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

MAESTRÍA EN CIBERDEFENSA Y CIBERSEGURIDAD

TRABAJO FINAL DE MAESTRÍA

Aportes para la ciberseguridad en los servicios web del Estado Nacional Argentino: Programas de *Bug Bounty*

AUTOR: ESP. RUBÉN DARÍO AYBAR

DIRECTOR: MG. DARÍO OSVALDO RIZZO

Septiembre 2023

Esta página ha sido dejada en blanco intencionalmente.

Resumen

El objetivo que se persigue conseguir al escribir esta tesis de fin de Maestría es realizar un aporte al Estado Nacional Argentino desde una metodología exploratoria descriptiva y con carácter documental en fase inicial, presentando bases teóricas respondiendo a las siguientes preguntas de investigación: ¿El Estado Nacional Argentino debería evaluar la creación de una Política Pública Nacional de programas de bug bounty? y también si ¿Debería contar con su propia plataforma de programas de bug bounty o debería utilizar una plataforma de terceros?

Para responder las preguntas planteadas se realizará:

- Primero: analizar antecedentes sobre la creación e implementación de programas de bug bounty en el mundo.
- Segundo: elaborar una propuesta a cada una de las preguntas planteadas como hipótesis en base de las estadísticas obtenidas en una encuesta realizada a Organismos de la Administración Pública Nacional (APN).

El lector podrá encontrar al leer los diferentes apartados de esta tesis y en cada uno de los capítulos los aspectos fundamentales que le permitirán adentrarse, en el conocimiento de que son las políticas públicas, la historia de los bugs, los orígenes de los programas de bug bounty, el porqué de su utilización juntamente con los beneficios que generan para las empresas privadas y para los ciudadanos que participan en los programas, prácticas que si son aplicadas en el ámbito de la administración gubernamental de un país pueden generar resiliencia ayudando a las áreas de ciberseguridad, que suelen contar con pocos agentes para atender las tareas pertinentes a la búsqueda de vulnerabilidades, así también a que los proyectos de desarrollo de sistemas culminan con implementarse en ambientes productivos cada día con mayor celeridad relegando la seguridad para después, lo que lleva a sistemas productivos vulnerables a ciberdelincuentes y afectando los datos de los ciudadanos del país.

Palabras Claves
Ciberseguridad – Bug Bounty – Seguridad de la información – Vulnerabilidades – Gobierno – Hackers – Crowdsourcing

Abstract

The objective pursued when writing this Master's thesis is to make a contribution to the Argentine National State from a descriptive and documentary exploratory methodology in the initial phase, presenting theoretical bases answering the following research questions: The National State Should Argentina evaluate the creation of a National Public Policy for bug bounty programs? and also if you should have your own platform of bug bounty programs or should you use a third party platform?

To answer the questions posed, the following will be carried out:

• First: analyze background on the creation and implementation of bug bounty programs in the world.

• Second: prepare a proposal for each of the questions posed as hypotheses based on the statistics obtained in a survey of National Public Administration Organizations (APN).

The reader will be able to find when reading the different sections of this thesis and in each of the chapters the fundamental aspects that will allow him to delve into the knowledge of what public policies are, the history of bugs, the origins of bug programs bounty, the reason for their use together with the benefits they generate for private companies and for citizens who participate in the programs, practices if they are applied in the field of government administration of a country can generate resilience by helping cybersecurity areas , which usually have few agents to attend to the tasks pertinent to the search for vulnerabilities as well as the systems development projects culminating in being implemented in productive environments every day with greater speed, relegating security to later, which leads to productive systems vulnerable to cybercriminals and affecting the data of the country's citizens.

Keywords

Cybersecurity – Bug Bounty – Information Security – Vulnerabilities – Government – Hackers – Crowdsourcing

Agradecimientos

A mí familia (Monserrat, Luca y Alicia) quienes siempre me siguen apoyando cuando me embarco en otra locura nueva, en este caso en particular estuvieron acompañándome en todo, al cursar la maestría y redactando esta obra, ellos son los que me aguantaron en cada una de las tres tesis que escribí hasta el momento, brindándome su tiempo para que pueda lograr ese objetivo. ¡¡¡Los Amo!!!

A mis padres Alicia y Eduardo, mi mamá Alicia la imagino siempre feliz que su hijo una vez más pueda conseguir otra meta que se trazó en su vida. Ella siempre está guiándome desde el cielo, ella está siempre en mi mente y mi corazón, y sé que está poniéndose orgullosa por los logros que fui consiguiendo en mi vida.

Mi papá siempre está brindándome su apoyo en cada proyecto y poniéndose orgulloso con cada hito que voy consiguiente en este camino llamado vida.

A mi tutor Mg. Darío Osvaldo Rizzo a quién no dude en elegir cuando tuve que seleccionar quién iba a ocupar este rol tan importante y con tanta responsabilidad, su experiencia en el campo de la ciberseguridad demuestra la excelencia profesional. También es un placer extra el tener de tutor a un Amigo, Colega y Compañero de Especialización dejando una amistad forjada a fuego para toda la vida.

Una gran admiración y cariño a la dedicación del director Dr. Ing. Roberto Uzal y el subdirector Esp. Ing. Carlos Amaya de la Maestría en ciberdefensa y ciberseguridad de la gran casa de estudio que es la Universidad de Buenos Aires, al igual que a todo el cuerpo docente de la Maestría quienes nos brindaron su conocimiento generando pensamiento crítico en los Maestrandos.

A mis compañeros de Maestría Cohorte 2019 quienes me aportaron la sinergia para generar entre todos nuevos conocimientos para toda nuestra vida. ¡Gracias Totales a todos ellos!!!!!!

Índice

Índice de Figuras

Índice de Tablas

Índice de Abreviaturas

APN	Administración Pública Nacional
BBP	Bug Bounty Program
BBVA	Banco Bilbao Vizcaya Argentaria
BSoD	Blue Screen of Death
CIA	Central Intelligence Agency
CIO	Chief Information Officer
COMDEX	Computer Dealers' Exhibition
CPT	Captain
CTO	Chief Technology Officer
CVSS	Common Vulnerability Scoring System Calculator
DNM	Dirección Nacional de Migraciones
DoD	Departamento de Defensa de los Estados Unidos
EE. UU.	Estados Unidos de Norte América
FundéuRAE	Fundación del Español Urgente
GDE	Gestión Documental Electrónica
Interpol	Organización Internacional de Policía Criminal
IOSFA	Instituto de Obra Social de las Fuerzas Armadas y de Seguridad
IoT	Internet of Things
NASA	National Aeronautics and Space Administration
NICT	New Information and Communication Technologies
NIST	National Institute of Standards and Technology
NMAH	National Museum of American History
PFA	Policía Federal Argentina
PSA	Policía de Seguridad Aeroportuaria
QA	Quality Assurance
SCADA	Supervisory Control And Data Acquisition
SDLC	Systems Development Life Cycle
URSS	Unión de Repúblicas Socialistas Soviéticas
VCP	Vulnerability Contributor Program
VDP	Vulnerability Disclosure Policy
VRP	Vulnerability Reward Program
Y2K	Year 2000
ZDI	Zero Day Initiative

"Cómo el mundo está cada vez más interconectado, todos comparten la responsabilidad de asegurar el ciberespacio"
Newton Lee

Introducción

En esta tesis de fin de Maestría se presenta un aporte utilizando una metodología exploratoria descriptiva y con carácter documental en fase inicial sobre una debilidad detectada en los Organismos del Estado Nacional Argentino, esta debilidad se encuentra en los ciberataques a sus sitios web, alterando alguno de los principios fundamentales de la seguridad de la información: Confidencialidad[1], Integridad[2] o Disponibilidad[3], el aporte que se pretende realizar es una búsqueda bibliográfica que muestre antecedentes de programas de bug bounty impulsados desde diferentes Estados/Naciones, los cuales invitan a participar a los ciudadanos a estos programas, reportando vulnerabilidades detectadas en servicios web oficiales de diferentes Organismos puestos a disposición del programa como su alcance (del inglés scope), todo ello a cambio de una recompensa. Este aporte se plantea para que a futuro pueda ser tomado a consideración e implementación de forma práctica en el Estado Nacional Argentino.

Considerando los problemas que día tras día atraviesan cada uno de los Organismos que componen el ecosistema de la Administración Pública de la Argentina (Jefatura de Gabinete de Ministros, 2021), en lo que respecta a ciberataques a sus infraestructuras informáticas en general y sus plataformas de gestión web expuestas a internet en particular; los casos de ciberataques a estos sitios cada año van en un aumento exponencial, permitiendo a los ciberdelincuentes acceder a información sensible de los ciudadanos, almacenada en los servidores de cada uno de los Organismos afectados.

Por lo expuesto en los párrafos anteriores se considera de total relevancia el tema seleccionado ya que debe ser tratado de forma urgente, acercando una solución que ayude a los equipos de ciberseguridad de los Organismos del Estado Nacional Argentino a detectar los

[1] Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
[2] Integridad: Cualidad o condición de la información que garantiza que no ha sido modificada por personas no autorizadas.
[3] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

fallos de forma proactiva y no tras una brecha de seguridad como viene ocurriendo en los últimos años.

- Infiltración en la cuenta oficial de la ministra Patricia Bullrich (perfil.com, 2017) y de la Policía de Seguridad Aeroportuaria (PSA) (LA NACIÓN, 2019), hechos ocurridos en enero de 2017 y 2019 respectivamente.
- Ransomware y filtración de información en la Dirección Nacional de Migraciones (DNM) (Dirección Nacional de Migraciones, 2020), hecho ocurrido en agosto de 2020.
- Filtración de datos Obra Social de las Fuerzas Armadas (IOSFA) (IOSFA, 2021) hecho ocurrido en septiembre de 2021.

Objetivos

El objetivo general de la tesis es:

- Desarrollar un aporte desde una metodología de investigación exploratoria descriptiva y con carácter documental en fase inicial, analizando si fuera pertinente que el estado evalúe crear una Política Pública Nacional de bug bounty y si el Estado debiera evaluar el desarrollar su propia plataforma o utilizar una plataforma de terceros (como por ejemplo HackerOne).

Los objetivos específicos de la tesis son:

- Describir qué son, cómo se gestan, quienes participan y cómo se arma una agenda de políticas públicas.
- Describir qué son y cómo nacieron los bugs.
- Describir qué son y cómo nacieron los programas de bug bounty.
- Analizar los programas de bug bounty gubernamentales en diferentes países del mundo.
- Argumentar si el Estado Nacional Argentino debería evaluar la creación de su propia Política Pública Nacional de bug bounty.

- Argumentar cuál es la mejor solución para implementar programas de bug bounty en el Estado Nacional Argentino.

Metodología

Para la presente obra se utilizará una metodología exploratoria descriptiva y con carácter documental en fase inicial.

Según Hernández Sampieri, R., Fernández Collado, C. & Baptista Lucio, P. (2006) en su obra "Metodología de la Investigación" explican que

> La investigación exploratoria es un tipo de investigación que se realiza cuando el tema de estudio es poco conocido o ha sido poco explorado. Su objetivo principal es obtener una comprensión inicial y general del tema, lo que puede proporcionar una base para investigaciones posteriores más detalladas. (pp 100-101)

En cuanto a la metodología descriptiva también explican Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006) en el libro "Metodología de la Investigación" que

> Con frecuencia, la meta del investigador consiste en describir fenómenos, situaciones, contextos y eventos; esto es, detallar cómo son y cómo se manifiestan. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis (Danhke, 1989). Es decir, miden, evalúan o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar. En un estudio descriptivo se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para así (valga la redundancia) describir lo que se investiga. (p 102)

Se prevé un estudio de textos para conocer el estado del arte del bug bounty aplicado a los Organismos públicos de los países del mundo, también será utilizado un enfoque cuantitativo de tipo encuestas transversales.

