	Obligatorias	Optativas	Obligatorias	Optativas
1	28%	18%	28%	14%
2/3	27%	27%	10%	19%
4 o +	0%	10%	0%	19%

Figura 8. Cantidad de materias ofertadas (optativas y obligatorias) relativas a ciberseguridad en las carreras relacionadas a Informática analizadas de España (22) y Argentina (21)

Si comparamos la situación de España y Argentina, podemos observar, que son bastante similares, en lo que respecta a las ofertas de materias atinentes a la ciberseguridad en carreras de grado no informáticas. En ambos casos, es muy bajo a nulo, lo que indica que la mayor parte de los profesionales que surgen de esas carreras no cuentan ni siquiera con las nociones básicas de ciberseguridad para desenvolverse en su ámbito laboral.

Si miramos la situación de las carreras informáticas, podemos distinguir, que en España hay una oferta un poco más amplia de materias relacionadas a la ciberseguridad. Sin embargo, las materias optativas, tal como su nombre lo indica, no requieren la obligatoriedad de que el alumno las curse. Entonces, si tomamos en cuenta las carreras que sólo ofrecen materias no obligatorias sumado a las que no poseen ninguna oferta en materias optativas ni obligatorias, en España es el 45% y en Argentina, el 62%. En ambos casos es un porcentaje bastante elevado, pero aún más en nuestro país. Lo que implica, al igual que la situación de los no informáticos, con la gravedad de que se trata de técnicos, que un gran porcentaje de los profesionales que egresan de carreras informáticas, no cuentan ni siquiera con las nociones y conocimientos básicos en ciberseguridad. Todo esto, sin detenernos en la poca variedad de ofertas, que, en la mayoría de los casos, se trata sólo de una materia.

4.3.4 Situación de las Personas Respecto de su Formación en Ciberseguridad.

Uno de los objetivos planteados en el presente trabajo es definir perfiles de profesionales que surjan a partir del análisis de los conocimientos que se posee en materia de ciber para presentar propuestas que mejoren la situación. Para ello, vamos a indagar un poco más sobre la realidad y las percepciones de las personas respecto de sus conocimientos en ciberseguridad.

Al respecto, se elaboró una encuesta sobre la formación de las personas en ciberseguridad, la cual fue realizada a 215 personas entre 23 y 73 años, de distintos ámbitos laborales, edades y ramas de conocimiento, mediante la herramienta Google Forms entre los días 06 y 16 de septiembre de 2021. En el Anexo J se puede observar el diseño de la encuesta y en el Anexo K se puede observar un muestreo correspondiente al 10% de las encuestas realizadas.

En las figuras 9 a 23 se muestran las respuestas a cada una de las preguntas realizadas en la encuesta con sus correspondientes porcentajes:

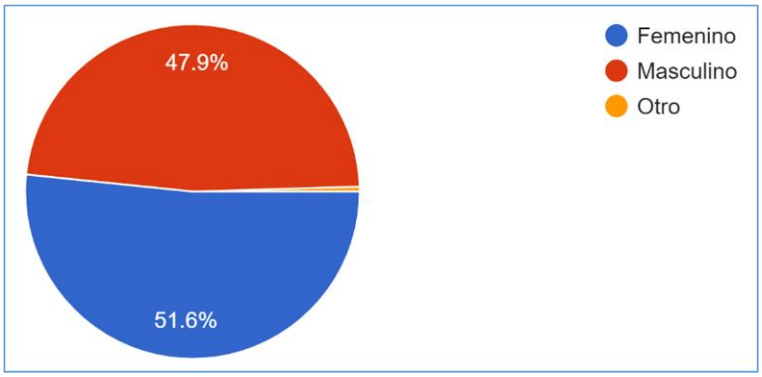


Figura 9. Respuestas encuesta a pregunta 1. Sexo (total 215)

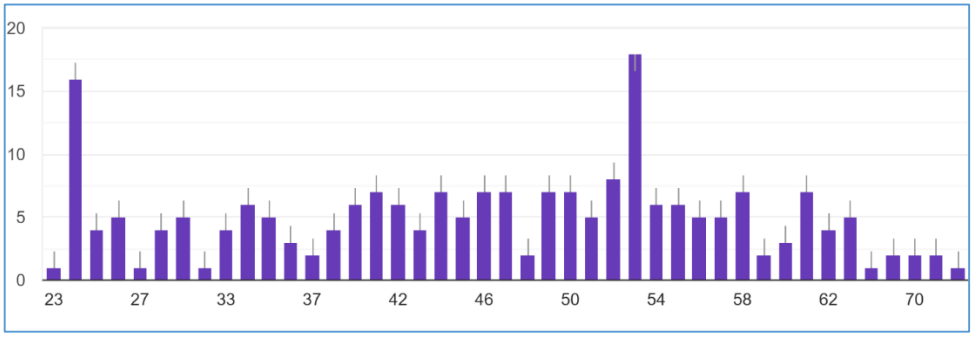


Figura 10. Respuestas encuesta a Pregunta 2. Edad (total 215)

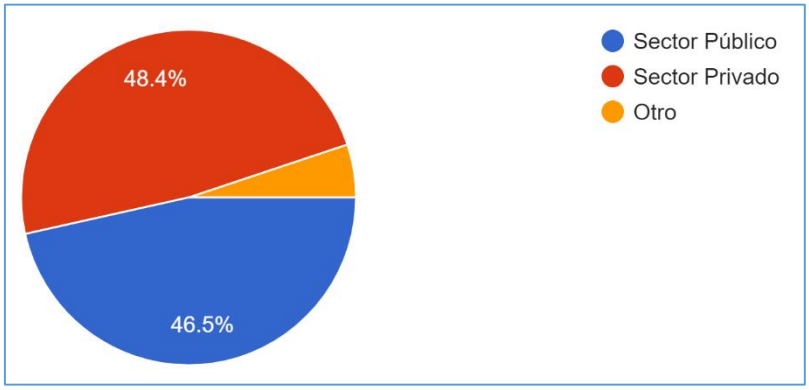


Figura 11. Respuestas encuesta a pregunta 3. Trabaja en: (total 215)

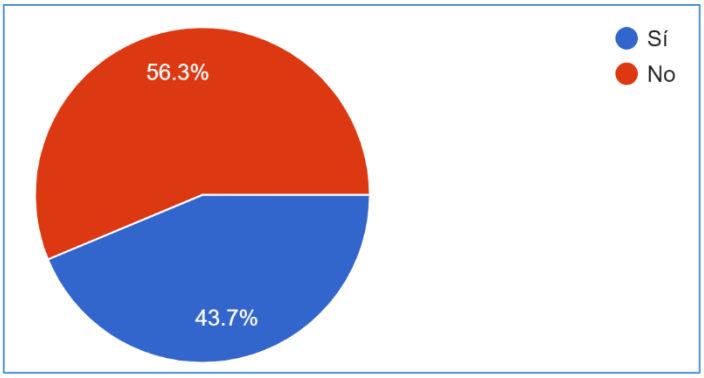


Figura 12. Respuestas encuesta a pregunta 4. ¿Tiene personal a cargo? (total 215)

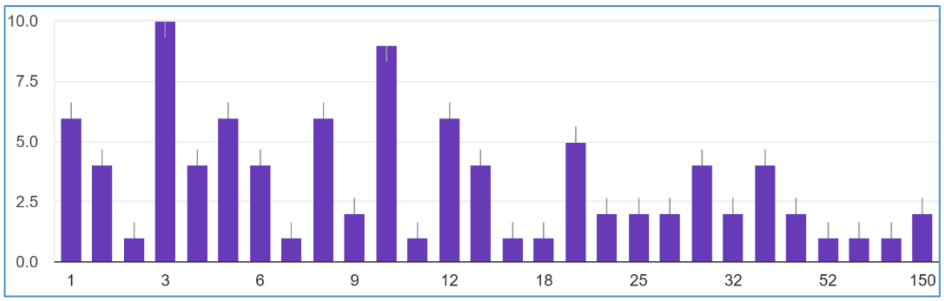


Figura 13. Respuestas encuesta a pregunta 4.1 Cantidad de personal a cargo (total 94)

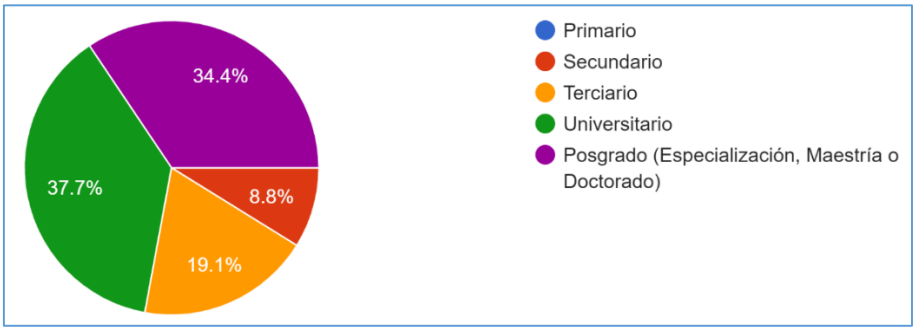


Figura 14. Respuestas encuesta a pregunta 5. Máximo nivel de estudios alcanzado (total 215)

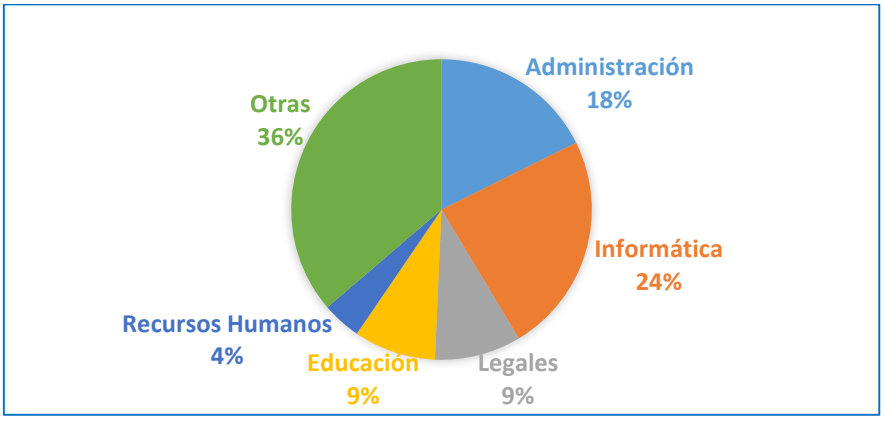


Figura 15. Respuestas encuesta a pregunta 6. ¿En qué área se desempeña dentro de su ámbito laboral? (total 215)

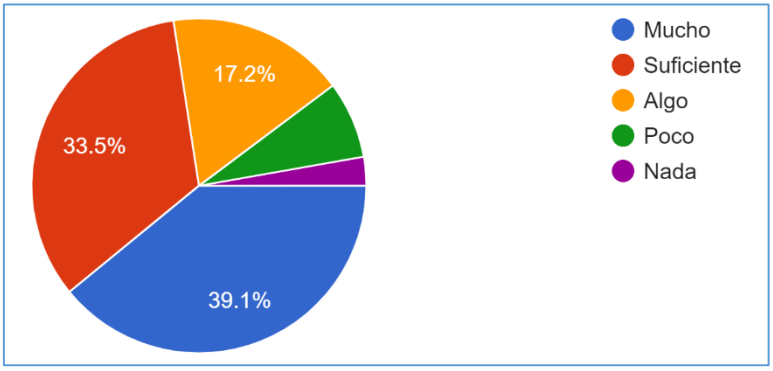


Figura 16. Respuestas encuesta a pregunta 7. ¿Cuán involucrado está en el uso de tecnologías de información y comunicación (TIC) en su ámbito laboral? (total 215)

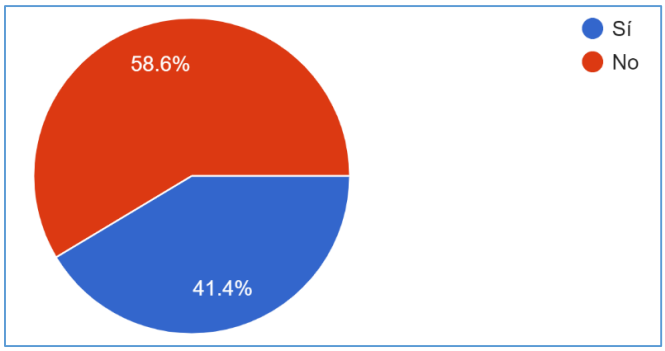


Figura 17. Respuestas encuesta a pregunta 8. ¿Su trabajo está relacionado de alguna forma a la seguridad informática? (total 215)

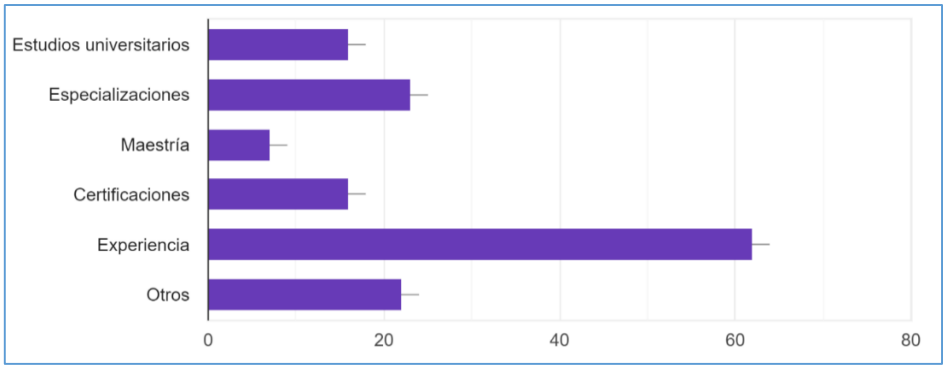


Figura 18. Respuestas encuesta a pregunta 8.1 ¿De qué forma o a través de qué medio adquirió conocimientos en ciberseguridad? (total 89)

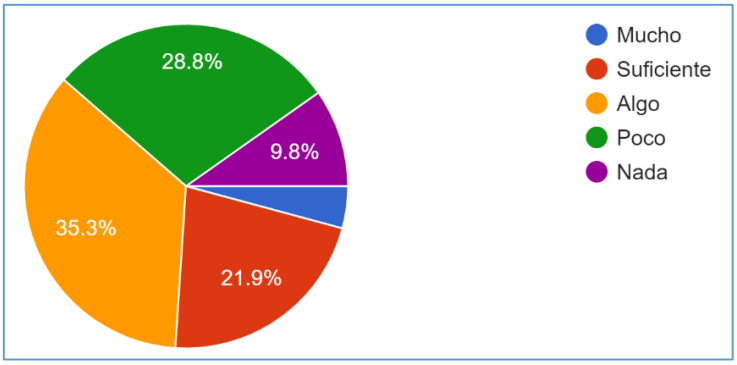


Figura 19. Respuestas encuesta a pregunta 9. ¿Cuánto considera Ud. que sabe sobre seguridad informática? (total 215)

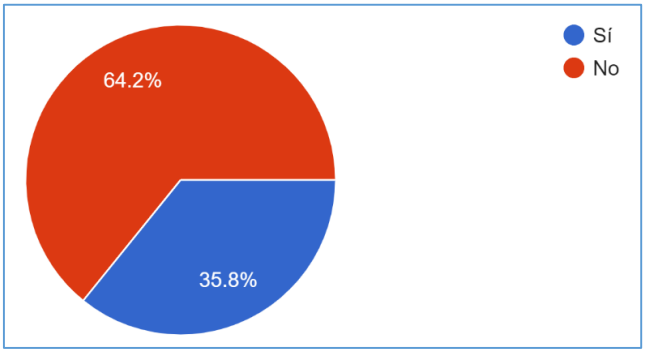


Figura 20. Respuestas encuesta a pregunta 10. ¿Se brindan cursos/jornadas de capacitación/concientización en seguridad informática en la organización en donde Ud. trabaja? (total 215)

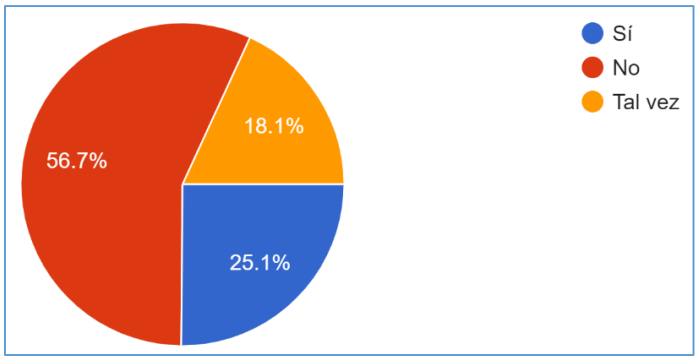


Figura 21. Respuestas encuesta a pregunta 11. ¿Alguna vez fue víctima de un problema de seguridad informática? (total 215)

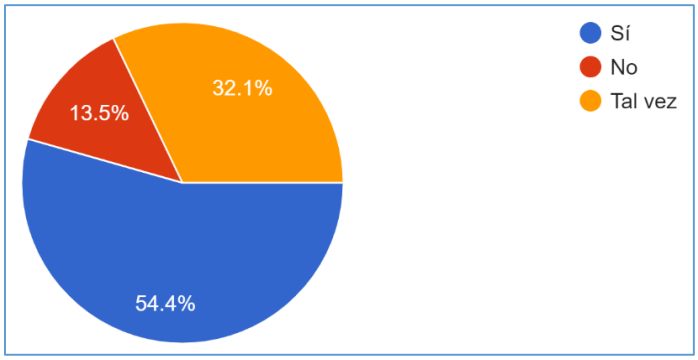


Figura 22. Respuestas encuesta a pregunta 12. ¿Asignaría tiempo y recursos para capacitarse en Seguridad Informática? (total 215)

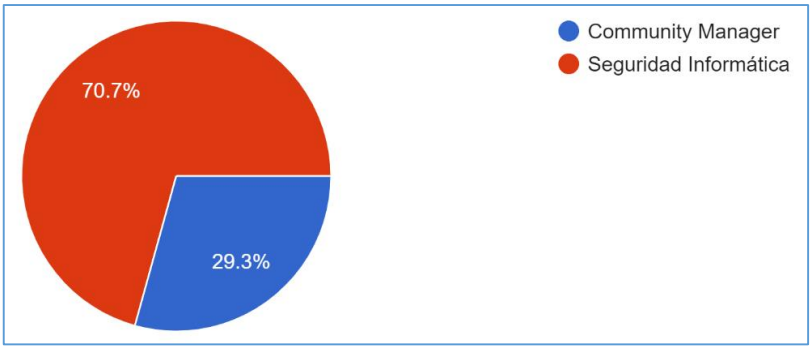


Figura 23. Respuestas encuesta a pregunta 13. Si en su trabajo le ofrecen una beca para realizar una capacitación, ¿cúal de estas dos opciones elegiría? (total 215)

La diversificación de casos de la muestra tomada, en cuanto a género, profesiones, oficios y edades nos da un indicio sobre la gran variedad de respuestas y opiniones con las que contaremos para analizar.

Podemos observar, que los encuestados estaban divididos aproximadamente en partes iguales entre hombres y mujeres; lo mismo sucede entre personas que trabajan en el sector público y el sector privado. Todas forman parte del ámbito laboral en distintas temáticas. El 23.7 % (51) de los encuestados se desempeñan en áreas relacionadas a la Informática, el 17.7% (38) en Administración, el 8.9% (19) en Educación, el 9.3% (20) en Legales, el 4.2% (9) en Recursos Humanos y el 45.1% (97) restante se divide en menores

proporciones en Medicina, Ventas, Ingeniería, Marketing, Idiomas, Logística, Psicología, Finanzas y otra diversidad de áreas.

De la totalidad de los encuestados, el 89.8% (193) posee un nivel medio a alto de involucramiento en el uso de las TIC en su ámbito laboral. Estos valores se mantienen constantes si observamos la parte de la población que posee título universitario. El 72.1% (155) de los encuestados posee estudios universitarios, dentro de los cuales el 34.4% (74) cuenta, además, con estudios de posgrado. En este caso, vemos que el 70.3% (109) sobre la totalidad de las personas con estudios universitarios posee un alto nivel de involucramiento en el uso de las TIC en su ámbito laboral y el 18.7% (29) posee un nivel medio de involucramiento, lo que representa el 89% de la población. En relación a la percepción sobre sus conocimientos en materia de seguridad informática, sobre la población universitaria, observamos que 28,39% (44) considera tener un nivel alto de conocimientos; el 33.55% (52) un nivel medio y 38.06% (59) un nivel bajo a nulo.

Las personas que trabajan en áreas no relacionadas con la informática representan el 76.28% (164) de los encuestados; dentro de esta porción, el 67.68% (111) posee un nivel alto de involucramiento con las TIC en su ámbito laboral, el 20.12% (33) un nivel medio y el 12.20% (20) un nivel bajo a nulo. De esta forma vemos que también el valor se mantiene similar al anterior caso, en un 87.8% (144), las personas poseen un nivel medio a alto en el involucramiento con las TIC en su ámbito laboral. Ahora, vamos a ver dentro de esta porción de encuestados, es decir, personas no informáticas, cuánto consideran conocer sobre seguridad informática. En este caso, observamos que el 17.07% (28) dice tener un nivel alto, el 35.98% (59) considera tener un nivel medio y el 46.95% (77) considera tener un nivel bajo a nulo.

Si miramos la porción de personas encuestadas que se desenvuelven en temáticas relativas a la Informática en su ámbito laboral, estas representan el 23.72% (51) de la totalidad. De las 51, el 54.9% (28) considera tener un nivel alto de conocimientos en ciberseguridad y 45.1% (23) posee un nivel medio a bajo. Por otro lado, de las 51 personas que trabajan en el ámbito informático, 21.5% (11) no realizan tareas relacionadas a la ciberseguridad, el 78.5% (40) realiza tareas relacionadas a la ciberseguridad. De estas 40, el 62.5% (25) considera tener un nivel alto de conocimientos en el tema y el restante 37.5% (15) considera tener un nivel medio a bajo. Además, de estas 40 personas informáticas que adquirieron sus conocimientos en ciberseguridad podemos distinguir que el 42.5% (17) lo han hecho en base a certificaciones y/o experiencia. De las 40 personas informáticas que además trabajan en ciberseguridad, el 60% (24) posee estudios universitarios o superiores,

dentro de ese 60%, hay un 33% (8) que adquirió sus conocimientos en ciberseguridad en base a estudios no universitarios, es decir, experiencia, certificaciones u otros medios.

Si miramos la totalidad de la población encuestada (215), vemos que el 41.4% (89) realizan tareas inherentes a la ciberseguridad, de los cuales el 45% (40) son informáticos y el 55% (49) pertenecen a otras ramas, tales como economía finanzas, legales, educación, administración, logística, entre otras. De estas 89 personas que trabajan en temas de ciberseguridad, 59.5% (53) han adquirido sus conocimientos en ciberseguridad en base a experiencia, certificaciones y otro medio no universitario, sin embargo, de esas 53 personas, el 60% (32) han alcanzado un nivel de estudios universitarios o superior, el 40% (21) restante sólo completaron estudios secundarios o terciarios.

Si observamos la parte de la población con carrera universitaria o superior, que no se desempeña en áreas informáticas (124), vemos que el 30% (37) tienen relación con la ciberseguridad, de los cuales el 65% (24) obtuvo ese conocimiento a través de certificaciones o experiencia, pero no de estudios universitarios de grado ni posgrado. Al mismo tiempo, de estas 37 personas, el 35% (13) considera tener un nivel alto de conocimientos en ciberseguridad y el restante 65% (24) considera tener un nivel medio a bajo de conocimientos en el tema.

De los 215 participantes, el 46.5% (100) trabaja en el sector público, 48.4% (104) en el sector privado y 5.10% (11) en otros. De las 100 personas del sector público, 45% (45) recibe capacitaciones en ciberseguridad en su lugar de trabajo, mientras que, en el sector privado, es del 28% (29).

De los 215 participantes, el 56,74% (122) dice no haber sido víctimas de un incidente de seguridad, mientras que el 43.25% (93) restante aseguran o supone la posibilidad de haber sido víctimas de un problema de seguridad alguna vez. Sobre las 93 personas de esta última condición, el 12% (11) no invertiría tiempo y recursos en realizar un curso de seguridad informática, y el 45% (5) de ellos preferiría un curso de *Community Manager*[16] aunque el curso de seguridad fuera ofrecido en su trabajo. En cambio, de las 93 personas que aseguran o podrían haber sido víctimas de un problema de seguridad, el 88% (82) estaría dispuesta o al menos lo pensarían, a asignar recursos a una capacitación en ciberseguridad, mientras que 74% (61) de esas 82 haría el curso de seguridad si se los ofreciera la empresa. De la totalidad

[16] *Community Manager* es la persona responsable de construir y administrar la comunidad online y gestionar la identidad y la imagen de marca, creando y manteniendo relaciones estables y duraderas con sus clientes. (https://www.iebschool.com/blog/que-es-un-community-manager-redes-sociales/)

de las 93 personas, el 72% (67) estaría dispuesta a realizar un curso de seguridad brindado por la organización en donde se desempeñan.

De las 122 personas que nunca fueron víctimas de un incidente de seguridad, 85% (104) estaría dispuestos o al menos lo pensarían, en invertir recursos en una capacitación en seguridad, además, el 70% (85) de ellos lo harían si la capacitación la ofreciera la empresa u organismo en donde trabajan. De este modo, observamos que la decisión de capacitarse en seguridad informática es levemente mayor luego de haber sufrido un incidente de seguridad.

Resumiendo, observamos que un alto porcentaje, cerca del 90% (193) de las personas utiliza las TIC en su ámbito laboral en un nivel medio a alto. A los fines del estudio, nos centraremos en la parte de la población con formación universitaria 72% (155). Las vamos a dividir en dos: los universitarios informáticos 20% (31) y los no informáticos 80% (124), como podemos observar en la siguiente figura:

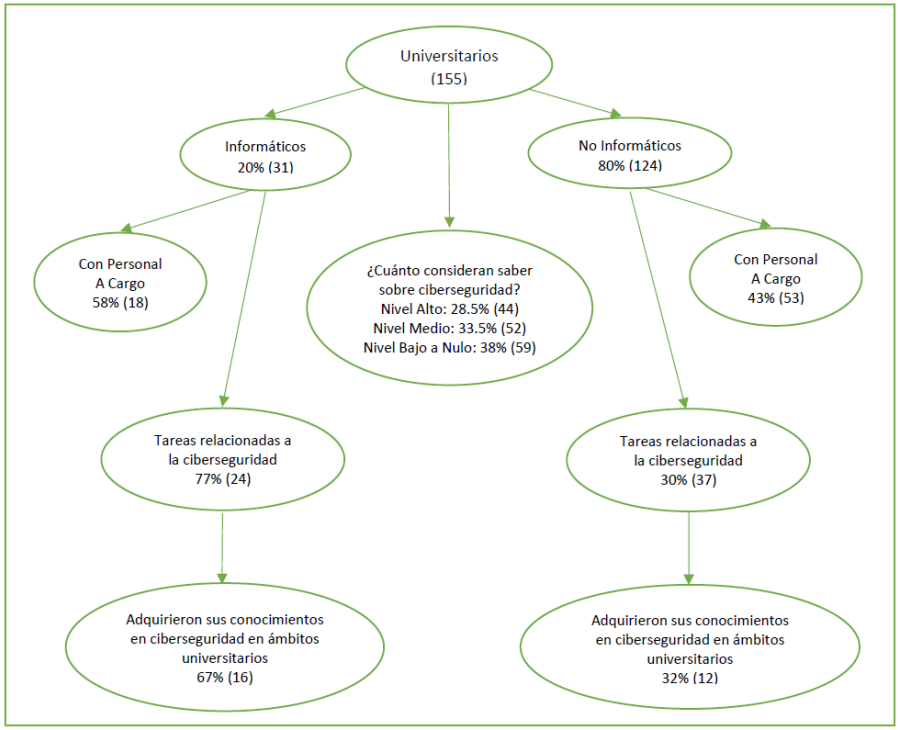


Figura 24. Resumen esquemático de la encuesta

Entonces, si miramos a los universitarios informáticos, el 58% (18) tienen personal a cargo. Por otro lado, 77% (24) de los 31 se desempeñan en tareas relacionadas a la ciberseguridad, 67% (16) adquirieró sus conocimientos en seguridad en un ámbito universitario, y 75% (12) de los 16 tienen personal a cargo. Vemos que aún existe una porción de personas que trabajan en temas relacionados a la ciberseguridad que a pesar de haber cursado una carrera universitaria no se formaron en la temática en el ámbito universitario.