Para el enfoque cuantitativo se dispondrá de encuestas con preguntas cerradas, las preguntas serán de opción múltiple en la que los encuestados deberán seleccionar la respuesta, dentro de las brindadas en la propia encuesta, que consideren más adecuada para su respuesta. La población objetivo serán las Áreas de Tecnología, Seguridad de la Información o de

Ciberseguridad de los Organismos de la Administración Pública Nacional (APN), con ello se busca conseguir datos que luego de procesados se transformarán en estadísticas a ser presentadas en la obra.

El método de recolección de los datos será a través de encuestas con formularios de Google, los formularios quedarán abiertos durante un periodo de veinte (20) días, en los cuales los encuestados podrán responder y enviar sus respuestas.

El posterior procesamiento de los datos obtenidos será tratado a través de las herramientas de análisis de datos y gráficos de los formularios de Google que permitirá realizar las siguientes tareas:

1. Revisar el avance de la encuesta en curso.
2. Ver el reporte por reporte e individual.
3. Extraer los resultados a una hoja de cálculo.
4. Procesar los resultados en la hoja de cálculo.
5. Realizar el análisis e interpretación.

Hipótesis

La hipótesis que será planteada en el trabajo final de Maestría es:

"**El desarrollo de una Política Pública para implementar un programa tipo bug bounty, sustentada desde el empleo de una plataforma propia o una plataforma de terceros que resulta en una ventaja estratégica que otorga mayor o menor resiliencia al Estado Nacional Argentino.**"

De la hipótesis se desprenden dos partes bien delimitadas, la primera de ellas surge en base a los antecedentes de programas que fueron creados en diferentes lugares del mundo obteniendo excelentes resultados, se puede utilizar como ejemplo el informe final del programa "hack the pentagon" (www.defense.gov, 2016) desarrollado durante el año 2016 por el gobierno de los Estados Unidos y que se puede encontrar en la página oficial del sitio de HackerOne.

La segunda parte de la hipótesis surge del desarrollo de una solución de software web como plataforma propia del Estado Argentino para que sea incorporada en la cartera de las infraestructuras críticas del país, como es el caso de la plataforma de Gestión Documental Electrónica (GDE) (PÚBLICA, 2020) o si debe realizar la utilización de una plataforma de terceros para la creación y seguimiento de los programas de bug bounty que vayan a ir surgiendo en base a las necesidades de los Organismos del Estado Argentino, al ser una solución innovadora, no pudiendo encontrar programas de bug bounty de otros países que se realicen en sus propias plataformas (desarrolladas por el propio Estado y/o Nación) y ello plantea un desafío más grande, pero así también si se implementara podría ser un caso de éxito para el Estado Argentino y de Latinoamérica.

De la hipótesis planteada en el trabajo, se podrá inferir la respuesta más adecuada para el aporte que se busca realizar, generando con ello un capítulo completo en la tesis para el análisis, y cuyos resultados constituyen el fundamento esencial de las conclusiones de la tesis y de las recomendaciones para futuros trabajo de investigación relacionados.

Motivación

Los ciberataques a nivel mundial siguen creciendo, todos los días se escucha o lee por los medios, redes sociales y hasta de colegas que se ha vulnerado algún sistema informático.

Según la portada oficial de la Organización Internacional de Policía Criminal (Interpol) de su sección de ciberdelincuencia dice,

> La ciberdelincuencia crece a un ritmo muy acelerado, con nuevas tendencias emergiendo continuamente. Los ciberdelincuentes se están volviendo más ágiles, explotan las nuevas tecnologías a una velocidad de vértigo, adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca vista hasta ahora. Las redes delictivas operan a escala planetaria, coordinando ataques complejos contra sus objetivos en cuestión de minutos. (Interpol, n.d.)

A consecuencia de ello, aumentaron las prácticas de bug bounty en las empresas y organismos del estado como se puede leer en el informe 2021 generado por HackerOne y que se encuentra disponible para su descarga en su sitio web oficial

> Desde el lanzamiento del Informe Hacker 2019 hace dos años, la comunidad HackerOne ha duplicado su tamaño a más de un millón de hackers registrados. Si bien gran parte de la comunidad aún está explorando y aprendiendo, ha habido un aumento del 63% en el número de piratas informáticos que envían informes en 2020. Eso es un aumento del 143% desde 2018, lo que demuestra que los piratas informáticos están aumentando sus habilidades y experiencia como organizaciones e industrias en todo el mundo invierte en soluciones impulsadas por hackers. (HackerOne Team, 2021)

En base a lo desarrollado en los párrafos anteriores es fácil darse cuenta que el Estado Argentino no está exento de ciberataques a sus sitios web gubernamentales, es más se ve todos los días tras leer las noticias de cómo son vulnerados sus sitios y dejando expuestos los datos de todos los ciudadanos, es por ello que la motivación de esta obra y siendo para una tesis de final de magíster de una carrera de ciberseguridad y ciberdefensa, desde esta obra se realice un aporte significativo para que pueda ser tenido en cuenta y aplicado mejorando la ciberseguridad del país y resguardando con ello la privacidad de los datos de sus ciudadanos.

“La explicación más simple y suficiente es la más probable, mas no necesariamente la verdadera”

La navaja de Ockham

Estado del Arte

El Bug Bounty, también conocido como programa de recompensas por errores o vulnerabilidades, se ha convertido en una parte esencial de la ciberseguridad moderna. En este "Estado del Arte", se explorarán los diferentes autores que realizaron investigaciones sobre las metodologías y normas que deberían ser utilizadas, escribieron obras concernientes en la detección y mitigación de vulnerabilidades en sistemas de software y plataformas online.

En su libro "The Art of Software Security Assessment" Mark Dowd et al. (2019) mencionan que los bugs en software representan una preocupación continua en la industria de la ciberseguridad. Los investigadores y hackers éticos desempeñan un papel fundamental en la identificación de estos bugs mediante pruebas de penetración y análisis de código.

Por su parte Katie Moussouris (2017), experta en seguridad y fundadora de Luta Security, destaca que los programas de Bug Bounty han demostrado ser una estrategia efectiva para descubrir y abordar vulnerabilidades en sistemas. Según su experiencia, estos programas permiten a las organizaciones aprovechar el conocimiento colectivo de una comunidad global de cazadores de bugs. También al ayudar a las Fuerzas Armadas de los Estados Unidos de Norteamérica no solo ofreciendo sus conocimientos, sino que Katie también es coautora y co-editora de la Norma ISO 29147 (divulgación de vulnerabilidades) y de la Norma ISO 30111 (procesos de manejo de vulnerabilidades). En colaboración con el Departamento de Defensa, Katie dirigió el lanzamiento del primer programa de recompensas por errores del gobierno de EE. UU., "Hack the Pentagon". También trabajó con el Departamento de Estado para ayudar a renegociar el Acuerdo de Wassenaar, cambiando específicamente el lenguaje de control de exportaciones para incluir exenciones técnicas para la divulgación de vulnerabilidades y la respuesta a incidentes.

Casey Ellis, CEO de Bugcrowd, en un artículo de 2018 titulado "La evolución de los programas de Bug Bounty", señala que los programas de Bug Bounty han evolucionado desde su inicio, pasando de ser percibidos como una solución de último recurso a convertirse en una práctica de seguridad comúnmente aceptada. Ellis destaca que las empresas líderes están adoptando programas de Bug Bounty como parte integral de su estrategia de seguridad.

Robert Vamosi (2018) en su libro "When Gadgets Betray Us: The Dark Side of Our Infatuation with New Technologies" argumenta que los bugs son inevitables en los sistemas de software y que el enfoque tradicional de "corregir después del hecho" no es suficiente. Vamosi sostiene que los programas de Bug Bounty son una forma proactiva de abordar las vulnerabilidades, al involucrar a la comunidad de hackers éticos para encontrar y corregir bugs antes de que sean explotados por actores maliciosos.

Alex Rice, CTO de HackerOne, en un artículo de 2019 titulado "The Bug Bounty Field Manual", señala que el éxito de los programas de Bug Bounty radica en la colaboración y el trabajo en equipo entre las organizaciones y los cazadores de recompensas. Rice enfatiza la importancia de establecer una comunicación efectiva, proporcionar retroalimentación constructiva y recompensar de manera justa a los cazadores de bugs para fomentar su participación continua.

Rui Florêncio (Florêncio, 2020) en un artículo titulado “Permissão para Atacar: Cómo Mejorar la Ciberseguridad de Portugal a través de un Programa de Bug Bounty Gubernamental” explora la posibilidad de implementar un programa de recompensas por errores (Bug Bounty) a nivel gubernamental en Portugal como una estrategia para mejorar la ciberseguridad del país. Portugal, al igual que otros países, enfrenta desafíos crecientes en términos de ciberseguridad debido a la evolución constante de las amenazas cibernéticas. El gobierno y las organizaciones se enfrentan a la difícil tarea de proteger la infraestructura crítica, los datos sensibles y los sistemas en línea contra ciberataques y vulnerabilidades.
La propuesta que propone Rui Florêncio se centra en la implementación de un programa de Bug Bounty por parte del gobierno portugués. Un programa de este tipo permitiría a los cazadores de recompensas éticos y expertos en seguridad identificar y reportar vulnerabilidades

en sistemas gubernamentales y plataformas en línea. A cambio, se les recompensará económicamente y se establecería un proceso de divulgación coordinada para resolver las vulnerabilidades de manera eficiente.

El autor de la tesis en base a los aportes realizados por los diferentes autores y siguiendo la misma línea de pensamiento que todos ellos plantean que los bugs bounty tanto a nivel de empresas u organismos gubernamentales va en aumento y es favorable en base a los resultados obtenidos, es por ello que la investigación en continuar investigando y aportando una solución para ser tomada en cuenta para el Estado Nacional Argentino, como mínimo que sea el punto de partida para pensar desde las políticas públicas el ponerlo en la agenda y que pueda ser llevado a debate y en caso de ser seleccionada como la mejor solución como política pública realizar una futura implementación, también cabe destacar que el caso más parecido es el que está desarrollado en su artículo por Rui Florêncio para que sea tomado en consideración por Portugal.

“Igual que el pensamiento vertical, el pensamiento lateral es un modo de usar la mente. Constituye un hábito y una actitud mental.”

Edward de Bono

Capítulo I: Marco Teórico

Introducción

En el presente capítulo, marco teórico de la tesis, se aborda el desarrollo de tres conceptos fundamentales que debe conocer el lector: políticas públicas, bugs y bug bounty.

En la actualidad, la tecnología juega un papel fundamental en la vida cotidiana de las personas, y ello ha llevado a un aumento significativo en la dependencia de la tecnología en diversas áreas, como la comunicación, la información y la gestión de servicios. Sin embargo, la tecnología no está exenta de fallos y vulnerabilidades, lo que puede afectar la seguridad y la privacidad de los usuarios. En este contexto, estas áreas de estudio tienen una gran relevancia en diversos campos, desde la administración pública hasta la seguridad informática.

Las políticas públicas son instrumentos utilizados por los gobiernos para abordar problemas sociales y tomar decisiones encaminadas a mejorar las condiciones de vida de la población. Estas políticas pueden tener diferentes objetivos, como promover el desarrollo económico, garantizar derechos básicos o prevenir conflictos sociales. Para su diseño e implementación se requiere un análisis riguroso que involucra aspectos políticos, económicos y sociales.

Por otro lado, los bugs (o errores) son fallos o defectos que se presentan en programas informáticos u otros sistemas tecnológicos. Estas fallas pueden afectar el funcionamiento correcto del sistema e incluso comprometer la seguridad de datos sensibles. La detección y corrección temprana de los bugs es fundamental para evitar posibles consecuencias negativas.

El concepto más novedoso dentro del ámbito tecnológico es el bug bounty (recompensa por errores). Esta práctica consiste en recompensar económicamente a aquellas personas que encuentren y reporten vulnerabilidades o bugs en sistemas digitales específicos puestos a disposición por una organización u organismo gubernamental. De esta manera, las

organizaciones u organismos gubernamentales fomentan una colaboración activa con expertos externos al ofrecerles incentivos económicos a cambio de sus conocimientos técnicos.