Si nos centramos en los universitarios no informáticos (124), observamos que el 43% (53) tiene personal a cargo; por otro lado, vemos que cerca del 30% (37) del total desarrolla tareas relacionadas a la ciberseguridad, lo que habla de la intervención de personas de otros ámbitos en las tareas de seguridad, 51% (19) de ellos tienen personal a cargo, con lo cual ocupan puestos decisorios; de los 19 sólo el 31% (6) adquirieron sus conocimientos en ciberseguridad dentro del ámbito universitario. De los universitarios no informáticos que trabajan en temas de ciberseguridad sólo el 32% (12) adquirió sus conocimientos en el tema en un ámbito universitario.

En general, podemos observar que hay un bajo porcentaje (28.5%) de la población universitaria con conocimientos elevados sobre ciberseguridad. Que, además, muchos de ellos (45%), informáticos o no, ocupan puestos decisorios, con lo cual manejan información sensible para la empresa u organismo. Además, casi el 40% relaciona su trabajo con la ciberseguridad. De ellos, sólo el 46% adquirió esos conocimientos en el ámbito universitario. Es decir, que hay un 54% que se formó en ciberseguridad en base a la experiencia, certificaciones u otros medios no universitarios.

Por un lado, nos encontramos con un 38% de población universitaria, que tiene un nivel bajo a nulo de conocimientos en ciberseguridad. Por otro, vemos que hay un porcentaje alto (45%) de personas que ocupan puestos jerárquicos, de los cuales casi el 70% cuenta con nivel medio a nulo de conocimientos en ciberseguridad.

4.3.5 Situación de Organizaciones Respecto de Formación del Personal en Ciberseguridad.

A fin de completar la investigación se realizaron una serie de entrevistas a cuatro destacados referentes o gerentes de áreas de ciberdefensa y ciberseguridad en reconocidas instituciones de los ámbitos estatal y privado en nuestro país. En el Anexo L se puede observar la entrevista realizada el día 18 de agosto de 2021 al Sr Juan Bosoms, CSIRT Manager del Banco Macro S.A. En el Anexo M se puede observar la entrevista realizada el día 10 de septiembre de 2021 al Mg. Lic. Daniel Perles, *Engineer Development Director*[17] de Avaya. En el Anexo N se puede observar la entrevista realizada el día 15 de septiembre de 2021 al Sr. Oscar Niss, Subsecretario de Ciberdefensa del Ministerio de Defensa de la República Argentina. En el Anexo O se puede observar la entrevista realizada el día 27 de septiembre de 2021 al General de Brigada Aníbal Intini, Comandante Conjunto de

[17] *Engineer Development Director*, en castellano, Director de Desarrollos de Ingeniería.

Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas. Son de destacar algunas de las opiniones y conceptos vertidos por los expertos entrevistados.

Juan Bosoms explicó que es muy común que en empresas no haya técnicos con títulos universitarios, los que se especializan a través de certificaciones. Esto se debe a que consideran que en las carreras tradicionales tienen sistemas no actualizados, por eso se interesan más en las capacidades de las personas, sin embargo, comentó que: "Sería conveniente que todos los profesionales conozcan el abc de la ciberseguridad". La problemática de la escasez de personas con formación en ciberseguridad se da a nivel mundial, y fue en ascenso en los últimos años, ya a principios de 2020 se contemplaba un porcentaje de demanda insatisfecha del 32%.

Daniel Perles comentó que las personas de su empresa cuentan con formación universitaria y dado que es una empresa de tecnología, todos se mantienen actualizados a través de cursos y certificaciones. Respecto de las ofertas académicas en materia de ciberseguridad considera que actualmente están mejorando y hay nuevas alternativas en carreras de grado y posgrado sin embargo piensa que: "falta formación en áreas duras de cibersoldados para estar a la altura de grupos de hackers chinos, rusos, APT, etc".

Oscar Niss expresó, por su parte, las dificultades que tiene el Estado para retener gente capacitada, por los costos que ello implica. Explicó: "Si comparamos con países de la región, Paraguay, Bolivia, Chile, Uruguay o Perú, estamos muy bien posicionados en formación de recursos humanos en ciberseguridad". Sin embargo, en referencia al personal no técnico, considera que, en una escala de 1 a 10, la formación en el uso seguro de tecnologías está en 3 puntos. Sobre la formación, considera conveniente que abarque a personas no técnicas, que puedan integrar equipos de ciberseguridad. Que el personal técnico, además de contar con una formación más dura, también debe ser parte de la concientización. Además, comentó: "Respecto a la capacitación, ayuda a mitigar el riesgo, por lo tanto, también los incidentes".

Aníbal Intini, por su parte, comentó la situación particular de las Fuerzas Armadas. En este ámbito la formación incluye a las personas de todos los cuadros, es decir a todas las disciplinas. Al igual que en otros lugares, se da una alta rotación de gente por la volatilidad de los jóvenes, en este caso soldados. Uno de los hitos más importantes que se promovieron desde el Comando Conjunto de Ciberdefensa en materia de formación de RR.HH. fue la creación del Instituto de Ciberdefensa de las FF.AA. desde el año 2021 cuyo objetivo es "centralizar el esfuerzo en la capacitación en ciberdefensa en las Fuerzas Armadas, concientizar en los niveles formativos, y especializar a los cuadros permanentes y al personal

civil, lo que contribuirá eficazmente a la excelencia operativa de los integrantes de las organizaciones en ciberdefensa". El Instituto promueve la formación del personal de las Fuezas Armadas y del Ministerio de Defensa que desempeñan funciones en el ámbito de la Ciberdefensa. Además, destacó que se observa un crecimiento de la red, y, por ende, de las amenazas y las vulnerabilidades.

En las respuestas de los entrevistados en general, observamos que el personal que trabaja en esas áreas, es técnico, con conocimientos muy específicos en ciberseguridad. Si bien entre las personas hay quienes se formaron en carreras universitarias como licenciaturas o ingenierías relacionadas a la tecnología o a la informática, son muy pocos los que tienen algún tipo de posgrado en el tema. En general, todos coinciden en que la formación específica en ciberseguridad la adquirieron a través de certificaciones y capacitación continua, incluida la autodidacta.

En las empresas privadas, se observa que la normativa obliga a cumplir con capacitaciones en seguridad a todo el personal, inclusive para las personas que no son técnicos informáticos, y se da un seguimiento a través de exámenes. No sucede lo mismo en organismos estatales. De este modo, la percepción de las autoridades sobre los conocimientos en ciberseguridad de las personas en general, son mejores en los lugares en donde se da una capacitacón constante, lo que también proporciona un ambiente de concientización en el tema.

Respecto de las ofertas de formación en ciberseguridad en nuestro país, en general destacan que, si bien están en aumento, faltaría una capacitación más dura para un nivel específicamente técnico. Además, coinciden en la necesidad de una capacitación que abarque todas las disciplinas, ya sea para que profesionales de otras ramas integren equipos de ciberseguridad o que para que sepan y tomen conciencia de los incidentes de seguridad que pueden tener al manejar la tecnología o incluso infraestructuras críticas.

Por último, respecto de los ciberataques, como se puede observar en otros ámbitos, también se han incrementado en sus organizaciones, pero todos coinciden en que la capacitación de las personas es una herramienta más que ayuda a mitigar el riesgo. En particular, en las empresas en donde la formación es continua, se observa una respuesta positiva de la gente en ese sentido.

4.4 Comprobación Lógica de la Hipótesis.

Para realizar la comprobación de la hipótesis se consideraron los siguientes aspectos transcendentes:

- La metodología empleada para verificar en forma lógica las hipótesis;

- El marco teórico que sustentó las afirmaciones orientadoras de la investigación;
- Los instrumentos aplicados para la obtención de datos considerados válidos y confiables: Análisis de planes de estudio de carreras de grado en España y Argentina; resultados de la encuesta sobre la formación de las personas en ciberseguridad y entrevistas realizadas a importantes directores o gerentes de áreas de ciberdefensa y ciberseguridad en reconocidas instituciones de nuestro país;
- El análisis e interpretación de los datos en relación a la obtención de respuestas a las preguntas planteadas en la hipótesis.

Con lo anteriormente expresado, se tiene la firme convicción de que los aportes en la capacitación de las personas que incluyan a la ciberseguridad dentro de la oferta educativa, permitirán tener organizaciones más seguras y mejorar el posicionamiento del país sobre el tema.

Por lo tanto, la hipótisis central que señala que la formación académica disponible en nuestro país en materia de ciberseguridad resulta poco adecuada para las personas que se desempeñan en distintos ámbitos laborales en la Argentina, en línea con las necesidades actuales frente a la revolución tecnológica que vivimos, queda debidamente comprobada.

5. Conclusiones.

Durante el desarrollo del marco teórico se explicaron los conceptos de ciberseguridad esenciales para exponer los fundamentos básicos en los que se basó la investigación. En segundo lugar, vimos cuáles son las tecnologías y herramientas de la cuarta revolución industrial y cómo impactan las transformaciones digitales en distintos entornos y los problemas asociados. Se mostraron, luego, los riesgos y vulnerabilidades que se presentan a raíz de fallas o debilidades, en particular, las humanas. Por último, se presentaron distintas propuestas existentes a nivel estatal y privado, que muestran la importancia del concepto de la educación como una herramienta fundamental para mitigar los riesgos, minimizar los incidentes y lograr un ambiente laboral ciberseguro y ciberresiliente.

Durante el desarrollo de la investigación se utilizaron diferentes técnicas a fin de evaluar la hipótesis presentada. Entre ellas, se describieron algunos de los ciberataques sucedidos en los últimos tiempos producto de debilidades humanas; se exploraron los planes de estudio de carreras seleccionadas en España, como el país de habla hispana mejor posicionado en el ranking global elaborado por la ITU, y de Argentina. A través de un análisis cuantitativo, se evaluaron los resultados de la encuesta realizada sobre la formación de las personas en ciberseguridad. Y, por último, se utilizó el método cualitativo con entrevistas como herramienta para analizar la percepción de especialistas en la temática.

A partir del diagnóstico de los resultados, que dan respuesta a las preguntas que acompañan la hipótesis comprobamos de este modo, que la formación académica disponible en nuestro país en materia de ciberseguridad resulta poco adecuada para las personas que se desempeñan en distintos ámbitos laborales en la Argentina, en línea con las necesidades actuales frente a la revolución tecnológica que vivimos.

A partir de la investigación, se aprecian tres perfiles en los que podemos dividir a los profesionales respecto de las necesidades de formación en Ciberseguridad:

Profesional no informático: Persona dedicada a cualquier actividad diferente a la informática que utiliza las tecnologías como herramienta de apoyo a sus labores diarias.

Profesional Informático: Persona no especializada en ciberseguridad, que desarrolla su actividad en alguna rama de la informática, entre las que se destacan: microinformática, desarrollo de software, diseño web, soporte técnico de redes, administración de centrales telefónicas, administración de usuarios.

Profesional de Ciberseguridad: Persona especializada en ciberseguridad.

La ciberseguridad es una temática que nos atraviesa a todos. Las certificaciones y la formación continua, no tradicional, son necesarias para mantenerse actualizado a diario, sobre todo en lo que atañe al personal de tecnología, porque continuamente evolucionan las técnicas y procedimientos de ataque, al mismo ritmo o incluso más rápido que el avance de la innovación tecnológica y de las contramedidas, técnicas y herramientas destinadas a mitigar incidentes. La educación en ciberseguridad debe acompañar a los nuevos roles profesionales que surgen. La universidad debe sentar las bases para adquirir ese conocimiento y hoy por hoy es un punto débil.

Problemáticas actuales como la pandemia aceleraron las nuevas formas de trabajo como el teletrabajo. Más allá de las recomendaciones brindadas como las que suele emitir el INCIBE en España habitualmente, o blogs como segu-info en nuestro país, o publicaciones de expertos, se necesitan tomar medidas de fondo. Son muchas las cuestiones a mejorar, desde la educación inicial, la secundaria, la actualización de profesionales, entre otros. En este trabajo nos hemos centrado en los nuevos profesionales a fin de que obtengan los conocimientos básicos para desempeñar una vida laboral cibersegura con las condiciones para el aprendizaje que surgirá con la evolución de las tecnologías. Sea cual sea la profesión, todos estarán atravesados por las tecnologías de la información y de este modo podremos sumar un eslabón más en la cadena de ciberseguridad. No sólo resulta beneficioso a nivel

personal sino también a nivel laboral, empresarial y como suma de todos los esfuerzos, a nivel nacional, posicionando a nuestro país en un escalafón más alto en la materia.

De esta forma se busca preparar a las nuevas generaciones de profesionales para que tengan una titulación acorde a las nuevas necesidades del mercado, que cuenten con los conocimientos básicos para afrontar una vida laboral cibersegura, como orientadores hacia el resto de las personas, que incorporen hábitos cibersaludables e incluso tengan la posibilidad de conformar equipos decisores y cumplir funciones relacionadas a la ciberseguridad en empresas privadas u organismos estatales. Cada uno de nosotros, desde nuestro lugar puede realizar aportes a la ciberseguridad.