A lo largo de este capítulo explicaremos cada uno de estos conceptos en profundidad, analizando su importancia dentro del contexto actual. Se examinarán diversas teorías y modelos relacionados con las políticas públicas, así como también se abordarán los diferentes tipos de bugs que pueden ser detectados tanto en diferentes softwares como en componentes de hardware y sus implicaciones en la seguridad informática. Además, se explorará cómo el bug bounty ha revolucionado la forma en que se aborda la detección de vulnerabilidades en sistemas digitales.

1.1 Concepto de políticas públicas

Para el correcto planteo de esta tesis y brindando un contexto en este marco teórico para que el lector pueda comprender las conclusiones a las que quiere arribar el maestrando, se debe definir qué son las políticas públicas.

En una definición no exhaustiva y general se podría decir que las políticas públicas son acciones que realizan los Gobiernos, para alcanzar objetivos que satisfacen las necesidades a los problemas sociales, las autoridades a cargo de la administración del Estado deciden si disponen y emplean los recursos para intentar solucionar un problema o para responder a una demanda de la sociedad diseñando y administrando las políticas públicas.

Para comprender más a fondo el concepto de Políticas Públicas, lo primero que se debe realizar es la desagregación de las palabras “Política” y “Pública” para comprender la etimología de las palabras.

La palabra Política según el Doctor en Filosofía, con especialidad en Filosofía Política Luis F. Aguilar Villanueva (1992) la define como “un comportamiento propositivo, intencional, planeado, no simplemente reactivo, casual. Se pone en movimiento con el objetivo de alcanzar ciertos objetivos a través de ciertos medios: una acción con sentido”.

La misma es el arte de gobernar la organización y administración pública de un Estado en sus asuntos e intereses a nivel general, se pone en movimiento con la decisión de obtener metas involucrando a todo un conjunto complejo de decisiones y operadores.

Dentro de la misma se producen enfrentamientos y compromisos, de competiciones y coaliciones de conflictos y transacciones convenientes.

Los tres componentes que tiene la política son: los principios que orientan, los elementos de ejecución y las acciones que se deben llevar a cabo para conseguirlo.

La palabra Público/a se podría definir como espacio colectivo donde se discuten los aspectos que influyen en la vida en sociedad. Este concepto puede entenderse en oposición a la idea de privado. Es decir, a políticas desarrolladas por el sector privado o agentes no estatales para el mundo privado (por ejemplo. Las diferentes políticas de una empresa).

No existe una definición unívoca de políticas públicas pero la mayoría de los autores coinciden en definirlas como acciones o inacciones del Estado para solucionar ciertos problemas públicos.

Para tomar definiciones de varios autores destacados en la materia se puede comenzar con la definición formal que realizan sobre ella los argentinos Oscar Oszlak quien es uno de los politólogos e intelectuales argentinos más destacados de América Latina y Guillermo Alberto O'Donnell quien fue un destacado politólogo definieron como que

> la política estatal no constituye ni un acto reflejo ni una respuesta aislada, sino más bien un conjunto de iniciativas y respuestas, manifiestas o implícitas, que observadas en un momento histórico y en un contexto determinados permiten inferir la posición, agregaríamos predominante, del Estado frente a una cuestión que atañe a sectores significativos de la sociedad. (Ozlak & O'Donnell, 1995)

En tanto el doctor en Ciencia Política y licenciado en Sociología Manuel Tamayo Sáez (1997) define “Las políticas públicas son el conjunto de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas que, en un momento determinado, los ciudadanos y el propio gobierno consideran prioritarios”

También según define el destacado analista de políticas públicas Eugenio Lahera Parada

> Las políticas públicas son un factor común de la política y de las decisiones del gobierno y de la oposición. Así, la política puede ser analizada como la búsqueda de establecer o de bloquear políticas públicas sobre determinados temas, o de influir en ellas. A su

vez, parte fundamental del quehacer del gobierno se refiere al diseño, gestión y evaluación de las políticas públicas. (Lahera, 2004)

1.2 Que se intenta conseguir a través de las políticas públicas

Tras lo desarrollado en el apartado previo y definido por diferentes autores sobre lo que son las políticas públicas es importante resaltar que faltaría definir ¿qué es lo que se intenta conseguir a través de las políticas públicas? o lo que es lo mismo ¿para qué sirven las políticas públicas?

Se puede obtener una palabra que los diferentes autores ponen siempre en el foco, la palabra "problema" y que las Políticas Públicas deben brindar una solución a ese problema.

Un problema se puede definir como la distancia entre la concepción ideal sobre un asunto y la forma en que este se presenta en la realidad puede dar origen a un problema. Sin embargo, no toda condición o circunstancia es un problema, sino que depende de cómo lo interpreten los involucrados a partir de sus valores y de sus percepciones.

Ya definido el concepto de política se continúa con la política pública que comparte la definición, pero apunta a unas medidas que toma el gobierno de acuerdo con la agenda pública, esta última es la que se elabora de acuerdo con los resultados de la movilización de demandas y presiones de la sociedad, es importante que estas presiones lleguen a ser un tema para poner en la mesa de negociación, llegar acuerdos y lograr que se evalúa el problema.

Entendemos que la misma se basa en las necesidad o problemas que surgen en la comunidad y no pueden ser satisfechas por ellos mismos, sino que es el gobierno quien las puede cumplir. Para ellos cumplen con algunos aspectos.

Normas jurídicas: se basa en todo tipo de norma y ley establecida de manera que sea legal frente a la sociedad.

Requiere de infraestructura humana, organizacional y material.

Los recursos materiales deben ser contemplados, principalmente los financieros.

1.3 Ciclo vida de las políticas públicas

El Ciclo de vida de las políticas públicas se lo puede definir en cinco etapas o siendo que se va retroalimentando de la salida de la etapa previa y generando una mejora continua a partir de su implementación y puesta en práctica empíricamente.

Las principales fases del ciclo de las políticas públicas (Figura 1) según Lucy Winchester (2011) son las siguientes:

1) Establecimiento de la Agenda Pública
2) Formulación de Políticas
3) Proceso de Decisión
4) Implementación
5) Evaluación

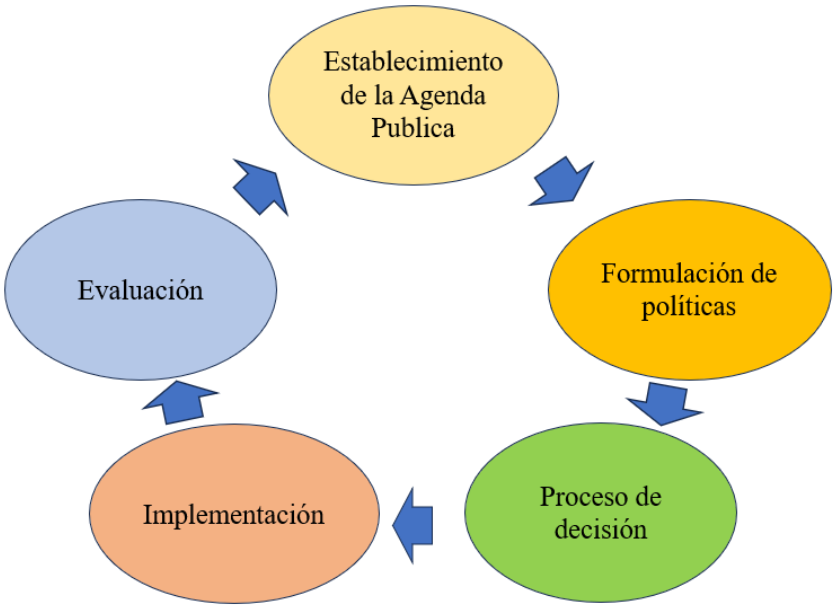


Figura 1 Representación Propia. Ciclo Vida de las Políticas Públicas.

Al conjunto de fases o etapas que se van ejecutando por un gobierno y en base a las acciones y decisiones que comienzan a influir en el problema que se está atacando se lo conoce como Políticas Públicas.

Cada una de estas fases o etapas se las puede definir según diferentes autores como se enuncian a continuación.

Establecimiento de la Agenda Publica: Según la define Aguilar Villanueva, Luis F (1992) como

> La forma adquirida por estos mecanismos, o rutas, por las que se elabora la agenda de gobierno es de capital importancia tanto en el plano político como en el administrativo. En el ámbito político, la manera en que es conformada la agenda en un sistema político es reflejo de la amplitud de la esfera pública. Deja ver a los actores que en efecto inciden en la vida pública, con qué valores, con qué intereses, así como por el lado de los excluidos ayuda a identificar qué valores e intereses se quedan fuera. En términos de gobierno y administración, el proceso de elaboración de la agenda es el momento en que se determina sobre qué se actuará o se dejará de intervenir, en dónde se pondrán los recursos y de qué manera; se trata, pues, de "la crucial decisión de decisiones"

Formulación de Políticas: Según la definición de Pedro Humberto Moreno Salazar (1993)

> la tarea principal de la formulación es la construcción de alternativas (escenarios) que consisten en enlistar todas las opciones imaginables para instigar a resolver el problema, y luego, hacer un estudio del conjunto de las mismas, para mediante criterios técnicos (eficiencia y eficacia) y políticos (legitimidad, equidad, justicia, mercado libre, control gubernamental) tratar de elegir la acción más adecuada. Varios autores del análisis de políticas sugieren que entre las opciones siempre se debe considerar la de "no hacer nada", dada la tasa de cambio del entorno que posiblemente llevaría a mitigar las causas y los efectos del problema, lo que haría inútil alguna de las opciones-soluciones.

Proceso de Decisión: Según define el doctor Manuel Tamayo Sáez (1997) sobre el proceso de decisión

> El análisis para la elaboración de las políticas es valioso, independientemente del modelo de elaboración que se considere, bien para orientar la decisión y el futuro, bien para comprender el funcionamiento de las políticas pasadas, descubrir los puntos de

mejora y la resistencia. La utilidad del análisis de las políticas depende del problema que se trate, de la política evaluada y de los condicionantes presentes.

Implementación: En la fase de implementación de la política pública inicia la puesta en marcha del plan de acción delineado en la etapa del diseño de política pública. Aquí se realiza el proceso de presupuestación, la creación legal del programa, el entrenamiento del equipo que lo llevará a cabo y la comunicación dentro de la agencia implementadora, así como con la ciudadanía. Esta fase es crucial, ya que el contenido y los posibles efectos de la política pública pueden ser modificados por la forma en que ésta se pone en práctica (Hill & Hupe, 2002).

Jeffrey L. Pressman y Aaron Wildavsky (1998) proponen que los programas públicos se evalúen para aprender y se implementen con el aprendizaje acumulado de experiencias pasadas. Estos autores dicen que la organización social está sujeta a contradicciones y a consecuencias imprevistas, y sólo aprendiendo de los errores se mejorará. El aprendizaje es la clave tanto de la implementación como de la evaluación.

Además, esta etapa se concentra en los factores que afectan la obtención de los resultados. Pedro Moreno (1993) y Josep M. Vallès (2002) plantean varios tipos de estos factores:

- Los relativos al tratamiento del problema (disponibilidad de una teoría y tecnología válidas, la diversidad del comportamiento del grupo afectado y/o a beneficiar, etcétera).
- Lo relativo a la habilidad de la estructura organizacional formal para operar formalmente la ejecución (objetivos consistentes y claros, incorporación de una teoría causal adecuada, reclutamiento de los funcionarios ejecutores, etcétera).
- El efecto neto de distintas variables políticas en el balance de apoyo y sostén de los objetivos establecidos (apoyo público, atención de los medios de difusión al problema, etcétera).

- El no prestar atención en el diseño de los diferentes operadores que intervendran en la implementación y el tipo de relaciones que mantendrían entre sí.
- La falta de recursos, dificultades de coordinación y hasta variables ambientales: en especial el ciclo político −estable o inestable−, el ciclo económico −de expansión o recesión−, el clima de opinión, la carga transformadora que incluye la misma política y las resistencias que puede provocar.

Evaluación: La evaluación única de resultados que se realiza al finalizar el proceso de ejecución, siempre se encarará de distinta forma que aquella que se da a lo largo de todo el proceso, desde su formulación y su implementación. En ambos casos, la metodología será la misma, pero se contará con distintos insumos y habrá que seguir distintos caminos según el caso. (Nirenberg, Brawerman, & Ruiz, 2003)

1.4 Concepto de bugs

Con la masividad de las nuevas tecnologías de la información y las comunicaciones (NTIC), el avance del Internet de las Cosas (IoT, Internet of Things del inglés) generando la interconexión de dispositivos a nivel mundial, los datos fluyen por el ciberespacio convirtiéndose en información luego de su procesamiento, ello hizo que se incremente la utilización de sistemas en las organizaciones, los organismos del estado y en los ciudadanos de cada país.

Todo ello lleva a que la cantidad de equipos físicos y software utilizado también tenga un incremento exponencial cada nuevo año como lo expresa la ley de Moore, y se afirma en el sitio oficial de Intel Latinoamérica

> En 1965, Gordon Moore realizó una predicción que marcaría el ritmo de la revolución digital moderna. Moore hizo una extrapolación de la cuidadosa observación de una tendencia emergente según la cual la computación aumentaría de manera radical en términos de potencia y disminuiría en términos de costo relativo, a un ritmo exponencial. Este concepto, denominado "Ley de Moore", se convirtió en la regla de

oro de la industria de la electrónica y en un trampolín para la innovación. Como cofundador, Gordon sentó las bases para que Intel creara los transistores más rápidos, pequeños y accesibles de la historia que impulsan las herramientas y los juguetes modernos. Incluso más de 50 años después, se siguen percibiendo sus beneficios y su impacto duradero de muchas maneras. (Intel, n.d.)

Y también dice

Como un metrónomo del mundo moderno, durante más de 50 años, la predicción de Gordon ha marcado la pauta de la innovación y el desarrollo. Esta visión de futuro sentó bases fértiles de las que surgiría toda la tecnología moderna, como el auge de la digitalización y los dispositivos electrónicos personales.

En un paso más adelante, la Ley de Moore y las innovaciones relacionadas avanzan hacia la integración transparente de la computación en nuestra vida cotidiana. Esta visión de un futuro habilitado e interconectado sin límites supone claros desafíos y beneficios por igual. La privacidad y las crecientes amenazas de seguridad son problemas persistentes que van en aumento. Sin embargo, los beneficios de la tecnología de la computación cada vez más inteligente y omnipresente, que aprende a anticiparse a nuestras necesidades, pueden ayudarnos a mantenernos más sanos, seguros y productivos a largo plazo. (Intel, n.d.)

Estos equipos físicos como servidores, computadoras, dispositivos inteligentes, etc. necesitan del componente de software, como puede ser el sistema operativo, para que puedan interactuar los usuarios con los programas.

Todo ello lleva a pensar que el software es desarrollado por programadores, hasta el hardware es creado por ingenieros que inventan y desarrollan placas, chips, microprocesadores y todos los componentes físicos de los dispositivos digitales, ello conlleva que estos

dispositivos tanto en su hardware o software puedan llegar a contener errores generados por los desarrolladores o ingenieros de forma no intencionada.

Bug deriva del término inglés insecto, en el campo de la informática se refiere a un fallo en un programa (un programa es una pieza de ingeniería de software especialmente diseñada para una función específica) una situación inesperada que no estaba prevista que ocurriera al momento de ser desarrollada por el programador, esa sería una definición no exhaustiva, ahora si se quiere una definición formal se puede tomar la que brinda el diccionario merriam-webster en su sitio oficial.

"2: an unexpected defect, fault, flaw, or imperfection

the software was full of bugs" (Webster, n.d.)

Pero esa es su definición formal en inglés, si se desea una definición formal en español se puede tomar la que brinda La Fundación del Español Urgente (FundéuRAE) "Fallo, imperfección, anomalía, defecto o error (inesperados) son alternativas en español para sustituir el anglicismo bug, común en textos sobre informática, redes sociales y tecnología digital" (Scalzo, 2013).

Como explica Max Kanat-Alexander (2015), autor del libro «Code Simplicity: The Science of Software Development» e ingeniero en Google, en la nota ¿Qué es un bug? del sitio web abc.es

> Un «bug», se puede referir a dos situaciones. La primera, el programa (llámese Candy Crush, Soundcloud o Facebook) no se comporta según las intenciones del programador, de su creador. La segunda, las intenciones del informático no satisfacen las expectativas razonables del usuario.

y con eso refiere a que no solamente los bugs traen aparejados errores o fallos en el propio código del programa escrito por él desarrollador, sino que se le puede llamar bug a que el software no cumpla con las necesidades que se había imaginado el usuario final que iba a recibir del desarrollador, por lo tanto, en ambos casos el desarrollador va a necesitar remediar esa situación a través de una actualización en el código.

Max Kanat-Alexander (2015) también explica sobre los bugs en los componentes de hardware, o sea la parte física de los dispositivos

> Los «bugs» no se presentan solo en software, también puede haber errores en hardware. Kanat-Alexander señala que es muy raro que un programador tenga intención de hacer explotar un ordenador, por lo que si el informático escribe un software y el ordenador colapsa, lo más probable es que se haya tratado de un error físico en el PC.
>
> Este es un ejemplo exagerado, ya que los bugs de hardware también pueden ocasionar consecuencias menos dramáticas.

Y Max Kanat-Alexander (2015) también complementa diciendo

> Algunos bugs pueden que no causen efectos severos en la funcionalidad del programa y puede pasar mucho tiempo sin ser detectado. Hay otra categoría de bugs que afecta a la seguridad. Este tipo de errores en el código puede permitir que un usuario con malas intenciones pueda acceder a los controles de un programa y obtener privilegios sin autorización.

Esto demuestra que los bugs son fallos o defectos tanto de software como de hardware y que según su nivel de criticidad pueden ser inofensivos o llevar a daños severos, esto es muy importante destacar ya que cuando se está hablando de bugs en infraestructuras críticas, las que en la Argentina fueron definidas por la Jefatura de Gabinete de ministros bajo la resolución 1523/2019 y sus Anexos (sin definir en profundidad cuáles son los organismos núcleos que la constituyen, sino solo la cartera macro) como

> Las Infraestructuras Críticas son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente. (JEFATURA DE GABINETE DE MINISTROS, www.argentina.gob.ar, 2019).

En el subapartado titulado “Los bugs más emblemáticos de la historia” de este Capítulo II Marco Teórico, se describen los bugs de seguridad detectados durante el pasado que, al ser descubiertos, en la mayoría de las ocasiones, fueron utilizados por ciberdelincuentes para la

realización de ciberataques que afectaron drásticamente la economía y reputación de organizaciones y organismos gubernamentales de diferentes países alrededor del mundo.

También es importante destacar el concepto de poder detectar los bugs lo más pronto posible en el ciclo de vida del desarrollo del software (SDLC – Systems Development Life Cycle del inglés), o como se lo conoce con el concepto de desplazarse a la izquierda (Shift the left del inglés); acorde a lo enunciado en el trabajo de tesis, el Especialista en Seguridad Informática Rubén Darío Aybar (2020) destaca que

> Uno de los principales problemas que se producen al comenzar un nuevo proyecto de desarrollo es la inclusión de errores en el mismo, según la metodología y la etapa en la que se encuentre el proyecto y sea detectado el error, generará un costo de reparación exponencialmente mayor.
>
> Estos errores pueden ser de funcionalidad o de seguridad, según el tipo de error puede ser descubierto por el personal de QA en el caso de ser funcionales o por el personal de seguridad en caso de ser una vulnerabilidad, aunque también pueden ser detectados por personas ajenas al proyecto, como ser ciber delincuentes y aprovecharse de ellos para su propio beneficio. (p. 7)

Barry Boehm es un ingeniero informático considerado una eminencia en su campo por los grandes aportes realizados en su área de incumbencia, quien en el año 1987 afirmó en una publicación suya titulada Industrial Metrics Top 10 List que “Encontrar y solucionar un problema de software después de la entrega suele ser 100 veces más caro que encontrarlo y solucionarlo durante la fase de requisitos y diseño” (Boehm, 1987, pp. 85-87).

Pero en otra publicación escrita por Barry Boehm y Víctor R. Basili en una revista del año 2001 titulada Software Defect Reduction Top 10 List expresan que

> En esta lista actualizada, hemos añadido la palabra "a menudo" para reflejar otras ideas sobre esta observación. Una de ellas muestra que el factor de escalado de costes para sistemas de software pequeños y no críticos es más bien de 5:1 que de 100:1. Esta relación revela que podemos desarrollar estos sistemas de manera más eficiente en un

modo menos formal y de prototipo continuo que sigue haciendo hincapié en hacer las cosas bien desde el principio y no desde el final. (Boehm & Basili, 2001, pp. 135-137)

y que sigue vigente hoy en día.

1.5 Concepto de bugs bounty

Si tomamos a la plataforma número uno, al momento de escribir la obra, en programas de bug bounty como una fuente confiable y habilitada para definir el término de mención se puede citar el post del blog de HackerOne: “What Is a Bug Bounty? Should You Offer One? And How To Do It” el cual dice

> Un bug bounty es una recompensa que ofrecen las organizaciones a los hackers éticos por descubrir vulnerabilidades de seguridad. Un programa de bug bounty puede ser público o privado. La organización establece el ámbito de aplicación y define el tipo de errores que se incluyen. (Vulnerability Management, 2021)

También en la investigación llamada The Hackers’ Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs, define y expone las prácticas de seguridad ofensiva dentro de las organizaciones y cómo ellas están cambiando hacia el bug bounty

> Tradicionalmente, las organizaciones confiaban en el trabajo de los expertos en seguridad internos (por ejemplo, las pruebas de seguridad realizadas por los red teams) y los expertos externos (por ejemplo, el pentesting) para descubrir las vulnerabilidades de sus productos y servicios. Por el contrario, los bug-bounty programs -también conocidos como vulnerability-reward programs o seguridad "crowd-sourced"- ofrecen incentivos a los expertos en seguridad externos para que evalúen la seguridad de los productos y servicios de una organización en su ámbito, y para que informen de las vulnerabilidades a cambio de recompensas (económicas o de otro tipo, como el reconocimiento).