Además, si bien para trabajar en ciberseguridad se exigen ciertas habilidades o certificaciones, los tomadores de decisiones suelen ser profesionales de diversas ramas, e incluso los equipos que atienden temas de ciberdefensa o ciberseguridad son multidisciplinarios, conformados por licenciados en ciencias políticas, en recursos humanos, abogados, economistas o ingenieros, entre otros. A partir de estos conceptos y del análisis efectuado, se desprende la necesidad de contar con materias atinentes a la ciberseguridad de carácter obligatorio en carreras de grado, tanto informáticas como no informáticas.

A continuación, se desarrollan las propuestas resultantes sobre la adecuación de los planes de estudio para las carreras universitarias de grado. Estos aportes ayudarán a mejorar el posicionamiento a nivel mundial de Argentina en materia de ciberseguridad.

Además, se sientan las bases para una futura investigación sobre cómo implementar las propuestas resultantes, las que podrían personalizarse según los intereses particulares de cada carrera.

6. Propuestas.

A continuación, se definen los lineamientos básicos a tener en cuenta en el contenido de las materias a incorporar en las distintas carreras de grado para la formación de las personas en ciberseguridad en nuestro país, relacionados directamente con los perfiles definidos. Los contenidos propuestos son los mínimos a ofrecer a los alumnos, para que los futuros profesionales cuenten con las herramientas básicas para realizar su importante aporte a la ciberseguridad. Además, esos contenidos son generales; de este modo, queda abierta la posibilidad de personalización de algunas temáticas, como puede ser el abordaje de casos reales con una orientación según la especialidad y los intereses propios de cada carrera. En el caso de las carreras informáticas, se propone agregar esos contenidos mínimos de carácter obligatorio, los que podrán, luego, desarrollarse más ampliamente con las materias de carácter optativo.

La formación básica en ciberseguridad para el profesional informático más allá de las actualizaciones que deberían abordar durante el ejercicio de su carrera, queda enmarcada dentro de las recomendaciones realizadas sobre la incorporación de dos (2) materias obligatorias en los planes de estudio de las carreras de grado: Ciberseguridad Básica y Ciberseguridad Avanzada.

La formación básica en ciberseguridad, para el profesional no informático queda enmarcadas dentro de las recomendaciones realizadas sobre la incorporación de una materia obligatoria y una optativa en los planes de estudio de las carreras de grado: Introducción a la Ciberseguridad (obligatoria) y Ciberseguridad para No Informáticos (optativa).

En cuanto a los profesionales de Ciberseguridad, la propuesta es agregar un módulo específico compuesto por cuatro (4) materias, en las carreras de tecnología/informática que sirva para formar profesionales con Orientación en Ciberseguridad, dentro de las carreras de grado. Cabe destacar, que se contemplan como incluídas dentro de la orientación las dos materias obligatorias previamente definidas para los planes de estudio de carreras informáticas. Las materias específicas de la orientación en ciberseguridad propuestas son: Introducción a la Criptografía; Auditoría; Seguridad en Software y Seguridad en Redes.

El esquema propuesto con los lineamientos básicos es el siguiente:

a) Carreras Informáticas.

Ciberseguridad Básica: Conceptos básicos asociados a la ciberdefensa y ciberseguridad; principios básicos de la seguridad informática: disponibilidad, integridad, confidencialidad, no repudio, autenticación, control de acceso; infraestructuras críticas; seguridad en internet de las cosas; machine learning; inteligencia artificial; big data; soluciones basadas en la nube vs *on premise*[18]; VPN; seguridad física y seguridad lógica; fraudes; lavado de activos; cibercrimen; teletrabajo seguro, herramientas de seguridad (backups, plan de continuidad del negocio); factores de autenticación (gestión de identitades); ciberataques: malware, phishing, inyección SQL, cross site scripting, denegación de servicios; tipos de malware: virus, troyanos, gusanos, spyware, adware; botnet; ingeniería social; robo de identidad; ciberbulling; sextorsión; grooming.

Ciberseguridad Avanzada: Desarrollo seguro de aplicaciones; seguridad en redes; casos reales de ciberataques; resiliencia; actualidad de la ciberseguridad; gestión de

[18] *On-premise* o en local se refiere al tipo de instalación de una solución de software, la cual se lleva a cabo dentro del servidor y la infraestructura (TIC) de la empresa. (https://www.ticportal.es/glosario-tic/on-premise)

la ciberseguridad; auditoría; normativa vigente; técnicas/métodos criptográficos; hacking ético.

b) Carreras No informáticas.

Introducción a la Ciberseguridad: Conceptos básicos asociados a la ciberdefensa y ciberseguridad; principios básicos de la seguridad informática: disponibilidad, integridad, confidencialidad, no repudio, autenticación, control de acceso; ciberamenazas; herramientas de seguridad: backups, VPN; conceptos básicos de criptografía; ciberataques; phishing; factores de autenticación (gestión de identidades); tipos de malware: virus, troyanos, gusanos, spyware, adware; botnets; ingeniería social; robo de identidad; ciberbulling; sextorsión; grooming.

Ciberseguridad para No informáticos: Normativa legal vigente; revisión de casos reales de ciberataques; formas de mitigación; buenas prácticas en el uso de correo electrónico e internet; uso de contraseñas; redes sociales; seguridad en teléfonos móviles; seguridad en el teletrabajo.

c) Orientación en Ciberseguridad en carreras informáticas.

Introducción a la Criptografía: Tipos de criptografía; algoritmos criptográficos; firma digital; certificados digitales; blockchain.

Auditoría: Normas de auditoría; normas legales; seguridad física y seguridad lógica; políticas de seguridad; análisis de riesgos; plan de continuidad del negocio.

Seguridad en Software: Seguridad en el ciclo de vida del desarrollo de software; seguridad en sistemas operativos; seguridad por diseño; seguridad en bases de datos; análisis de malware; validación de seguridad de sistemas; detección de ataques de días cero; ingeniería inversa.

Seguridad en Redes: Seguridad en el diseño*;* VLANs; Redes definidas por software o SDN, Redes privadas virtuales o VPN; Sistema de detección de intrusiones o IDS; Sistema de prevención de intrusiones o IPS; tests de penetración; análisis de tráfico; protección DDOS; seguridad en la nube; protocolos de comunicaciones.

7. Bibliografía y Referencias.

Arano Chávez, R.M., Delfín Beltrán, L.A., Escudero Macluf, J. (2016). Una necesidad en las empresas: La ciberseguridad. *Revista electrónica de Investigación de la Universidad de Xapala*, no. Especial, pp. 56-66.

Berkeley University of California. (s.f.). *How to Protect Against SQL Injection Attacks*. https://security.berkeley.edu/education-awareness/how-protect-against-sql-injection-attacks

Blažič, B.J. (2021). Cybersecurity Skills in EU: New Educational Concept for Closing the Missing Workforce Gap. En *Cybersecurity Threats with New Perspectives.* https://www.intechopen.com/online-first/75922

Blockchain Federal Argentina. (s.f.). *Blockchain*. https://bfa.ar/index.php/blockchain/blockchain

Bobadilla, J. (2020). *Machine Learning y Deep Learning: Usando Python, Scikit y Keras*. Ediciones de la U.

Comando Conjunto de Ciberdefensa. (s.f.). Estado Mayor Conjunto de las Fuerzas Armadas. http://fuerzas-armadas.mil.ar/ComandoConjuntoDeCiberdefensa/Mision.aspx

Corletti Estrada, A. (2011). *Seguridad Por Niveles.* https://darfe.es/index.php/es/nuevas-descargas/category/3-libros

Corletti Estrada, A. (2017). *Ciberseguridad (Una Estrategia Informático/Militar).* https://darfe.es/index.php/es/nuevas-descargas/category/3-libros

Decreto 50 de 2019 [Presidencia de la Nación Argentina]. Por medio del cual se aprueba el Organigrama de Aplicación de la Administración Nacional centralizada hasta nivel de Subsecretaría. 19 de diciembre de 2019. B.O. No. 34266.

Decreto 480 de 2019 [Presidencia de la Nación]. Por medio del cual se crea el Comité de Ciberseguridad. 11 de julio de 2019. B.O. No. 34152.

Decreto 577 de 2017 [Presidencia de la Nación]. Por medio del cual se crea el Comité de Ciberseguridad en la órbita del Ministerio de Modernización. 28 de julio de 2017. B.O. No. 33677.

Dirección Nacional de Ciberseguridad. (s.f.). Jefatura de Gabinete de Ministros. https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad

Directiva 2008/114/CE [Consejo de la Unión Europea]. Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. 8 de diciembre de 2008. DOUE-L-2008-82589.

Escolano, F., Cazorla, M.A., Alfonso, M.I., Colomina, O. y Lozano, M.A. (2003). *Inteligencia Artificial. Modelos, Técnicas y Áreas de Aplicación*. Thomson Ediciones Spain.

González Barrales, O. (2016). Ciberseguridad, retos y prospectiva. *Revista electrónica de Investigación de la Universidad de Xapala*, no. Especial, pp. 132-143.

Hernández Rodríguez, C., Cano Flores, M., García López, T. (2016). La universidad y su relación con la ciberseguridad. *Revista electrónica de Investigación de la Universidad de Xapala*, no. Especial, pp. 94-107.

Higuera, A. (23 de marzo de 2021). *Cuidado con la última estafa de phishing: se hacen pasar por la DGT y te envían un correo electrónico con una multa*. 20 minutos. https://www.20minutos.es/noticia/4629217/0/cuidado-con-la-ultima-estafa-de-phishing-se-hacen-pasar-por-la-dgt-y-te-envian-un-correo-electronico-con-una-multa/

Instituto Nacional de Ciberseguridad. (2016). *Ciberseguridad en la identidad digital y la reputación online: Una guía de aproximación para el empresario*. https://www.incibe.es/protege-tu-empresa/guias/guia-ciberseguridad-identidad-online

Instituto Nacional de la Administración Pública. (s.f.). INAP. Portal de Capacitación. Jefatura de Gabinete de Ministros. https://capacitacion.inap.gob.ar/

International Telecommunication Union. (2019). *Global Cibersecurity Index 2018*. https://www.itu.int/pub/D-STR-GCI.01-2018/es

International Telecommunication Union. (2021). *Global Cibersecurity Index 2020*. https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

Jaimovich, D. (22 de abril de 2021). *Apple, víctima de un ataque de ransomware: le piden USD 50 millones para no revelar los diseños secretos de productos*. Infobae. https://www.infobae.com/america/tecno/2021/04/22/apple-victima-de-un-ataque-de-ransomware-le-piden-usd-50-millones-para-no-revelar-los-disenos-de-las-nuevas-macbooks/

Joyanes Aguilar, L. (2017). Ciberseguridad: La colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0. *Cuaderno de estrategia 185*. *Ciberseguridad: la cooperación público-privada*. http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2017/Cuaderno_185.html

Kizza, J.M. (2017). *Guide to Computer Network Security (Computer Communications and Networks).* (4ª Ed.). En A.J. Sammes (Ed.). Centre for Forensic Computing - Cranfield University.

Leiva, M. (21 de septiembre de 2019). *Posgrados 2020: ¿Cuánto cuesta estudiar en la Argentina?* Ámbito. https://www.ambito.com/economia/educacion/posgrados-2020-cuanto-cuesta-estudiar-la-argentina-n5055682

Ministerio de Justicia y Derechos Humanos. (03 de diciembre de 2018). *Recaudos a tener en cuenta para no ser víctima de "sextorsión"*. https://www.argentina.gob.ar/noticias/recaudos-tener-en-cuenta-para-no-ser-victima-de-sextorsion

Ministerio de Justicia y Derechos Humanos. (s.f.). *Justicia Cerca. Acoso por Internet.* https://www.argentina.gob.ar/justicia/derechofacil/aplicalaley/acoso-internet

Ministerio de Justicia y Derechos Humanos. (s.f.). *¿Qué es un adware?* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-adware

Ochoa, M. (11 de diciembre de 2020). *Los ciberataques que marcaron el 2020*. IT Masters Mag. https://www.itmastersmag.com/noticias-analisis/los-ciberataques-que-marcaron-el-2020/

Proyecto de Ley. Creación del Instituto de Ciberseguridad Argentino (INCIBAR). Expediente S-30/21. https://www.senado.gob.ar/

Ramos, D.R., Olivera Gómez, D.A. (2016). Las amenazas cibernéticas. *Revista electrónica de Investigación de la Universidad de Xapala*, no. Especial, pp. 35-55.

Resolución 781 de 2015 [Ministerio de Defensa]. Por medio de la cual se aprueba la Política de Seguridad de la jurisdicción Ministerio de Defensa. 24 de julio de 2015.

Resolución 829 de 2019 [Secretaría de Gobierno de Modernización]. Por medio de la cual se aprueba la Estrategia Nacional de Ciberseguridad. 24 de mayo de 2019.

Rodríguez Llerena, A. E. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, pp. 116-131.

Santiago, E.J. y Sánchez Allende, J. (2017). Riesgos de Ciberseguridad en las Empresas, *Tecnologí@ y Desarrollo. Revista de Ciencia Tecnología y Medio Ambiente, Volumen XV*. https://revistas.uax.es/index.php/tec_des/article/view/1174/964

Schwab, K. (2016). *La cuarta revolución industrial.* Penguin Random House Grupo Editorial. https://books.google.com.ar/books

Unión Internacional de Telecomunicaciones. (2008). *Recomendación UIT–T X.1205. Aspectos generales de la ciberseguridad.* https://www.itu.int/rec/T-REC-X.1205-200804-I/es

Webometrics. (2021). *Ranking web de universidades*. https://www.webometrics.info/es

8. Anexos.

Anexo A - Diez universidades mejores rankeadas de España con sus sitios web.

Universidad	Sitio Web
Universidad de Barcelona	https://www.ub.edu/web/portal/es/
Universidad Autónoma de Barcelona	https://www.uab.cat/es/
Universidad de Valencia	https://www.uv.es/castellano
Universidad de Granada	https://www.ugr.es/
Universidad Autónoma de Madrid	http://www.uam.es/UAM/Home.htm?language=es
Universidad de Sevilla	https://www.us.es/
Universidad Politécnica de Catalunya BarcelonaTech	https://www.upc.edu/es
Universidad Pompeu Fabra	https://www.upf.edu/
Universidad Politécnica de Valencia	http://www.upv.es/
Universidad Politécnica de Madrid	https://www.upm.es/

Anexo B - Materias atinentes a ciberseguridad en carreras de grado de Derecho en las universidades seleccionadas en España.