El bug bounty se diferencia de los vulnerability disclosure programs (es decir, programas que promueven la divulgación no basada en incentivos), y su valor ha recibido recientemente un creciente reconocimiento tanto empresarial como político (propuestas normativas). (Omer Akgul, 2020)

Según Manuel Santamaría López (2016) quien se desempeña como CIO (Chief Information Officer) de la empresa Tarlogic define bug bounty como

> Los programas de recompensa por vulnerabilidades, conocidos como bug bounties o VRP (Vulnerability Reward Program), recompensan la labor de los hackers que descubren y notifican las vulnerabilidades en los sistemas informáticos de las organizaciones siguiendo un código de buenas prácticas denominado Responsible Disclosure, evitando que las vulnerabilidades se hagan públicas antes de haber sido corregidas.
>
> Organizar este tipo de programas de recompensas como método complementario al pentesting tradicional, tiene evidentes beneficios para las organizaciones:
>
> - Pone a disposición de la empresa un equipo de investigadores ilimitado
> - No existe un coste de lanzamiento. Solo se paga por el resultado (cero vulnerabilidades igual a cero euros).
> - Agiliza el descubrimiento de problemas de seguridad en los sistemas.
> - Transmite liderazgo y madurez en el sector (p. 74-75)

Otra definición también puede ser la que plantean Carlos A. Lozano y Shahmeer Amir (2018) en el libro titulado Bug Bounty Hunting Essentials que dice

> El programa de recompensas por fallos, también conocido como programa de recompensas por vulnerabilidad (VRP), es un mecanismo de crowdsourcing[4] que

[4] Se trata de un término acuñado por el periodista estadounidense Jeff Howe, para dos significados principales: 'la subcontratación de un trabajo que tradicionalmente hacía una persona, a un amplio grupo de personas en forma de convocatoria abierta' y 'la aplicación de los principios de código abierto a otros campos no relacionados con la programación'. (Fundeu, 2011)

> permite a las empresas pagar individualmente a los hackers por su trabajo de identificación de vulnerabilidades en su software. El programa de recompensas por fallos puede incorporarse a los procedimientos de una organización para facilitar sus auditorías de seguridad y evaluaciones de vulnerabilidad, de modo que complemente la estrategia general de seguridad de la información.
>
> Hoy en día, hay una serie de proveedores de software y aplicaciones que han formado sus propios programas de recompensa por errores, y recompensan a los hackers que encuentran vulnerabilidades en sus programas. (p. 74-75)

Por lo que se explica en todas las definiciones el bug bounty es un programa de recompensas que realizan las empresas u organismos para que hackers éticos busquen y reporten fallos en sus infraestructuras de hardware y software.

Además, plantean que los programas de bug bounty pueden ser públicos o privados y tienen un scope (alcance), por ello a continuación se van a definir cada uno de estos términos.

Programas Públicos

Los programas de bug bounty públicos son aquellos que están abiertos a todos; cualquiera puede realizar una búsqueda de vulnerabilidades y enviar el reporte a estos programas, siempre y cuando cumpla con las políticas del programa de recompensas por fallos.

Programas Privados

Los programas de bug bounty privados están abiertos sólo a los bugs hunters invitados. En ellos, las empresas piden a los bugs hunters con un cierto nivel de experiencia y un historial aprobado para que auditen la seguridad de la empresa y le presenten un reporte con los fallos detectados. Los programas privados de por sí son mucho menos competitivos que los públicos debido al limitado número de bugs hunters que participan. Por lo tanto, es mucho más fácil

encontrar bugs en ellos. Los programas privados también suelen tener un tiempo de respuesta mucho más rápido porque reciben menos informes en promedio.

Scope (Alcance)

Según la desarrolladora e investigadora de seguridad Vickie Li (2021) en el libro Bug bounty bootcamp: the guide to finding and reporting web vulnerabilities que escribió sobre la práctica de bug bounty desde su propia experiencia, ella describe sobre el scope (alcance)

> En primer lugar, considere el ámbito de aplicación. El scope de un programa en sus páginas de políticas especifica qué y cómo se le permite hackear. Hay dos tipos de ámbitos: activos y vulnerabilidad. El ámbito de los activos le indica qué subdominios, productos y aplicaciones puede atacar. Y el ámbito de la vulnerabilidad especifica qué vulnerabilidades aceptará la empresa como errores válidos. (p. 9-10)

Por ejemplo, la empresa podría enumerar los subdominios de su sitio web que están dentro y fuera del alcance:

Activos incluidos en el alcance	Activos fuera del alcance
a.example.com b.example.com c.example.com users.example.com landing.example.com	dev.example.com test.example.com

Tabla 1 Representación Propia. Scope (Alcance) Activos.

También comenta Li (2021)

> Los activos que aparecen en el scope son a los que se le permite hackear. Por otro lado, los activos que aparecen como fuera de alcance están fuera de los límites para los bugs bounty hunters. Ten mucho cuidado y respeta las reglas. Hackear un activo fuera de alcance es ilegal.

La empresa también suele enumerar las vulnerabilidades que considera válidas:

Vulnerabilidades en el alcance de la aplicación	**Vulnerabilidades fuera del alcance de la aplicación**
Todas excepto las enumeradas como fuera del ámbito de aplicación	Self-XSS Clickjacking Missing HTTP headers and other best practices without direct security impact Denial-of-service attacks Use of known-vulnerable libraries, without proof of exploitability Results of automated scanners, without proof of exploitability

Tabla 2 Representación Propia. Scope (Alcance) Vulnerabilidad.

Por ello el leer el alcance del programa de bug bounty en el cual se participará es probablemente lo más importante que se debe hacer, incluso antes de mirar el sitio web objetivo. Será realmente frustrante cuando se pase una semana buscando vulnerabilidades en un programa de bug bounty sólo para descubrir que el dominio que se ha probado no está incluido en el ámbito de aplicación. El ámbito convencional de un programa de recompensas por fallos contiene la siguiente información:

- Declaración de la misión
- Servicios participantes
- Dominios excluidos
- Recompensas y calificaciones
- Requisitos de participación
- Directrices de conducta
- Vulnerabilidades no calificadas
- Compromiso con los investigadores (p. 9-10)

Conclusiones del capítulo

En conclusión, en este capítulo se ha presentado el marco teórico de tres conceptos fundamentales y transversales a toda la tesis: políticas públicas, bugs y bug bounty, estos conceptos tienen una gran relevancia en la actualidad y abarcan diferentes áreas de estudio, desde la administración pública hasta la seguridad informática.

En primer lugar, hemos explorado las políticas públicas como instrumentos utilizados por los gobiernos para abordar problemas sociales y mejorar las condiciones de vida de la población, hemos comprendido que su diseño e implementación requiere un análisis riguroso que considera aspectos políticos, económicos y sociales.

Por otro lado, nos adentramos en el mundo de los bugs (o errores) en programas informáticos u otros sistemas tecnológicos como pueden ser bugs en las piezas de hardware, también hemos comprendido que estos fallos pueden afectar el funcionamiento correcto del sistema e incluso comprometer la seguridad de datos sensibles por lo tanto la detección temprana y corrección oportuna de estos bugs es fundamental para evitar consecuencias negativas.

Finalmente, exploramos el concepto novedoso del bug bounty (recompensa por errores), hemos comprendido cómo esta práctica fomenta una colaboración activa con expertos externos al ofrecer incentivos económicos, en productos de las marcas o hasta en ser publicados en un Hall of Fame (salón de la fama) a cambio de sus conocimientos técnicos para encontrar vulnerabilidades o bugs en sistemas digitales específicos.

A lo largo del capítulo también se han presentado diversas teorías y modelos relacionados con las políticas públicas y se han examinado los diferentes tipos de bugs y sus implicaciones en la seguridad informática.

Es importante destacar que estos conceptos continúan evolucionando rápidamente debido al avance tecnológico y a los constantes desafíos sociales, por lo tanto, es necesario seguir investigando y actualizando los conocimientos en estos campos para poder adaptarse de manera efectiva a las nuevas demandas que surgen día tras día y ayudan a comprender y generar pensamiento crítico para luego poder trazar nuevas propuestas integradoras que puedan ser incorporadas en la agenda de las Políticas Públicas de Estado Nacional Argentino.

En resumen, el estudio del marco teórico de las políticas públicas, bugs y bug bounty nos permite comprender la importancia de abordar problemas sociales desde una perspectiva integral, considerando aspectos políticos, económicos y sociales. Asimismo, nos muestra la necesidad de mantenernos actualizados sobre las últimas tendencias y tecnologías para poder ayudar a prevenir y solucionar problemas de seguridad informática.

"Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología"
Bruce Schneier

Capítulo II: Historia de los Bugs y Bugs Bounty

Introducción

En el mundo digital actual, los bugs (o errores) son una realidad cotidiana que afecta a sistemas y aplicaciones de todo tipo. Desde el primer programa informático escrito, los bugs han sido una preocupación constante para los desarrolladores y expertos en tecnología. Sin embargo, ¿sabías que la historia de los bugs tiene un origen mucho más antiguo?

En este capítulo, se presentará la historia de los bugs, desde sus primeras manifestaciones en la historia analógica en la cual es sorprendente encontrar que el primer inventor en utilizar la palabra bug fue Thomas Alva Edison comenzó a usar el término en la década de 1870 al momento que se encontraba trabajando en la invención de ese gran invento llamado fonógrafo, y que muchos años después ya en la era de la informática y que ha llegado hasta la actualidad. A lo largo de este viaje, descubriremos cómo los bugs han evolucionado a medida que la tecnología ha avanzado, y cómo las diferentes teorías y prácticas de programación han influido en su detección y corrección.

Para entender la historia de los bugs digitales, es necesario remontarnos a los inicios de la informática, en la década de 1940, cuando se desarrolló el primer computador electrónico, los bugs no eran un problema conocido en estos nuevos dispositivos, sin embargo, a medida que los programas informáticos se hicieron más complejos, las fallas y errores comenzaron a surgir. Los primeros programadores utilizaban técnicas de depuración para encontrar y corregir los bugs, pero no había un método estandarizado para hacerlo.

En la década de 1950 y 1960, la programación se convirtió en una disciplina más formalizada, y se desarrollaron métodos y técnicas para la detección y corrección de bugs. Durante este período, se crearon los primeros lenguajes de programación de alto nivel, como COBOL y FORTRAN, que facilitaron la programación y la detección de errores, sin embargo,

a medida que los sistemas informáticos se hicieron más grandes y complejos, los bugs se volvieron más difíciles de encontrar y corregir.

En la década de 1970 y 1980, la informática experimentó un gran crecimiento, y se desarrollaron nuevas tecnologías como los ordenadores personales y las redes de computadoras. Esto llevó a una mayor complejidad en los sistemas informáticos, lo que a su vez generó un aumento en la frecuencia y gravedad de los bugs. Durante este período, se desarrollaron nuevas herramientas y técnicas para la detección y corrección de bugs, como el uso de depuradores y el desarrollo de metodologías de pruebas de software.

En la década de 1990 y 2000, la informática experimentó una revolución con la aparición de Internet y el auge de la tecnología web. Esta nueva era de la informática llevó a una mayor interconexión entre sistemas y aplicaciones, lo que a su vez generó nuevos desafíos en términos de seguridad y estabilidad. Durante este período, se desarrollaron nuevas técnicas de pruebas de software y se crearon herramientas de seguridad para proteger contra ataques cibernéticos y vulnerabilidades de seguridad.

En la actualidad, la historia de los bugs continúa evolucionando con el auge de la inteligencia artificial, el aprendizaje automático y el Internet de las cosas (IoT), los sistemas informáticos se han vuelto más complejos e interconectados que nunca. Esto ha generado nuevos desafíos en términos de seguridad y estabilidad, y ha llevado a la aparición de nuevos tipos de bugs, como los errores de aprendizaje automático y las vulnerabilidades de seguridad en la nube.

2.1 Historia de los bugs en ciberseguridad

La historia de los bugs es sumamente interesante ya que todo el mundo pensaría que la misma nace a finales de la década del 40 en la era de las tecnologías digitales, conocida como la “Revolución Digital” o también como la “Tercera Revolución Industrial” que incorporó las tecnologías digitales al proceso de las tecnologías analógicas y mecánicas, lo cual en parte es correcto como será desarrollado a continuación, pero la historia comenzó muchos años antes, con la tecnología eléctrica y el aparato llamado telégrafo.

En la historia de la informática se recuerda un acontecimiento ocurrido en la década del 40 que es la documentación en un cuaderno de bitácoras lo que se dio en llamar “first actual

case of bug being found"; traducido, esto significa "primer caso real de un insecto -o error- encontrado", una polilla fue puesta en el cuaderno tras un error que afectó el correcto funcionamiento en la computadora Mark II y posteriormente popularizado por la Dr. Grace Hopper, quedando como un hito en la historia, pero la persona que verdaderamente acuño el termino bug fue el reconocido inventor Thomas Alva Edison y a continuación se fundamenta esta afirmación.