Universidad	Institución	Carrera de grado	Materias atinentes a la Ciberseguridad
Universidad de Barcelona	Facultad de Derecho	Grado en Derecho	No se observan
Universidad Autónoma de Barcelona	Facultad de Derecho	Grado en Derecho	No se observan
Universidad de Valencia	Facultad de Derecho	Grado en Derecho	No se observan
Universidad de Granada	Facultad de Derecho	Grado en Derecho	No se observan
Universidad Autónoma de Madrid	Facultad de Derecho	Grado en Derecho	No se observan
Universidad de Sevilla	No posee	No posee	No se observan

Universidad Politécnica de Catalunya BarcelonaTech	Facultad de Derecho	Grado en Derecho	No se observan
Universidad Pompeu Fabra	Facultad de Derecho	Grado en Derecho	Optativa: Derecho de las Telecomunicaciones y de las Nuevas Tecnologías
Universidad Politécnica de Valencia	No posee	No posee	No se observan
Universidad Politécnica de Madrid	No posee	No posee	No se observan

Anexo C - Materias atinentes a ciberseguridad en carreras de grado de Economía en las universidades seleccionadas en España.

Universidad	Institución	Carrera de grado	Materias atinentes a la Ciberseguridad
Universidad de Barcelona	Facultad de Economía y Empresa	Grado en Economía	No se observan
Universidad Autónoma de Barcelona	Facultad de Economía y Empresa	Grado en Economía	No se observan
Universidad de Valencia	Facultad de Economía	Grado en Economía	No se observan
Universidad de Granada	Facultad de Ciencias Económicas y Empresariales	Grado en Economía	No se observan
Universidad Autónoma de Madrid	Facultad de Ciencias Económicas y Empresariales	Grado en Economía	No se observan
Universidad de Sevilla	Facultad de Ciencias Económicas y Empresariales	Grado en Economía	No se observan
Universidad Politécnica de Catalunya BarcelonaTech	Escuela Técnica Superior de Ingeniería Industrial de Barcelona	Grado en Tecnologías Industriales y Análisis Económico	No se observan
Universidad Pompeu Fabra	Facultad de Economía y Empresa	Grado en Economía	No se observan
Universidad Politécnica de Valencia	No posee	No posee	No se observan

Universidad Politécnica de Madrid	No posee	No posee	No se observan

Anexo D - Materias atinentes a ciberseguridad en carreras de grado relacionadas a Informática en las universidades seleccionadas en España.

Universidad	Facultad	Carrera de grado	Materias atinentes a la Ciberseguridad
Universidad de Barcelona	Facultad de Matemáticas e Informática	Grado en Ingeniería Informática	No se observan.
Universidad Autónoma de Barcelona	Escuela de Ingeniería	Grado en Ingeniería Informática	Obligatorias: Información y Seguridad; Garantía de la Información y Seguridad en la Intensificación de Sistemas de Información y en Tecnologías de la Información.
Universidad de Valencia	Escuela Técnica Superior de Ingeniería	Grado en Ingeniería Informática	Obligatorias: Seguridad Informática
Universidad de Granada	Escuela Técnica Superior de Ingeniería Informática y Telecomunicaciones	Grado en Ingeniería Informática con menciones en Computación y Sistemas Inteligentes; Ingeniería de computadores; Ingeniería del software; Sistemas de información y Tecnologías de la información	Obligatoria: Seguridad y protección de sistemas informáticos; Optativas: Criptografía y computación (especialidad Computación y Sistemas Inteligentes); Seguridad en Sistemas Operativos (especialidad Ingeniería del Software); Recuperación de Información; Derecho Informático.

Universidad Autónoma de Madrid	Escuela Politécnica Superior	Grado en Ingeniería Informática	Optativas: Fundamentos de Criptografía y Seguridad Informática
Universidad de Sevilla	Escuela Técnica Superior de Ingeniería Informática – Facultad de Matemáticas	Doble Grado en Ingeniería Informática – Tecnologías Informáticas y en Matemáticas	Optativas: Criptografía; Teoría de Códigos y Criptografía; Seguridad en Sistemas Informáticos y en Internet
Universidad de Sevilla	Escuela Técnica Superior de Ingeniería Informática	Grado en Ingeniería Informática – Mención "Sistemas de Información" / "Tecnología de la Información" / Computación	Optativas: Criptografía; Seguridad en Sistemas Informáticos y en Internet
Universidad Politécnica de Catalunya BarcelonaTech	Facultad de Informática de Barcelona	Bachelor's degree in Bioinformatics (interuniversitario UPF-UPC-UB)	No se observan
Universidad Politécnica de Catalunya BarcelonaTech	Escuela Politécnica Superior de Ingeniería de Manresa (EPSEM)	Grado en Ingeniería de Sistemas TIC	Optativas: Gestión de Calidad y de Sistemas Integrados Calidad/Seguridad/ Medio Ambiente; Seguridad y Secreto en la Codificación de la Información
Universidad Politécnica de Catalunya BarcelonaTech	Facultad de Informática de Barcelona (FIB) - Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona (ETSETB) -	Grado en Ciencia e Ingeniería de Datos	No se observan

	Facultad de Matemáticas y Estadística (FME)		
Universidad Politécnica de Catalunya BarcelonaTech	Facultad de Informática de Barcelona (FIB)	Grado en Ingeniería Informática - Menciones: Computación / Ingeniería de Computadores / Ingeniería del Software / Sistemas de Información / Tecnologías de la Información	Obligatoria: Seguridad Informática (sólo para la mención Tecnologías de la Información) Optativas: Computación y criptografía cuánticas; Criptografía; Gestión de la Ciberseguridad.
Universidad Politécnica de Catalunya BarcelonaTech	Escuela Politécnica Superior de Ingeniería de Vilanova i la Geltrú	Grado en Ingeniería Informática - Mención: Tecnologías de la Información	Obligatoria: Seguridad y Administración de Redes; Optativa: Recuperación de la Información
Universidad Pompeu Fabra	Escuela de Ingeniería	Grado en Ingeniería en Informática	Obligatoria: Criptografía y Seguridad Optativas: Seguridad en Computadoras; Recuperación de la información y análisis de la web
Universidad Politécnica de Valencia	Escuela Técnica Superior de Ingeniería Informática	Grado en Ingeniería Informática	Optativas: Seguridad en los Sistemas Informáticos; Sistemas de almacenamiento y recuperación de la Información; Seguridad en redes y sistemas informáticos; Ciberseguridad en dispositivos móviles; Criptografía; Hacking ético; Quantum

			Computing; Seguridad web; Social web behaviour & network analysis
Universidad Politécnica de Valencia	Escuela Técnica Superior de Alcoy	Grado en Ingeniería Informática	Optativas: Seguridad en los Sistemas Informáticos; Seguridad en redes y sistemas informáticos
Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos	Doble Grado en Ingeniería de Computadores y en Tecnologías para la Sociedad de la Información	Obligatorias: Fundamentos de Seguridad; Seguridad de la Información; Seguridad en Sistemas y Redes
Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingenieros Informáticos	Doble Grado en Ingeniería Informática y en Administración y Dirección de Empresas	Obligatorias: Fundamentos de Seguridad; Seguridad de la Información; Seguridad en Sistemas y Redes
Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos	Doble Grado en Ingeniería del Software y en Tecnologías para la Sociedad de la Información	Obligatorias: Fundamentos de Seguridad; Seguridad de la Información; Seguridad en Sistemas y Redes
Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos	Grado en Ingeniería de Computadores	Obligatorias: Fundamentos de Seguridad; Seguridad de la Información; Seguridad en Sistemas y Redes
Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingenieros Informáticos	Grado en Ingeniería Informática	Obligatoria: Seguridad de las Tecnologías de la Información

Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingenieros Informáticos	Grado en Matemáticas e Informática	Optativa: Teoría de Códigos y Criptografía
Universidad Politécnica de Madrid	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos	Grado en Sistemas de Información	Obligatorias: Fundamentos de Seguridad; Seguridad de la Información; Auditoría y Control de TI Optativas: Seguridad en Sistemas y Redes

Anexo E - Diez universidades mejores rankeadas de Argentina con sus sitios web.

Universidad	Sitio Web
Universidad de Buenos Aires	http://www.uba.ar/
Universidad Nacional de la Plata	https://unlp.edu.ar/
Universidad Nacional de Mar del Plata	http://www2.mdp.edu.ar/
Universidad Nacional del Centro de la Provincia de Buenos Aires	https://www.unicen.edu.ar/
Universidad Nacional de Tucumán	http://www.unt.edu.ar/
Universidad Tecnológica Nacional	https://utn.edu.ar/es/
Universidad Nacional de Córdoba	https://www.unc.edu.ar/
Universidad Nacional de Quilmes	http://www.unq.edu.ar/
Universidad Nacional de San Juan	http://www.unsj.edu.ar/
Universidad Nacional de San Luis	http://unsl.edu.ar/

Anexo F - Materias atinentes a ciberseguridad en carreras de grado de Derecho en las universidades seleccionadas en Argentina.

Universidad	Institución	Carrera de grado	Materias atinentes a la Ciberseguridad
Universidad de Buenos Aires	Facultad de Derecho	Abogacía	No se observan.
Universidad Nacional de la Plata	Facultad de Ciencias Jurídicas y Sociales	Abogacía	No se observan
Universidad Nacional de Mar del Plata	Facultad de Derecho	Abogacía	Obligatoria: Inteligencia Artificial, Tecnología y Derecho
Universidad Nacional del Centro de la Provincia de Buenos Aires	Facultad de Derecho	Abogacía	No se observan

Universidad Nacional de Tucumán	Facultad de Derecho y Ciencias Sociales	Abogacía	No se observan
Universidad Tecnológica Nacional	No posee	No posee	No se observan
Universidad Nacional de Córdoba	Facultad de Derecho	Abogacía	Optativas: Informática; Cibercrimen
Universidad Nacional de Quilmes	No posee	No posee	No se observan
Universidad Nacional de San Juan	Facultad de Ciencias Sociales	Abogacía	No se observan
Universidad Nacional de San Luis	Facultad de Ciencias Económicas, Jurídicas y Sociales	Abogacía	Optativa: Derechos Informáticos

Anexo G - Materias atinentes a ciberseguridad en carreras de grado de Economía en las universidades seleccionadas en Argentina.

Universidad	Institución	Carrera de grado	Materias atinentes a la Ciberseguridad
Universidad de Buenos Aires	Facultad de Ciencias Económicas	Licenciatura en Economía	No se observan
Universidad Nacional de la Plata	Facultad de Ciencias Económicas	Licenciatura en Economía	No se observan
Universidad Nacional de Mar del Plata	Facultad de Ciencias Económicas y Sociales	Licenciatura en Economía	No se observan
Universidad Nacional del Centro de la Provincia de Buenos Aires	Facultad de Ciencias Económicas	Licenciatura en Economía Empresarial	Obligatorias: Tecnologías de Información Optativas: Control y Seguridad Informática
Universidad Nacional de Tucumán	Facultad de Ciencias Económicas	Licenciatura en Economía	No se observan
Universidad Tecnológica Nacional	No posee	No posee	No se observan
Universidad Nacional de Córdoba	Facultad de Ciencias Económicas	Licenciatura en Economía	No se observan
Universidad Nacional de Quilmes	Departamento de Economía y Administración	Licenciatura en Economía del Desarrollo	No se observan
Universidad Nacional de San Juan	Facultad de Ciencias Sociales	No posee	No se observan

Universidad Nacional de San Luis	Facultad de Ciencias Ecomómicas, Jurídicas y Sociales	No posee	No se observan

Anexo H - Materias atinentes a ciberseguridad en carreras de grado relacionadas a Informática en las universidades seleccionadas en Argentina.

Universidad	Institución	Carrera de grado	Materias atinentes a la Ciberseguridad
Universidad de Buenos Aires	Facultad de Ingeniería	Ingeniería en Informática	Optativas: Criptografía y Seguridad Informática
Universidad de Buenos Aires	Facultad de Ingeniería	Licenciatura en Análisis de Sistemas	Optativas: Criptografía y Seguridad Informática; Auditoría de Sistemas
Universidad de Buenos Aires	Facultad de Ciencias Económicas	Licenciatura en Sistemas de Información de las Organizaciones	Obligatorias: Auditoría y Seguridad de los Sistemas de Información;
Universidad de Buenos Aires	Facultad de Ciencias Exactas y Naturales	Licenciatura en Ciencias de la Computación	Optativas: Seguridad de la Información; Criptografía; Criptología
Universidad Nacional de La Plata	Facultad de Informática	Licenciatura en Informática	Optativas: Desarrollo Seguro de Aplicaciones; Introducción a la Forensia Digital; Seguridad y Privacidad en Redes; Introducción a la Ciberseguridad
Universidad Nacional de La Plata	Facultad de Informática	Licenciatura en Sistemas	Optativas: Desarrollo Seguro de Aplicaciones; Introducción a la Forensia Digital; Seguridad y Privacidad en Redes; Introducción a la Ciberseguridad

Universidad Nacional de La Plata	Facultad de Informática/Facultad de Ingeniería	Ingeniería en Computación	Optativas: Desarrollo Seguro de Aplicaciones; Seguridad y Privacidad en Redes
Universidad Nacional de Mar del Plata	Facultad de Ingeniería	Ingeniería en Computación	Obligatorias: Seguridad en Redes de Computadoras
Universidad Nacional de Mar del Plata	Facultad de Ingeniería	Ingeniería en Informática	Optativas: Gestión de la Seguridad Informática
Universidad Nacional del Centro de la Provincia de Buenos Aires	Facultad de Ciencias Exactas /Facultad de Ingeniería/Unidad de Enseñanza Universitaria de Quequén	Ingeniería en Sistemas	No se observan
Universidad Nacional de Tucumán	Facultad de Ciencias Exactas	Ingeniería en Computación	No se observan
Universidad Nacional de Tucumán	Facultad de Ciencias Exactas	Licenciatura en Informática	No se observan
Universidad Tecnológica Nacional	Facultad Regional Buenos Aires/ Concepción del Uruguay/Córdoba/Delta/ La Plata/Mendoza/ Resistencia/Rosario/ San Francisco/Santa Cruz/ Santa Fe/Trenque Lauquen/Tucumán/ Venado Tuerto/ Villa María	Ingeniería en Sistemas de Información	Optativas: Seguridad Informática; Seguridad en Redes; Criptografía; Ciberseguridad Industrial; Pericias Informáticas; Seguridad Activa de las Comunicaciones; Seguridad en Aplicaciones Web
Universidad Nacional de Córdoba	Facultad de Matemática, Astronomía, Física y Computación	Licenciatura en Ciencias de la Computación	Optativas: Seguridad
Universidad Nacional de Córdoba	Facultad de Ciencias Exactas, Físicas y Naturales	Ingeniería en Computación	No se observan
Universidad Nacional de Quilmes	Departamento de Ciencia y Tecnología	Licenciatura en Informática	Obligatoria: Derechos de Autor y Derechos de Copia en la Era Digital

Universidad Nacional de San Juan	Facultad de Ciencias Exactas, Físicas y Naturales	Licenciatura en Sistemas de Información	Obligatorias: Inteligencia Artificial; Auditoría de Sistemas de Información
Universidad Nacional de San Juan	Facultad de Ciencias Exactas, Físicas y Naturales	Licenciatura en Ciencias de la Computación	Obligatoria: Inteligencia Artificial
Universidad Nacional de San Luis	Facultad de Ciencias Físico, Matemáticas y Naturales	Ingeniería en Computación	Obligatoria: Seguridad y Medio Ambiente Optativas: Introducción a la Seguridad de Redes; Seguridad y Calidad de Servicios en Redes; Ciberseguridad; Op. Seguridad de Sistemas de Software
Universidad Nacional de San Luis	Facultad de Ciencias Físico, Matemáticas y Naturales	Ingeniería en Informática	Obligatorias: Seguridad y Medio Ambiente; Auditoría Informática; Calidad y Certificación del Proceso y del Producto de Software
Universidad Nacional de San Luis	Facultad de Ciencias Físico, Matemáticas y Naturales	Licenciatura en Ciencias de la Computación	Obligatoria: Aspectos Legales, Sociales, Auditoría y Peritaje Informáticos Optativas: Ciberseguridad; Op. Seguridad de Sistemas de Software; Introducción a la Seguridad de Redes

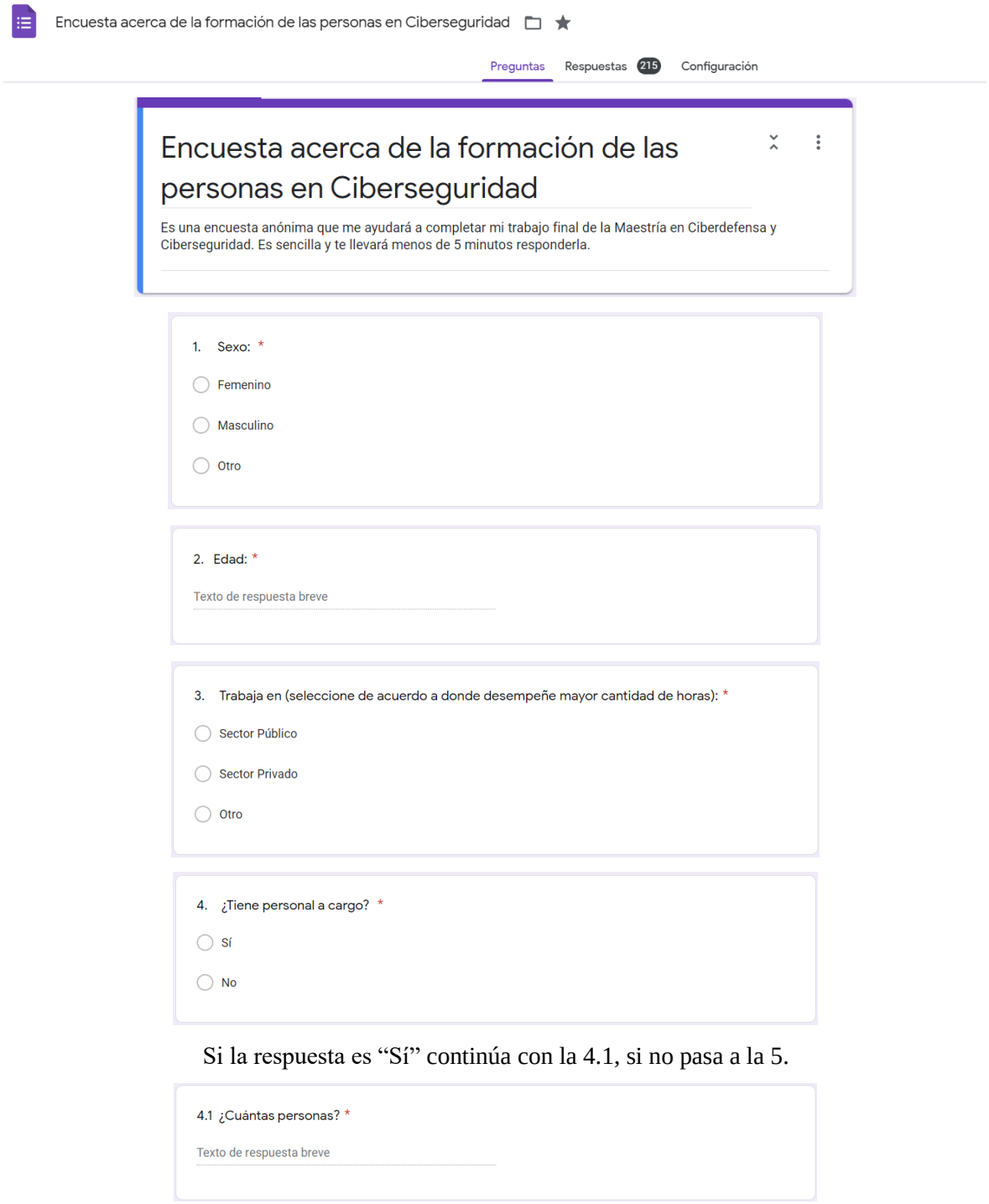
Anexo I - Carreras relacionadas a la ciberseguridad en las 10 universidades mejores rankeadas de Argentina y la Universidad de la Defensa Nacional.

Universidad	Institución	Titulación	Requisitos
Universidad de Buenos Aires	Facultad de Ingeniería / Facultad de Ciencias	Especialista en Seguridad Informática de la	Antecedentes académicos y profesionales atinentes

	Económicas / Facultad de Ciencias Exactas	Universidad de Buenos Aires	
Universidad de Buenos Aires	Facultad de Ingeniería / Facultad de Ciencias Económicas / Facultad de Ciencias Exactas	Magister en Seguridad Informática de la Universidad de Buenos Aires	Antecedentes académicos y profesionales atinentes
Universidad de Buenos Aires	Facultad de Ciencias Económicas	Magister de la Universidad de Buenos Aires en Ciberdefensa y Ciberseguridad	Profesionales de todas las disciplinas a desempeñarse en posiciones de liderazgo
Universidad Nacional de La Plata	Facultad de Informática https://unlp.edu.ar/	Especialista en Redes y Seguridad	Profesionales de Informática e Ing. Electrónica
Universidad de la Defensa Nacional	Facultad de Ingeniería del Ejército https://www.fie.undef.edu.ar/ o Centro Regional Universitario Córdoba IUA https://www.iua.edu.ar/	Especialista en Criptografía y Seguridad Teleinformática	Profesionales Ingenieros, Electrónicos, Informáticos o de Sistemas y también a Matemáticos, Físicos, Ingeniero Electricista y/o Electromecánico que acrediten haber trabajado en esta Especialidad o posean conocimientos suficientes sobre estas disciplinas
Universidad de la Defensa Nacional	Facultad de Ingeniería del Ejército https://www.fie.undef.edu.ar/ o Centro Regional Universitario Córdoba IUA https://www.iua.edu.ar/	Magister en Ciberdefensa	Articulación con la Especialidad en Criptografía y Seguridad Teleinformática

Anexo J - Encuesta sobre la formación de las personas en ciberseguridad realizada a 215 participantes entre los días 06 y 16 de septiembre de 2021.

Link de acceso: (https://docs.google.com/forms/d/e/1FAIpQLSfmGPOeGwVBMjoTbc_rp8Ak890EwcDjha8vjt96brxwg2fSxA/viewform?usp=sf_link)



Si la respuesta es “Sí” continúa con la 4.1, si no pasa a la 5.

5. Máximo nivel de estudios alcanzado: *

- ○ Primario
- ○ Secundario
- ○ Terciario
- ○ Universitario
- ○ Posgrado (Especialización, Maestría o Doctorado)

6. ¿En qué área se desempeña dentro de su ámbito laboral? *

- ○ Administración
- ○ Recursos Humanos
- ○ Informática
- ○ Legales
- ○ Otra...

7. ¿Cuán involucrado está en el uso de tecnologías de información y comunicación (TIC) en su ámbito laboral? *

- ○ Mucho
- ○ Suficiente
- ○ Algo
- ○ Poco
- ○ Nada

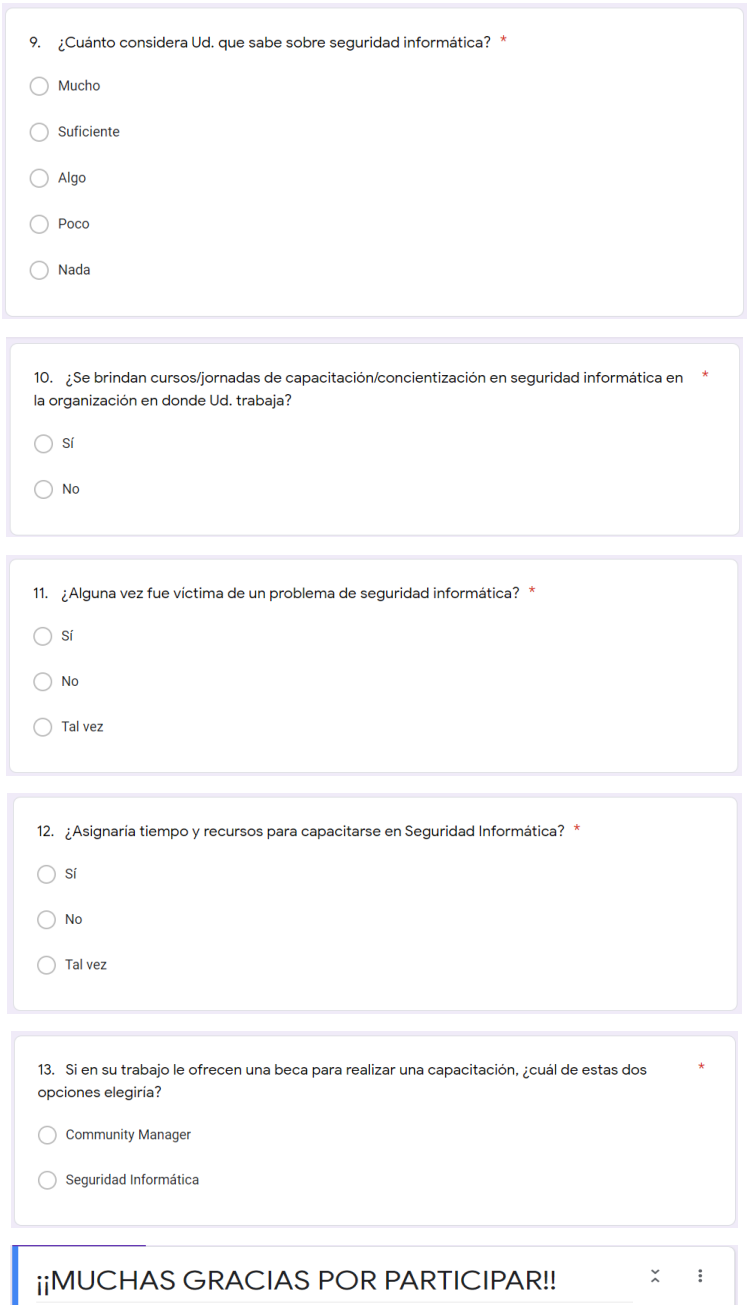
8. ¿Su trabajo está relacionado de alguna forma a la seguridad informática? *

- ○ Sí
- ○ No

Si la respuesta es “Sí” continúa con la 8.1, si no pasa a la 9.

8.1 ¿De qué forma o a través de qué medio adquirió conocimientos en ciberseguridad? *

- ☐ Estudios universitarios
- ☐ Especializaciones
- ☐ Maestría
- ☐ Certificaciones
- ☐ Experiencia
- ☐ Otros



Anexo K – Muestreo, correpondiente al 10% de la encuesta realizada sobre la formación de las personas en Ciberseguridad.