Según se encuentra documentado en escritos de Thomas Alva Edison, también en el diccionario Oxford de la lengua inglesa, y como se refiere en la nota escrita por Laurence Zuckerman (2000) titulada "THINK TANK; If There's a Bug in the Etymology, You May Never Get It Out" para la sección Think Tank del diario New York Time

> La historia de la polilla rebelde es un ejemplo particularmente obstinado de lo que se conoce como etimología popular. No importa lo que los historiadores e investigadores hagan para apagarlo, la molesta historia de la polilla sigue regresando. " Este es el concepto erróneo de nuestro tiempo en términos de los orígenes de las palabras ", dijo Fred R. Shapiro, bibliotecario de la Universidad de Yale y editor de un nuevo libro titulado provisionalmente " El diccionario de citas de Yale ". la historia de forma intermitente durante más de 16 años.
>
> Señaló que el Oxford English Dictionary incluye una referencia a una entrevista con Thomas Edison en una edición de 1889 del diario Pall Mall Gazette en la que el inventor se refiere a encontrar un "bug" en su fonógrafo, el artículo pasó a definir el término como "una expresión para resolver una dificultad, y que implica que algún insecto imaginario se ha ocultado en su interior y está causando todos los problemas".

En la nota escrita en la edición de 1889 de la Pall Mall Gazette cita las siguientes palabras de Thomas Alva Edison:

> *"El Señor Edison informó que había pasado las dos noches anteriores trabajando para corregir un "bug" -error- en su fonógrafo; esta es una expresión que*

> *alude a resolver una dificultad, insinúa que algún insecto imaginario se ha colado dentro de la máquina y está causando problemas".*

Aún más, el término "bug" aparece en cartas privadas de Edison desde el año de 1876, más de 10 años antes de que se publicara ese reportaje. Así, en una carta de 1878, Edison comenta sobre fallas tecnológicas argumentando que estas requieren de mucho tiempo de una observación acuciosa, además de estudio y trabajo, antes de lograr un éxito o un fracaso comercial. Con esto, hace una metáfora en relación con cúmulos de errores que se presentan como una infestación de insectos. (Mendez, 2018)

También en la nota escrita por Alexander B. Magoun y Paul Israel (2013) en el sitio Spectrum de la IEEE afirman que "El uso de "bug" para describir una falla en el diseño u operación de un sistema técnico se remonta a Thomas Edison. Acuñó la frase hace 140 años para describir problemas técnicos durante el proceso de innovación."

Una vez que se pudo fundamentar la afirmación que el término bug fue acuñado por el inventor Thomas Alva Edison al referirse a un error en el fonógrafo, o sea en un aparato analógico de su época, se pasa a relatar la historia que sí ocurrió en un aparato digital y por eso es la más célebre.

El escritor y productor Caryl-Sue (2020) en el sitio oficial de la National Geographic escribió

El 9 de septiembre de 1947, un equipo de científicos e ingenieros informáticos informó del primer error informático del mundo. Un error es una falla o falla en un sistema. Thomas Edison informó de "errores" en sus diseños ya en el siglo XIX, pero este fue el primer error identificado en una computadora. Hoy en día, los errores de software pueden afectar el funcionamiento, la seguridad y la protección de los sistemas operativos de las computadoras. La "depuración" y la gestión de errores son partes importantes de la industria de la informática. Este error, sin embargo, fue literalmente un insecto.

También refiriéndose a lo que se encuentra en exposición en el Museo Smithsonian - National Museum of American History (NMAH) como el primer registro escrito con la muestra empírica de un “bug”,

> En 1947, unos ingenieros que trabajaban en el ordenador Mark II de la Universidad de Harvard encontraron una polilla atascada en uno de los componentes. Grabaron el insecto en su cuaderno de bitácora y lo etiquetaron como "primer caso real de bug encontrado". Las palabras "bug" y "debug" pronto se convirtieron en parte habitual del lenguaje de los programadores informáticos.
>
> Entre los que trabajaban en el Mark II en 1947 estaba la matemática y programadora informática Grace Hopper, que más tarde se convertiría en contralmirante de la Marina. Este cuaderno de bitácora probablemente no era de Hopper, pero ella y el resto del equipo del Mark II ayudaron a popularizar el uso del término bug informático y la frase relacionada "debug". (National Museum of American History, n.d.)

la polilla muerta quedó plasmada en la historia como se puede apreciar en la Figura 2.

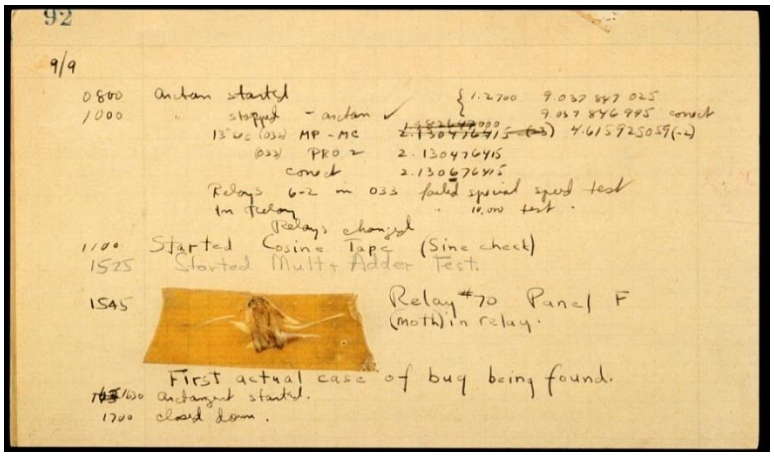


Figura 2 Cuaderno de bitácora con Bug de computadora.

Fuente *(National Museum of American History, n.d.)*

2.3 Los bugs más relevantes de la historia

En el apartado 2.2.3 se comentaron los dos hechos históricos más emblemáticos y que dieron origen al término bug en informática, el primero de ellos propiciado por Thomas Alva Edison en el siglo XIX y el segundo en el siglo XX en un aparato digital y popularizado por Grace Hopper dejando una huella en la historia.

En este apartado se desarrollarán otros hechos de la historia ocurridos con posterioridad a lo vivido con Grace Hopper y la polilla, pero no por ello menos importantes, sino totalmente lo contrario, con el advenimiento de las nuevas tecnologías de la información y las comunicaciones los bugs tomaron un rol importantísimo en la historia de la informática, por el impacto que provocan en los Estados, la sociedad y los negocios cada vez que ocurre o es detectado uno de ellos.

La siguiente es la recopilación y exposición de algunos de los hechos más relevantes de bugs ocurridos hasta la fecha de redacción de esta obra.

Como se puede apreciar en la Figura 3 se presenta una línea de tiempo con los bugs más relevantes desde 1962 hasta el año 2000.

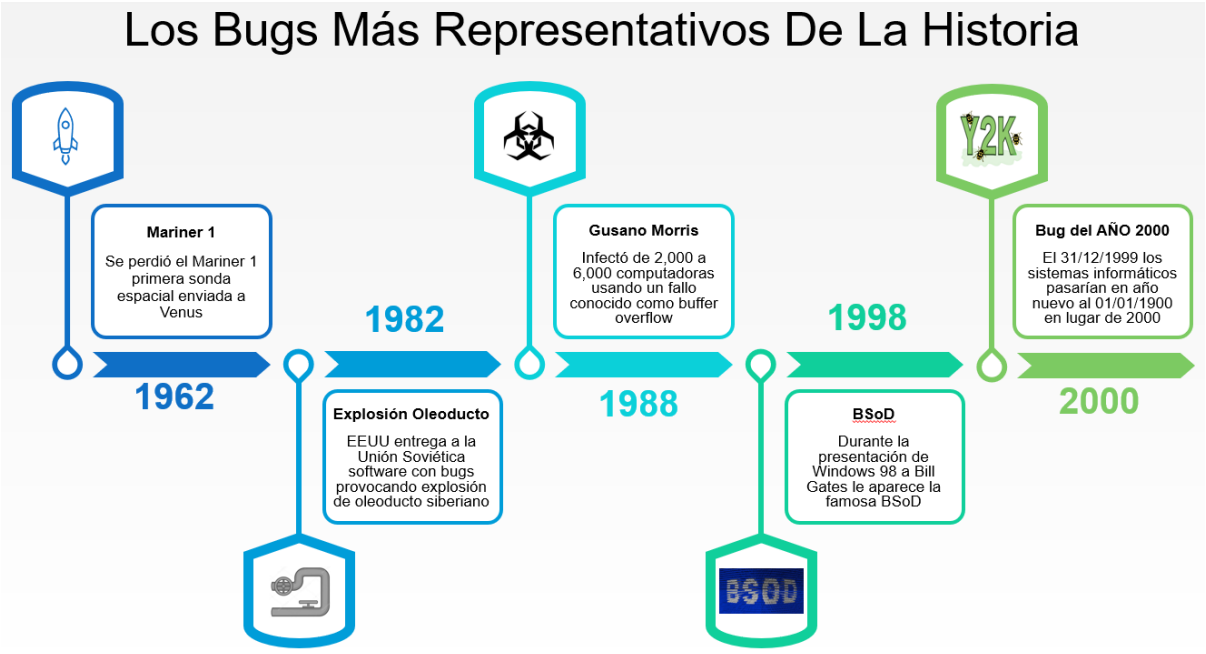


Figura 3 Representación Propia. Línea de tiempo Bugs entre 1962-2000.

1962: El sitio oficial de la NASA (National Aeronautics and Space Administration) presenta el fallo de la sonda Mariner I con el siguiente comentario "El primer intento de los Estados Unidos de enviar una nave espacial a Venus, el Mariner 1 fue destruido por el oficial de seguridad de alcance unos 290 segundos después del lanzamiento cuando se desvió de su curso" (NASA, n.d.).

En el relato del párrafo anterior no se menciona ningún problema con un bug, pero en realidad la sonda si se desvío de su curso original a causa de un error en la pieza de código que se había desarrollado, en esa pieza de código se había cometido el error de obviar colocar un guion medio "-".

Según lo redactado por el oficial de la NASA Dr. David R. Williams (n.d.)

> El fallo fue aparentemente causado por una combinación de dos factores. El funcionamiento incorrecto del equipo de la baliza aérea del Atlas provocó la pérdida de la señal de velocidad del vehículo durante un período prolongado. La baliza aérea utilizada para obtener los datos de velocidad no funcionó durante cuatro períodos que oscilaron entre 1,5 y 61 segundos de duración. Además, la Junta de Revisión Post-Vuelo del Mariner 1 determinó que la omisión de un guion en las instrucciones informáticas codificadas en el programa de edición de datos permitió la transmisión de señales de guía incorrectas a la nave espacial. Durante los periodos en que la baliza aérea no estaba operativa, la omisión del guion en el programa de edición de datos hizo que el ordenador aceptara incorrectamente la frecuencia de barrido del receptor de tierra cuando buscaba la señal de la baliza del vehículo y combinara estos datos con los datos de seguimiento enviados al cálculo de guiado restante. Esto hizo que el ordenador oscilara automáticamente en una serie de correcciones de rumbo innecesarias con comandos de dirección erróneos que finalmente desviaron la nave espacial de su curso.

Este gran fracaso de la Mariner I resultó en la pérdida de la suma de U$S18,5 millones de dólares a la NASA.

1982: Un caso muy relevante que se puede citar es el que involucra a los Estados Unidos de Norte América y la ex Unión Soviética u oficialmente Unión de Repúblicas Socialistas Soviéticas (URSS).