	Marca temporal	1.Sexo:	2. Edad:	3.Trabaja en (seleccione de acuerdo a donde desempeñe mayor cantidad de horas):	4.¿Tiene personal a cargo?	4.1 ¿Cuántas personas?	5.Máximo nivel de estudios alcanzado:	6.¿En qué área se desempeña dentro de su ámbito laboral?	7.¿Cuán involucrado está en el uso de tecnologías de información y comunicación (TIC) en su ámbito laboral?
1									
2	9/7/2021 15:03:42	Femenino	54	Sector Público	Sí	40	Posgrado (Especialización, Maestría o Doctorado)	Informática	Mucho
3	9/7/2021 16:34:42	Femenino	24	Sector Privado	No		Universitario	Administración	Algo
4	9/7/2021 18:32:52	Femenino	51	Sector Público	No		Posgrado (Especialización, Maestría o Doctorado)	Comercial	Suficiente
5	9/8/2021 17:34:01	Masculino	42	Sector Público	No		Universitario	Telecomunicaciones	Algo
6	9/8/2021 18:21:08	Femenino	51	Sector Público	No		Universitario	Administración	Nada
7	9/8/2021 23:21:23	Femenino	24	Sector Privado	Sí	4	Posgrado (Especialización, Maestría o Doctorado)	Administración	Suficiente
8	9/9/2021 17:55:48	Masculino	61	Sector Privado	No		Universitario	Informática	Mucho
9	9/9/2021 18:21:34	Femenino	53	Sector Privado	No		Universitario	Administración	Suficiente
10	9/9/2021 22:29:34	Femenino	27	Sector Público	No		Universitario	Educación	Suficiente
11	9/11/2021 14:22:05	Otro	61	Sector Público	No		Universitario	Recursos Humanos	Suficiente
12	9/11/2021 17:20:46	Masculino	63	Sector Público	Sí	9	Posgrado (Especialización, Maestría o Doctorado)	Informática	Mucho
13	9/11/2021 18:03:34	Femenino	34	Sector Público	Sí	10	Universitario	Legales	Algo
14	9/11/2021 19:53:52	Femenino	54	Sector Público	No		Posgrado (Especialización, Maestría o Doctorado)	Legales	Nada
15	9/12/2021 16:13:50	Masculino	52	Sector Privado	Sí	10	Universitario	Informática	Mucho
16	9/12/2021 18:24:01	Femenino	44	Sector Público	Sí	30	Universitario	Administración	Algo
17	9/12/2021 20:32:29	Masculino	58	Sector Público	Sí	8	Universitario	Informática	Mucho
18	9/12/2021 20:49:47	Femenino	43	Sector Público	No		Universitario	Infraestructura	Algo
19	9/13/2021 13:07:31	Femenino	49	Sector Privado	No		Posgrado (Especialización, Maestría o Doctorado)	Psicología	Algo
20	9/14/2021 13:17:52	Femenino	46	Sector Privado	Sí	5	Posgrado (Especialización, Maestría o Doctorado)	Administración	Nada
21	9/16/2021 11:48:45	Masculino	61	Sector Público	No		Posgrado (Especialización, Maestría o Doctorado)	Educación Universitaria	Mucho
22	9/16/2021 12:18:20	Masculino	58	Sector Público	Sí	32	Posgrado (Especialización, Maestría o Doctorado)	Informática	Mucho

	Marca temporal	8.¿Su trabajo está relacionado de alguna forma a la seguridad informática?	8.1 ¿De qué forma o a través de qué medio adquirió conocimientos en ciberseguridad?	9.¿Cuánto considera Ud. que sabe sobre seguridad informática?	10. ¿Se brindan cursos/jornadas de capacitación/concientización en seguridad informática en la organización en donde Ud. trabaja?	11.¿Alguna vez fue víctima de un problema de seguridad informática?	12.¿Asignaría tiempo y recursos para capacitarse en Seguridad Informática?	13.Si en su trabajo le ofrecen una beca para realizar una capacitación, ¿cuál de estas dos opciones elegiría?
1								
2	9/7/2021 15:03:42	Sí	Especializaciones, Maestría, Experiencia	Suficiente	No	Sí	Sí	Seguridad Informática
3	9/7/2021 16:34:42	No		Poco	Sí	Sí	Sí	Seguridad Informática
4	9/7/2021 18:32:52	Sí	Experiencia	Algo	Sí	Sí	Sí	Seguridad Informática
5	9/8/2021 17:34:01	Sí	Especializaciones	Algo	Sí	No	Sí	Seguridad Informática
6	9/8/2021 18:21:08	No		Nada	No	No	Tal vez	Community Manager
7	9/8/2021 23:21:23	No		Algo	Sí	No	Tal vez	Seguridad Informática
8	9/9/2021 17:55:48	Sí	Experiencia	Mucho	No	No	Sí	Seguridad Informática
9	9/9/2021 18:21:34	No		Nada	Sí	No	No	Seguridad Informática
10	9/9/2021 22:29:34	No		Poco	Sí	No	Sí	Seguridad Informática
11	9/11/2021 14:22:05	Sí	Estudios universitarios, Especializaciones, Experiencia, Otr	Suficiente	No	No	Sí	Seguridad Informática
12	9/11/2021 17:20:46	Sí	Especializaciones	Suficiente	Sí	Sí	Sí	Seguridad Informática
13	9/11/2021 18:03:34	No		Poco	Sí	No	No	Seguridad Informática
14	9/11/2021 19:53:52	No		Nada	No	Tal vez	No	Community Manager
15	9/12/2021 16:13:50	Sí	Especializaciones, Experiencia, Otros	Mucho	No	No	Sí	Seguridad Informática
16	9/12/2021 18:24:01	No		Nada	No	No	Sí	Seguridad Informática
17	9/12/2021 20:32:29	Sí	Especializaciones	Algo	No	Tal vez	Sí	Community Manager
18	9/12/2021 20:49:47	No		Nada	No	No	Tal vez	Community Manager
19	9/13/2021 13:07:31	No		Algo	No	No	Tal vez	Community Manager
20	9/14/2021 13:17:52	No		Nada	No	No	Sí	Seguridad Informática
21	9/16/2021 11:48:45	Sí	Estudios universitarios	Suficiente	Sí	Sí	Tal vez	Seguridad Informática
22	9/16/2021 12:18:20	Sí	Estudios universitarios, Maestría	Mucho	Sí	Sí	Sí	Seguridad Informática

Anexo L - Entrevista realizada al Sr. Juan Bosoms, CSIRT Manager del Banco Macro S.A, el día 18 de agosto de 2021.

1. Cantidad de Personal a cargo:

   Treinta (30).

2. En cuanto al personal a su cargo:

   2.1 ¿Qué tipo de nivel alcanzado de formación tienen? ¿Grado? ¿Posgrado? ¿Especializaciones? ¿Certificaciones?

   Aproximadamente, el 20% cuenta con carreras de grado, el 10% con carreras de pregrado (tecnicaturas) y el 70% con certificaciones.

   2.2 ¿Estos estudios tiene que ver con tecnología/informática/ciberseguridad?

   Las personas que cuentan con títulos de pregrado y grado se dividen en carreras de ingeniería y licenciaturas en sistemas, carreras tradicionales. Los conocimientos en ciberseguridad los adquieren a través de las certificaciones. Es muy común que en determinadas áreas en los bancos no haya gente con títulos universitarios, son autodidactas y se especializan a través de certificaciones. Algunas fuentes dicen que empresas como Google, por ejemplo, tienen un porcentaje muy alto de técnicos que no tienen título universitario. Ellos lo atribuyen a que en las carreras tradicionales ven sistemas no actualizados, por eso se interesan más en las capacidades que tienen las personas para pensar y la experiencia en resolver problemas, en el área de ciberseguridad. El problema es que hay especialistas en seguridad a los que continuamente le están cambiando las formas de ataque, por eso una persona que ocupa un puesto de esas características tiene que tener sed de aprender diariamente.

   2.3 ¿El personal de su área realiza periódicamente capacitaciones/actualizaciones en ciberseguridad? ¿De qué tipo o a través de qué medios?

   Sí, constantemente el personal de ciberseguridad realiza capacitaciones. Lo hacen a través de variadas plataformas o sistemas. Puede ser a través de MOOCs (Udemy,

Coursera, Udacity, etc), de manera autodidacta o de certificaciones específicas de seguridad informática reconocidas internacionalmente con *hands on*[19] en sistemas vigentes. Todas en modalidad on-demand desde Internet.

Otras formas de entrenamientos que utilizamos mucho son los CTFs, competencias llamadas capture the flags, en donde se ponen a prueba los conocimientos técnicos en exploits de vulnerabilidades y criptoanálisis. Se hacen compitiendo contra otros equipos, por tiempo y orden de resolución. Suelen realizarse entre entidades financieras organizados por PRISMA u otras organizaciones a nivel global. Algunos son gratuitos y otros pagos.

2.4 ¿Considera suficiente la cantidad de personal especializado con que cuenta el área?

No, y es una problemática a nivel mundial. Cuando viajé en 2016 a Silicon Valley, en donde estuve con gente de HP y Micro Focus ya hablaban de un 17% de trabajo que no habían podido cumplir a nivel EE.UU., incluso contando con gente de otros países como Irlanda, México e India. En 2017 visité el área de Seguridad de Cisco Talos[20], es otra empresa distinta, en la otra costa de EE.UU. y hablaban de un 24% de demanda insatisfecha, es decir trabajos de ciberseguridad no cubiertos. A principios de 2020, estuve en la RSA Conference[21] en San Francisco, en donde comentaron que el porcentaje había subido a un 32%.

3. En la organización en donde ud. trabaja, se brindan cursos/jornadas de capacitación/concientización en Ciberseguridad Sí/No

Sí.

3.1 ¿A quiénes está destinado? ¿A personal jerárquico, técnicos, informático, personal en general, otros?

Está destinada a todo el personal, es uno de los puntos auditados por el ente regulador. En todos los bancos es obligatoria la capacitación en ciberseguridad, como lo es en prevención y control de lavado de capitales y terrorismo, e incluso se toman exámenes a medida que se avanza en la capacitación.

3.2 ¿Se incluye en las capacitaciones a personal de otras disciplinas no informáticas?

Sí, las capacitaciones están destinadas a todas las personas que trabajan en el banco.

[19] *Hands on* es una terminología que proviene del inglés y significa "poner las manos sobre" y se relaciona a la experiencia de campo en cierta temática.

[20] Cisco Talos es uno de los equipos de inteligencia de amenazas comerciales más grandes del mundo, compuesto por investigadores, analistas e ingenieros de clase mundial. (https://www.cisco.com/c/en/us/products/security/talos.html)

[21] RSA Conference o conferencia RSA es donde el mundo habla de seguridad. Es el medio para facilitar las conversaciones entre los profesionales de la ciberseguridad del mundo sobre preocupaciones, ideas y soluciones actuales y futuras. Genera eventos globales y contenido de ciberseguridad en línea durante todo el año. Debe su nombre a los tres cofundadores de la compañía: Ron Rivest, Adi Shamir, y Leonard Adleman. (https://www.rsaconference.com/usa)

4. ¿Cuál es su percepción sobre el resto del personal de la Empresa, Organismo o Fuerza respecto de los conocimientos que tienen en materia de ciberseguridad?

   Son las personas que reciben capacitación por e-learnig y las campañas de concientización. Además, suelen realizarse ataques de fishing para poner a prueba sus conocimientos, con esto demuestran que tienen un nivel inicial aceptable.

5. ¿Cuál es su opinión sobre las ofertas de formación académica en materia de ciberseguridad en nuestro país?

   Existen diplomaturas y maestrías que alcanzan para lograr un nivel de conocimiento general en ciberseguridad, de nivel analista. No alcanza para un nivel técnico especializado que tenga que responder a incidentes reales de relativa complejidad, ni para reunir la experiencia necesaria para cubrir puestos en CSIRTs o SOCs.

6. ¿Considera necesaria una formación multidisciplinaria en el tema?

   Sería aconsejable que el resto de las carreras que no son de ingeniería cuenten con al menos dos materias, podría ser una materia obligatoria y otra optativa, o dos optativas, de ciberseguridad. Hoy por hoy, la tecnología atraviesa todas las profesiones, por ejemplo, en el área de medicina, un ataque de ransomware podría afectar a todos los equipos de un sanatorio. Si las personas tuviesen una formación básica en ciberseguridad, cuidarían esos activos, no llevarían un pendrive, no harían click en cualquier correo. El profesional podría tener los conocimientos como para no cometer errores que puedan llevar a desactivar todo un hospital, por ejemplo. Sería conveniente que todos los profesionales conozcan el abc de la ciberseguridad.

7. ¿Piensa que entender en seguridad de la información podría ayudar a hacer más amigable y seguro el uso de las tecnologías a las personas en general?

   Sí, es una necesidad y debido al contexto pandemia y a la cantidad de ciberfraudes, es común que la mayoría de la población si no fue víctima de un fraude, haya estado en contacto cercano con algún damnificado. El público en general está tomando mayor conciencia.

8. ¿Qué percepción tiene respecto de ciberataques? ¿Se han incrementado en su organización? ¿La capacitación de las personas ayudó a mitigar los efectos de los incidentes que se detectaron?

   Los ciberataques se han incrementado en el último tiempo y mutan diariamente. Las campañas de concientización llegan y mitigan al menos un poco la cantidad de incidentes. Se observa un efecto social importante, cuando las personas llaman al área de seguridad incluso por falsos positivos, o cuando comentan entre ellos sobre un correo

que les llegó, y alguien les dice a dónde llamar o qué hacer. Se va propagando el conocimiento dentro del entorno de la organización.

Anexo M - Entrevista realizada al Mg. Lic. Daniel Perles, Engineer Development Director de Avaya, el día 10 de septiembre de 2021.

1. Cantidad de Personal a cargo:

   Diez (10) personas.

2. En cuanto al personal a su cargo:

   2.1 ¿Qué tipo de nivel alcanzado de formación tienen? ¿Grado? ¿Posgrado? ¿Especializaciones? ¿Certificaciones?

   Todos cuentan con formación universitaria. Algunos cuentan con carreras de posgrado. Al tratarse de una empresa de tecnología, todos cuentan con certificaciones específicas sobre temas relacionados a la ciberseguridad.

   2.2 ¿Estos estudios tiene que ver con tecnología/informática/ciberseguridad?

   Sí, la formación universitaria es en carreras afines como licenciatura en Ciencias de la Computación. También, hay personas formadas en la maestría en Ciberdefensa y Ciberseguridad. Las personas que trabajan en la empresa se encuentran en distintas partes del mundo, como India o EE.UU. Las certificaciones que se acreditan son sobre tecnología en general y también sobre temas de seguridad, ambas de carácter internacional.

   2.3 ¿El personal de su área realiza periódicamente capacitaciones/actualizaciones en ciberseguridad? ¿De qué tipo o a través de qué medios?

   Sí, continuamente.