Cuando EE.UU. le proporcionó software con fallos que fueron implantados entre las líneas de código de forma intencional a los soviéticos, tras la ejecución del software en las plantas de los oleoductos

> El resultado fue la más colosal explosión no nuclear e incendios jamás vistos desde el espacio. En la Casa Blanca, funcionarios y asesores recibieron la advertencia de satélites infrarrojos de un extraño evento en medio de un lugar despoblado del territorio soviético. El NORAD (Comando de Defensa Aeroespacial Norteamericano) temía que fuera el lanzamiento de misiles desde un lugar donde no se conocía que hubiera cohetes basificados; o quizás fuera la detonación de un dispositivo nuclear. Los satélites no habían detectado ninguna pulsación electromagnética característica de las detonaciones nucleares. Antes de que tales indicios pudieran convertirse en una crisis internacional, Gus Weiss llegó por un pasillo para decirles a sus colegas del CSN (Consejo de Seguridad Nacional) que no se preocuparan, afirma Thomas Reed en su libro (9).
>
> La campaña de contramedidas basadas en el Dossier Farewell fue una guerra económica. Aunque no hubo bajas personales debido a la explosión del gasoducto, hubo un daño significativo para la economía soviética. (Director, 2016) según se expresa en el sitio web elciudadano.com.

Según se puede leer en el artículo titulado ¿Distopía en la red? Escrito por los sociólogos Juan Agulló y Rafael Rico (2009) dan cuenta desde la parte geopolítica los hechos ocurridos desde ambos puntos de vista

> La primera Bomba Lógica es probable que estallara, en 1982, cerca de la ciudad siberiana de Tobolsk.

Los hechos, como casi todo lo sucedido durante la Guerra Fría, siguen siendo confusos. La versión estadounidense apunta a la detonación, como consecuencia de un sabotaje, del entonces segundo oleoducto más grande del mundo. La versión ruso-soviética alude, por el contrario, a un pequeño incidente magnificado. Lo interesante de la anécdota es que, real o ficticia, remite a una forma sofisticada (pero verosímil) de utilización del conocimiento con fines sociopolíticos complejos.

En Tobolsk ocurrió, no en vano, algo –más que extraño- futurista: los autores materiales de la explosión habrían sido ingenieros de la URSS… aunque ¡no necesariamente desertores! En dicha paradoja, solo aparente, radica el quid de la cuestión: las Bombas Lógicas son programas informáticos ocultos que solo se activan si se cumplen determinadas premisas de programación. En este caso, el software utilizado para gestionar el Oleoducto Transiberiano habría sido alterado antes de su compra -probablemente con un algoritmo- para provocar, mediante una utilización rutinaria del mismo, una catástrofe.

También el Magister Dario Rizzo (2020) en su tesis de maestría también expone sobre el hecho histórico,

Al nombrar las palabras ciberataques a infraestructuras críticas, es inevitable que el término Internet sea pensado casi de forma inmediata. Sin embargo, el primer ciberataque sucedió tiempo antes de que Internet existiera tal como la conocemos.

Tuvo lugar en 1982, en el cual los atacantes consiguieron instalar un troyano en el sistema SCADA el que controlaba un oleoducto siberiano, provocándose una enorme explosión en el mismo. El ataque fue diseñado y ejecutado por la C.I.A., el que se mantuvo en secreto hasta el año 2004, cuando Thomas C. Reed, quien fuera subsecretario del Ministerio de Defensa de los Estados Unidos y asesor del expresidente

Ronald Reagan, publicara el libro "At the Abyss: An Insider's History of the Cold War", donde exponía esta historia (p. 39)

1988: El hecho se desarrolló cuando un joven estudiante de tan solo 23 años, graduado de la Universidad de Cornell y llamado Robert Tappan Morris liberó el primer gusano informático de la historia, infectando el 10% de internet de esa época (unas 60.000 máquinas conectadas en total), entre las cuales también se estima que fueron afectados sistemas de la NASA, provocando esto, pérdidas que alcanzaron la suma de noventa y seis mil millones de dólares.

El Gusano de Morris explotaba vulnerabilidades en distintos servicios, entre ellos un fallo en el modo debug de sendmail, un buffer overflow en fingerd y una incorrecta configuración del rsh/rexec que permitía saltar entre equipos sin validación.

En particular la vulnerabilidad de fingerd (Figura 4) explotada se debió a un bug que permitía realizar un buffer overflow, ello ocurría al pasarle una entrada de datos de más de 512 bytes, lo que al explotar la vulnerabilidad proporcionaba un acceso shell en el equipo afectado. Esta, según dicen, fue la vía más exitosa de infección del gusano.

El buffer overflow del fingerd tenía una shellcode que invocaba a execve("/bin/sh", 0,0).

```
pushl   $68732f      '/sh\0'
pushl   $6e69622f    '/bin'
movl    sp, r10
pushl   $0
pushl   $0
pushl   r10
pushl   $3
movl    sp,ap
chmk    $3b
```

Figura 4 Representación Propia. payload del exploit de fingerd.

1998: Durante la presentación del nuevo y renovado sistema operativo Windows 98 en COMDEX[5], la empresa Microsoft con el propio Bill Gates arriba del escenario y esperando los aplausos del público, ocurrió lo menos esperado, quien es el actualmente el responsable de

[5] **COMDEX** (una abreviatura de Computer Dealers' Exhibition) era una exposición de ordenadores llevada a cabo en Las Vegas, cada noviembre desde 1979 hasta el 2003.

marketing de Microsoft Chris Capossela, presentaba la instalación de un scanner en Windows 98 beta con la novedad del plug-and-play y ahí salió la pantalla azul, entre risas el propio dueño de la empresa Bill comenta para todos los espectadores "Esa debe ser la razón por la que aún no hemos publicado Windows 98" como se puede apreciar en el video que a día de hoy se puede seguir viendo. (Vuusteri, 2021)

"Este error ya venía ocurriendo desde versiones previas de Windows como la 95 y también posteriores al evento ocurrido siguió apareciendo el BSoD" (Pastor, 2018)

En el año 2014 el propio Raymon Chen (2014) en el blog de Microsoft comenta que "él y su equipo fueron los verdaderos desarrolladores que escribieron la pantalla azul de la muerte (BSoD)."

2000: El hecho histórico ocurrido entre el 31 de diciembre de 1999 y el 1 de enero del año 2000 que se dio en llamar Y2K, (siglas en inglés por la Y de Year y la K de Kilo que es una unidad de 1000) lo que forma Year 2000 o también como el error del milenio.

Cuando los desarrolladores de la época, hablando de la década del 60, comenzaron a utilizar en las variables de sus programas dos dígitos para las fechas en vez de cuatro, ello género que en vez de almacenar el número completo 19xx solo se almacenaba xx para el año dando por sobreentendido que era una fecha del siglo XX (1900).

Esto se debía a la poca cantidad de memoria disponible con la que contaban los ordenadores de esa época y por lo cual no se podía desperdiciar recursos en el desarrollo de software.

Lo que nunca se imaginaron los desarrolladores de la época y posteriores fue que los programas desarrollados iban a llegar al siglo XXI generando el tener que cambiar los primeros dos dígitos, o sea el 19 por el 20 como por ejemplo de 1999 al 2000, lo que a finales de la década del 80 y durante la década del 90 comenzó a preocupar a los desarrolladores de software dándose cuenta de que si iba a ser un problema el cambio de milenio, ya que las computadores iban a interpretar el 00 de cambio de milenio del año 2000 como el 01 de enero del año 1900 generando que los programas tomen esa fecha y la consecuencia en todos los sectores que su software depende de la fecha correcta.

Según una nota de la página oficial de la National Geographic sobre el Y2K dice

Los bancos, que calculan las tasas de interés a diario, se enfrentaron a problemas reales. Las tasas de interés son la cantidad de dinero que un prestamista, como un banco, cobra a un cliente, como un individuo o una empresa, por un préstamo. ¡En lugar de la tasa de interés de un día, la computadora calcularía una tasa de interés de al menos casi 100 años!

Los centros de tecnología, como las centrales eléctricas, también se vieron amenazados por el bug Y2K. Las plantas de energía dependen del mantenimiento rutinario de la computadora para controles de seguridad, como la presión del agua o los niveles de radiación. No tener la fecha correcta desbarataría estos cálculos y posiblemente pondría en riesgo a los residentes cercanos.

El transporte también depende de la fecha y hora correctas. Las aerolíneas en particular se vieron amenazadas, ya que las computadoras con registros de todos los vuelos programados se verían amenazadas; después de todo, hubo muy pocos vuelos de aerolíneas en 1900. (Rutledge, et al., 2011)

Avanzando en la década del 90 los fabricantes de hardware y software pusieron todo su esfuerzo para desarrollar parches que mitigaba el error Y2K, al llegar el momento de cambio de milenio se detectaron muy pocos problemas como comenta la nota de la National

Al final, hubo muy pocos problemas. En una instalación de energía nuclear en Ishikawa, Japón, algunos de sus equipos de radiación fallaron, pero las instalaciones de respaldo aseguraron que no hubiera una amenaza para el público. Estados Unidos detectó lanzamientos de misiles en Rusia y lo atribuyó al error Y2K. Pero los lanzamientos de misiles se planearon con anticipación como parte del conflicto de Rusia en su república de Chechenia. No hubo mal funcionamiento de la computadora. (Rutledge, et al., 2011)

Por su parte en la página oficial del banco BBVA en su sección OpenMint en una nota sobre bugs comenta sobre las consecuencias del error Y2K

> Este bug fue real. Se gastaron miles de millones de dólares para actualizar sistemas informáticos en todo el planeta. Además, se registraron algunos incidentes, aunque no muy críticos: En España, fallaron unos parquímetros. El instituto francés de meteorología publicó en su web un parte del tiempo del 1 de enero de 19100 y en Australia, las máquinas validadoras de algunos autobuses dejaron de funcionar. (Aberouch, 2015)

Como final del apartado de 2.2.4 Los bugs más relevantes de la historia se nombrarán algunos de los hechos más destacados posteriores al año 2000 sin ser desarrollados, simplemente se comentan para que el lector tenga información si quisiera seguir ampliando su conocimiento sobre el tema.

- "El 14 de agosto del 2003 al noreste y medio oeste de los EE.UU se generó un apagón debido a un error de software en el sistema de alarma de la sala de control de FirstEnergy." (fyccorp.com, 2020)
- "Aeropuerto Internacional de los Ángeles en el año 2007 al fallar una tarjeta de red deficiente fue la causante de arruinar computadoras de inmigración provocando que unas 17 mil personas no pudieran volar a sus destinos durante 9 horas." (fyccorp.com, 2020)
- "Knight Capital[6] en el año 2012, el sistema tuvo un fallo de software y en vez de ejecutar las operaciones rigiéndose por una línea de tiempo planificada, terminó por realizar las transacciones una tras otra, causando una pérdida de casi 500 millones de dólares, en tan solo 45 minutos de mal funcionamiento la compañía estuvo a punto de perderlo todo." (fyccorp.com, 2020)
- Heartbleed en el año 2014 (CVE-2014-0160), vulnerabilidad "que fue descubierta por ingenieros de la firma de seguridad Codenomicon en conjunto

[6] Es una empresa dedicada a la compra y venta de acciones de la bolsa de Wall Street. (fyccorp.com, 2020)

con un investigador de Google. Afecta a una funcionalidad de OpenSSL llamada Heartbeat, y de ahí proviene su nombre." (welivesecurity, 2014)

- Accidente fatal de un Airbus A400M en el año 2015 "Un fallo, junto con una carga incorrecta del software de los motores, provocó que el 9 de mayo de 2015 un A400M en su primer vuelo de ensayo no fuera capaz de mantenerse más allá de tres minutos en el aire." (Velis, 2017)

2.4 Historia de los Bug Bounty y por qué su masividad en los últimos años

Los programas de bug bounty tienen su inicio en el año 1983, cuando la empresa Hunter & Ready desarrolló un sistema operativo llamado Versatile Real-Time Executive, este sistema operativo supuestamente estaba libre de "bugs".

Como los fundadores de la empresa James Ready and Colin Hunter estaban seguros de que su software estaba libre de "bugs" publicaron un anuncio en el cual indicaba con el slogan "Get a bug if you find a bug" invitando a cualquier persona con los conocimientos necesarios o que se sintiera capaz de detectar y reportar un fallo entre las líneas de código del sistema operativo Versatile Real-Time Executive y por ello recibir un Volkswagen Beetle (a.k.a. Bug) como recompensa.