   A través de distintas plataformas. Algunos ejemplos son: *Ethical Hacker*; *SIPsense*; Cisco; *Avaya Profesional*; *Amazon Web Service*; *Google Cloud*; *Linux*.

   Si bien estos cursos o certificaciones no son todos de ciberseguridad, salvo los de *Ethical Hacker* o *Cisco Security Profesional*, el resto son genéricos de cada producto que se trate en particular y todos tienen algún componente o módulo relacionado a la ciberseguridad. Tal es el caso, por ejemplo, de las capacitaciones de *Amazon Web Services*, en cada módulo o tema siempre se cubren todos los aspectos de seguridad relacionados.

   Respecto a productos tecnológicos que la misma empresa desarrolla, también se estudian los componentes de seguridad de los mismos.

   2.4 ¿Considera suficiente la cantidad de personal especializado con que cuenta el área?

   Sí.

3. En la organización en donde ud. trabaja, ¿se brindan cursos/jornadas de capacitación/concientización en Ciberseguridad Sí/No?

   Sí.

   3.1 ¿A quiénes está destinado? ¿A personal jerárquico, técnicos, informático, personal en general, otros?

   Se brindan cursos a todo el personal en general. Estos cursos son tercerizados, online, interactivos y con exámenes obligatorios. Educan sobre ciberseguridad en general, el manejo de la información en la empresa, cómo se comparte, cómo cuidarla, cómo tratar los mails, mensajes, phishing, ransomware, etc.

   3.2 ¿Se incluye en las capacitaciones a personal de otras disciplinas no informáticas?

   Sí, todo el personal de la empresa. El curso de obligatorio y se envía un curso nuevo cada seis (6) meses.

4. ¿Cuál es su percepción sobre el resto del personal de la Empresa, Organismo o Fuerza respecto de los conocimientos que tienen en materia de ciberseguridad?

   En mi caso se trata de una empresa de desarrollo de software y producción de comunicaciones, es por ello que 70% del personal es técnico y conoce bien el tema de ciberseguridad. El otro 30% conoce al menos los temas que se ven en los cursos online semestrales y obligatorios.

5. ¿Cuál es su opinión sobre las ofertas de formación académica en materia de ciberseguridad en nuestro país?

   Actualmente están mejorando y hay nuevas alternativas en carreras de grado y posgrado. Creo que falta formación en áreas duras de cibersoldados para estar a la altura de grupos de hackers chinos, rusos, APT, etc.

6. ¿Considera necesaria una formación multidisciplinaria en el tema?

   Sí, siempre es importante.

7. ¿Piensa que entender en Seguridad de la información podría ayudar a hacer más amigable y seguro el uso de las tecnologías a las personas en general?

   Sí, por supuesto.

8. ¿Qué percepción tiene respecto de ciberataques? ¿Se han incrementado en su organización? ¿La capacitación de las personas ayudó a mitigar los efectos de los incidentes que se detectaron?

   En el caso de mi organización no ha habido ataques significativos pues existe un área específica de ciberseguridad que esta a la altura de las circunstancias.

En mi parecer, creo que las personas al recibir la capacitación son más conscientes. Van aprendiendo, se van acostumbrando. Por ejemplo, el tema del ransomware, lo aprenden, si bien la empresa tiene un filtro para evitar que pasen, se ve una respuesta de las personas. Además, el tema de tener que dar fe de lo que leyeron en el curso, de la severidad en la responsabilidad, hace que sean más conscientes de los riesgos. Se acerca a un tema legal.

Anexo N - Entrevista realizada al Sr. Oscar Niss, Subsecretario de Ciberdefensa del Ministerio de Defensa de la República Argentina, el día 15 de septiembre de 2021.

1. Cantidad de Personal a cargo:

   Veinticinco (25)

2. En cuanto al personal a su cargo:

   2.1 ¿Qué tipo de nivel alcanzado de formación tienen? ¿Grado? ¿Posgrado? ¿Especializaciones? ¿Certificaciones?

   Aproximadamente el 20% cuenta con estudios de grado y certificaciones. El resto del personal son jóvenes que están cursando su carrera de grado. Lamentablemente en el estado es muy difícil contar con personas altamente especializadas por los costos que ello implica. Los estudiantes de carreras universitarias que recién comienzan tienen ideas y muchas ganas de hacer y aprender, pero una vez que adquieren conocimientos importantes y obtienen su título es muy difícil retenerlos. También muchos se capacitan de manera autodidacta, sobre todo los más jóvenes.

   2.2 ¿Estos estudios tiene que ver con tecnología/informática/ciberseguridad?

   En general son carreras de sistemas, ingenierías o licenciaturas en informática, sólo algunos casos en particular tienen o cursan algún posgrado específico en Ciberseguridad. Incluso, recién ahora algunas universidades están lanzando algunas carreras de grado en Ciberseguridad.

   2.3 ¿El personal de su área realiza periódicamente capacitaciones/actualizaciones en ciberseguridad? ¿De qué tipo o a través de qué medios?

   Sí, la formación se promueve permanentemente en el área. Semanalmente, el personal toma cursos de manera online. Son brindados por empresas de tecnología como IBM. Algunos son promocionados por otros países. Por ejemplo, en estos momentos hay dos capacitaciones en curso, una de España, y otra que se obtuvo por intermedio de embajada de EE.UU.

   2.4 ¿Considera suficiente la cantidad de personal especializado con que cuenta el área?

Definitivamente no, necesitaría más. Una problemática es concientizar al decisor, a la persona con la potestad de contratar gente sobre la importancia de esto. En Ciberseguridad y Ciberdefensa como en Tecnología en general, el 70% es capacidad y talento, el resto es hardware y software que se pueden comprar.

3. En la organización en donde ud. trabaja, se brindan cursos/jornadas de capacitación/concientización en Ciberseguridad Sí/No

   No, sólo se ha promovido alguna capacitación los años anteriores, pero debería ser más intensivo.

4. ¿Cuál es su percepción sobre el resto del personal de la Empresa, Organismo o Fuerza respecto de los conocimientos que tienen en materia de ciberseguridad?

   Creo que es lo mismo que sucede fuera de la jurisdicción también. Si tomamos una escala de 1 a 10, yo considero que la formación en el uso seguro de tecnologías está en 3 puntos. Creo que hacen falta más campañas de concientización, de formación y de capacitación. Creo que esto debe comenzar desde la educación primaria, así como hay educación vial o educación sexual, debería haber educación cibernética o digital de manera tal que cuando sean adolescentes o mayores y estén en un ámbito laboral sean conscientes. Así como aprendieron a no cruzar la calle con un semáforo en rojo, no pueden abrir un mail del cual desconocen su remitente.

5. ¿Cuál es su opinión sobre las ofertas de formación académica en materia de ciberseguridad en nuestro país?

   Considero que es buena la oferta, tanto a nivel formal en universidades o de instituciones particulares. Obviamente como es una materia nueva, va a ir mejorando con el tiempo. Incluso, si comparamos con países de la región, Paraguay, Bolivia, Chile, Uruguay o Perú, estamos muy bien posicionados en formación de recursos humanos en ciberseguridad. En Paraguay, por ejemplo, con quienes mantengo un contacto estrecho, recién ahora comenzaron a tener alguna formación parecida a la nuestra en una universidad en donde comenzaron a brindar una especialización.

6. ¿Considera necesaria una formación multidisciplinaria en el tema?

   Sí, totalmente. Sería muy conveniente que la formación abarque a personas no técnicas, que puedan integrar equipos de ciberseguridad. Inclusive el personal técnico, además de contar con una formación más dura, también debe ser formado en cuestiones de ciberseguridad y ser parte de la concientización.

7. ¿Piensa que entender en Seguridad de la información podría ayudar a hacer más amigable y seguro el uso de las tecnologías a las personas en general?

Sí, claro.

8. ¿Qué percepción tiene respecto de ciberataques? ¿Se han incrementado en su organización? ¿La capacitación de las personas ayudó a mitigar los efectos de los incidentes que se detectaron?

   Con respecto a los ciberataques, se han incrementado en el último año, como en todos lados, sobre todo, como producto del trabajo remoto a partir de la pandemia, se amplió la superficie de ataque enormemente. El phishing se ha difundido mucho más en este último tiempo. En general, más allá de la jurisdicción, hay estafas cometidas a través de campañas de phishing que se han incrementado, así como los ataques a servidores de VPN o a software que se utiliza para acceso remoto. Respecto a la capacitación, ayuda a mitigar el riesgo, por lo tanto, también los incidentes.

Anexo O - Entrevista realizada al Sr. General de Brigada Aníbal Intini, Comandante Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas, el día 27 de septiembre de 2021.

1. Cantidad de Personal a cargo:

   Setenta (70)

2. En cuanto al personal a su cargo:

   2.1 ¿Qué tipo de nivel alcanzado de formación tienen? ¿Grado? ¿Posgrado? ¿Especializaciones? ¿Certificaciones?

   En el equipo hay oficiales, suboficiales y soldados. Son desde analistas hasta ingenieros. Algunos han cursado las carreras de maestría en Ciberdefensa y Ciberseguridad en Ciencias Económicas y otros la maestría en Ciberdefensa de la UNDEF, pero en general se suelen especializar en la temática ciber dentro del área, con cursos que se organizan internamente.

   2.2 ¿Estos estudios tiene que ver con tecnología/informática/ciberseguridad?

   No necesariamente, es personal de cuadros, es decir oficiales, suboficiales y soldados voluntarios, todos de distintas especialidades.

   2.3 ¿El personal de su área realiza periódicamente capacitaciones/actualizaciones en ciberseguridad? ¿De qué tipo o a través de qué medios?

   Sí, en general se organizan cursos propios. En estos momentos se está desarrollando el curso Conjunto de Homologación de Competencias en Ciberdefensa para capacitar al personal que hoy es parte del sistema de ciberdefensa y para nivelar los conocimientos de los agentes. Además, se está propiciando la creación del Instituto de Ciberdefensa de las Fuerzas Armadas, una entidad educativa a nivel nacional, en

donde se ofrecerá un Bachillerato Universitario en Ciberdefensa, una Tecnicatura Universitaria en Ciberdefensa, una Licenciatura en Ciberdefensa, una Especialización en Ciberdefensa, que podrá articularse con las especializaciones y maestrías vigentes de la FIE y la CRU-IUA. A través del Instituto se busca centralizar el esfuerzo en la capacitación en ciberdefensa en las Fuerzas Armadas, concientizar en los niveles formativos, y especializar a los cuadros permanentes y al personal civil, lo que contribuirá eficazmente a la excelencia operativa de los integrantes de las organizaciones en ciberdefensa. En el ámbito internacional somos parte del Foro Iberoamericano de Ciberdefensa; participamos de la capacitación técnica y de gestión a través de la Junta Interamericana de Defensa y participamos de varios ejercicios de ciberdefensa.

2.4 ¿Considera suficiente la cantidad de personal especializado con que cuenta el área?

No. Esto mismo se observa a nivel global. Además, sucede que las personas jóvenes, como son los soldados, son difíciles de retener. Tienen un alto nivel de volatilidad. Una vez que se forman, se van. Esta problemática la tratamos de encarar a partir de la creación del Instituto de Ciberdefensa de las Fuerzas Armadas.

3. En la organización en donde ud. trabaja, se brindan cursos/jornadas de capacitación/concientización en Ciberseguridad Sí/No

Sí. Por un lado, están las capacitaciones que se brindan desde el Estado Mayor Conjunto de las FF.AA. y por otro, las Fuerzas Armadas también ofrecen cursos de capacitación al personal, como así también las escuelas de comunicaciones hacen todo tipo de eventos.

3.1 ¿A quiénes está destinado? ¿A personal jerárquico, técnicos, informático, personal en general, otros?

Están destinados a todo tipo de público, inclusive hay conferencias/cursos que son abiertas al público en general.

3.2 ¿Se incluye en las capacitaciones a personal de otras disciplinas no informáticas?

Sí, totalmente. De hecho, el personal militar pertenece a distintas ramas y todos tienen una variada formación.

4. ¿Cuál es su percepción sobre el resto del personal de la Empresa, Organismo o Fuerza respecto de los conocimientos que tienen en materia de ciberseguridad?

Hay una heterogeneidad enorme. No hubo homologación, hay gente con conocimientos muy diversos. Con las iniciativas que estamos llevando a cabo, vamos a intentar

incorporar soldados con secundario terminado, aunque no tengan conocimientos avanzados, para formarlos hasta por tres años.

5. ¿Cuál es su opinión sobre las ofertas de formación académica en materia de ciberseguridad en nuestro país?

   No cuentan con una variedad de ofertas de materias en ciberseguridad en carreras de grado. Los planes de estudio son antiguos. Esto obedece también a que hacer un cambio en un plan resulta un proceso difícil, burocrático, poco ágil, que no todos están dispuestos a llevar adelante.

6. ¿Considera necesaria una formación multidisciplinaria en el tema?

   Sí, se necesita un punto de vista variado, abogados, médicos, economistas, sobre todo, en los niveles altos de conducción estratégica-militar. Cuando hablamos de infraestructuras críticas, probablemente necesitemos de un especialista en electricidad, o energía nuclear, por ejemplo.

7. ¿Piensa que entender en Seguridad de la información podría ayudar a hacer más amigable y seguro el uso de las tecnologías a las personas en general?

   No amigable pero sí seguro. Como bien sabemos, el ser humano es el eslabón más débil, en eso ayuda trabajar sobre la concientización.

8. ¿Qué percepción tiene respecto de ciberataques? ¿Se han incrementado en su organización? ¿La capacitación de las personas ayudó a mitigar los efectos de los incidentes que se detectaron?

   Los ciberataques se han incrementado. La pandemia produjo un incremento del uso y de la penetración de la red y de los “aburridos”. Las amenazas sofisticadas no presentan cambios, en cambio el phishing, por ejemplo, sí. Además, crece la red, aumenta el porcentual de amenazas y posibles atacantes, más humanistas, más sofisticación, y la gente se vuelve más vulnerable. La capacitación ayuda un poco, pero no del todo. Luego de las capacitaciones hacemos testeos para ver qué aprendieron las personas, y no siempre los resultados salen bien.