En la Figura 5 se puede apreciar el anuncio y en la letra chica como explicaba que "Teniendo en cuenta nuestro gusto por los coches, es posible que desee aceptar nuestra oferta de $1,000 en su lugar." que para la época era mucho dinero en efectivo.

Cabe destacar que según comenta el fundador y CTO de HackerOne Alex Rice en su cuenta oficial de Twitter: "El creador del programa, Jim Ready, responde: "¿Cuántos errores de VW regalaste?" R: Siete, pero todos los ganadores se llevaron el dinero" (@senorarroz, 2016).

Figura 5 Folleto del Primer Programa de Bug Bounty año 1983.

Fuente *(derechodelared, 2019)*

2.5 Los Bug Bounty Programs de Empresas Privadas

En la Figura 6 se presenta una línea de tiempo en la cual se pueden apreciar los programas de bug bounty que fueron siendo publicados a través del tiempo a partir de la década de los años 90'

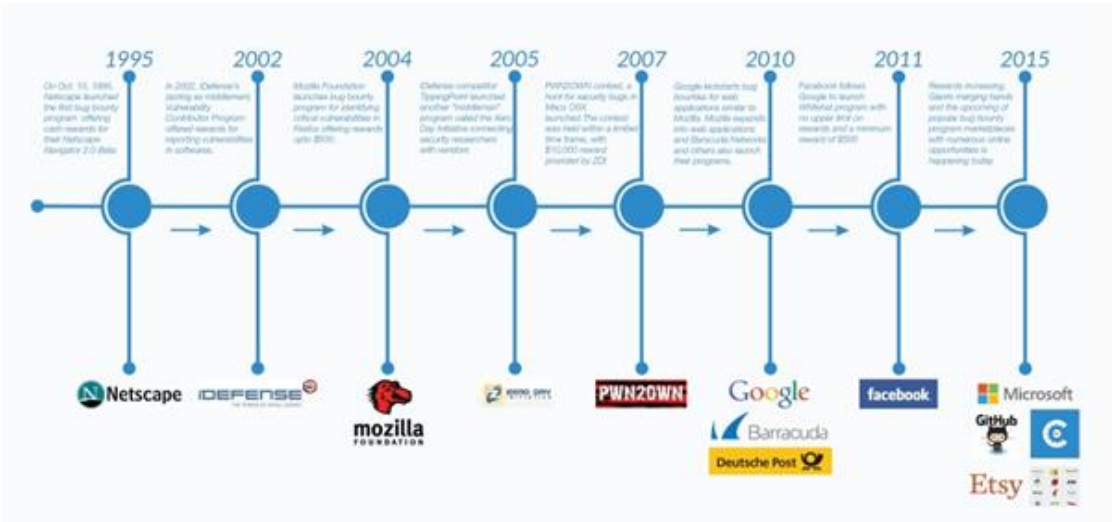


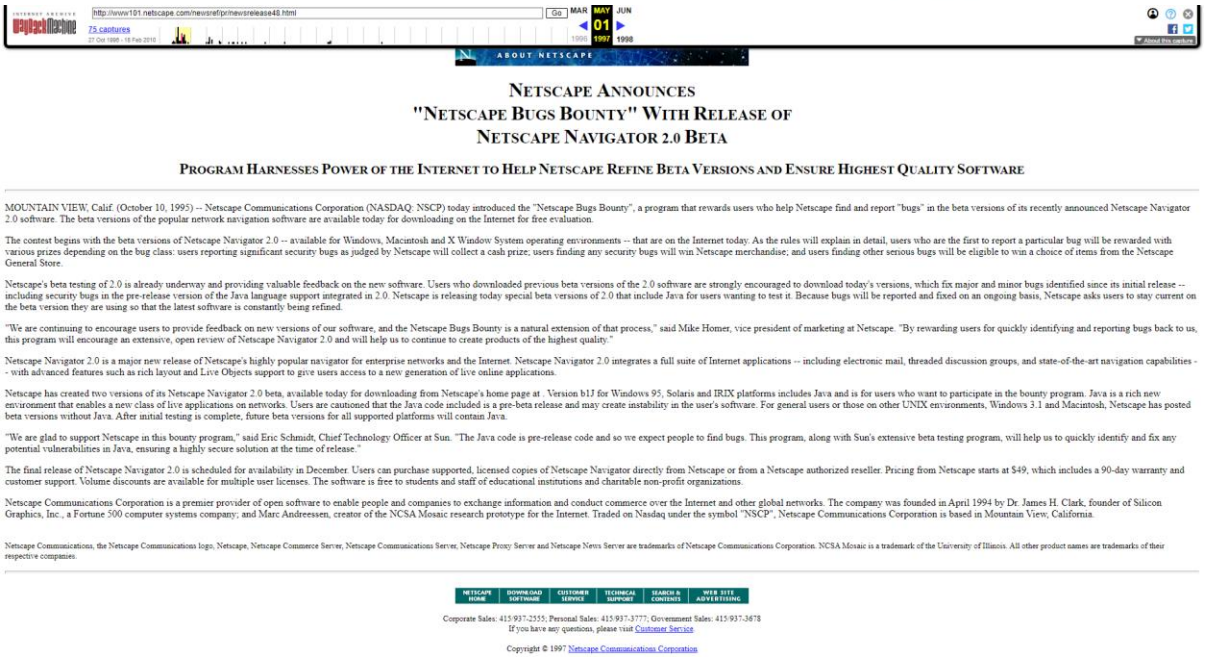
Figura 6 Línea de tiempo Programas de Bug Bounty.

Fuente *(Friis-Jensen, 2014)*

Tuvieron que pasar 12 años desde el folleto que publicó la empresa Hunter & Ready hasta que se presentara el segundo programa de bug bounty, o mejor dicho el primer programa de bug bounty, “Bugs Bounty” término que acuño Jarrett Ridlinghafer, ingeniero de Netscape pero esta vez ya en la década de los años 90, en la cual ya se habían comenzado a utilizar las conexiones de dialup para conectarse a internet en los hogares, el sistema operativo Windows de la empresa Microsoft se comenzaba a posicionar como el más utilizado de la época, que con los escritorios surgían los primeros navegadores, en principio, los usuarios utilizaban estos navegadores para acceder a sitios webs.

Por ello precisamente el día 10 de octubre del año 1995 la empresa Netscape Navigator decide publicar lo que dio en llamar el "Netscape Bugs Bounty", en la Figura 7 se puede apreciar el sitio web que aún se encuentra accesible a través del servicio de búsqueda de páginas antiguas WayBackMachine y se lee en el sitio oficial de la reconocida marca de antivirus Panda Security

> En pleno auge de su Netscape Navigator 2.0 Beta, la compañía animaba a desarrolladores de todo el mundo a encontrar errores de seguridad en su navegador. No se trataba de algo altruista ni realizado por mero entretenimiento: Netscape ofrecía una recompensa económica a los que abriesen las posibles brechas.
>
> Este hecho, que puede considerarse una mera anécdota, acabó desembocando en una práctica de lo más interesante. Y es que, sabiéndolo o sin saberlo, Netscape acababa de inventar el bug bounty, una iniciativa mediante la que las compañías deciden lanzar certámenes oficiales en los que animan a los mayores expertos en seguridad informática a encontrar fallos de seguridad en sus sistemas. (NETSCAPE ANNOUNCES "NETSCAPE BUGS BOUNTY" WITH RELEASE OF NETSCAPE NAVIGATOR 2.0 BETA, s.f)



ABOUT NETSCAPE

NETSCAPE ANNOUNCES "NETSCAPE BUGS BOUNTY" WITH RELEASE OF NETSCAPE NAVIGATOR 2.0 BETA

PROGRAM HARNESSES POWER OF THE INTERNET TO HELP NETSCAPE REFINE BETA VERSIONS AND ENSURE HIGHEST QUALITY SOFTWARE

MOUNTAIN VIEW, Calif. (October 10, 1995) -- Netscape Communications Corporation (NASDAQ: NSCP) today introduced the "Netscape Bugs Bounty", a program that rewards users who help Netscape find and report "bugs" in the beta versions of its recently announced Netscape Navigator 2.0 software. The beta versions of the popular network navigation software are available today for downloading on the Internet for free evaluation.

The contest begins with the beta versions of Netscape Navigator 2.0 -- available for Windows, Macintosh and X Window System operating environments -- that are on the Internet today. As the rules will explain in detail, users who are the first to report a particular bug will be rewarded with various prizes depending on the bug class: users reporting significant security bugs as judged by Netscape will collect a cash prize; users finding any security bugs will win Netscape merchandise; and users finding other serious bugs will be eligible to win a choice of items from the Netscape General Store.

Netscape's beta testing of 2.0 is already underway and providing valuable feedback on the new software. Users who downloaded previous beta versions of the 2.0 software are strongly encouraged to download today's versions, which fix major and minor bugs identified since its initial release -- including security bugs in the pre-release version of the Java language support integrated in 2.0. Netscape is releasing today special beta versions of 2.0 that include Java for users wanting to test it. Because bugs will be reported and fixed on an ongoing basis, Netscape asks users to stay current on the beta version they are using so that the latest software is constantly being refined.

"We are continuing to encourage users to provide feedback on new versions of our software, and the Netscape Bugs Bounty is a natural extension of that process," said Mike Homer, vice president of marketing at Netscape. "By rewarding users for quickly identifying and reporting bugs back to us, this program will encourage an extensive, open review of Netscape Navigator 2.0 and will help us to continue to create products of the highest quality."

Netscape Navigator 2.0 is a major new release of Netscape's highly popular navigator for enterprise networks and the Internet. Netscape Navigator 2.0 integrates a full suite of Internet applications -- including electronic mail, threaded discussion groups, and state-of-the-art navigation capabilities -- with advanced features such as rich layout and Live Objects support to give users access to a new generation of live online applications.

Netscape has created two versions of its Netscape Navigator 2.0 beta, available today for downloading from Netscape's home page at . Version b1J for Windows 95, Solaris and IRIX platforms includes Java and is for users who want to participate in the bounty program. Java is a rich new environment that enables a new class of live applications on networks. Users are cautioned that the Java code included is a pre-beta release and may create instability in the user's software. For general users or those on other UNIX environments, Windows 3.1 and Macintosh, Netscape has posted beta versions without Java. After initial testing is complete, future beta versions for all supported platforms will contain Java.

"We are glad to support Netscape in this bounty program," said Eric Schmidt, Chief Technology Officer at Sun. "The Java code is pre-release code and so we expect people to find bugs. This program, along with Sun's extensive beta testing program, will help us to quickly identify and fix any potential vulnerabilities in Java, ensuring a highly secure solution at the time of release."

The final release of Netscape Navigator 2.0 is scheduled for availability in December. Users can purchase supported, licensed copies of Netscape Navigator directly from Netscape or from a Netscape authorized reseller. Pricing from Netscape starts at $49, which includes a 90-day warranty and customer support. Volume discounts are available for multiple user licenses. The software is free to students and staff of educational institutions and charitable non-profit organizations.

Netscape Communications Corporation is a premier provider of open software to enable people and companies to exchange information and conduct commerce over the Internet and other global networks. The company was founded in April 1994 by Dr. James H. Clark, founder of Silicon Graphics, Inc., a Fortune 500 computer systems company; and Marc Andreessen, creator of the NCSA Mosaic research prototype for the Internet. Traded on Nasdaq under the symbol "NSCP", Netscape Communications Corporation is based in Mountain View, California.

Figura 7 Programa de Bug Bounty de Netscape Navigator 2.0 Beta.

Fuente *(Netscape, 1995)*

En el año 2002 la compañía iDefense (su nombre significa Infrastructure Defense), la cual luego sería comprada en el año 2005 por Verisign, iDefense no siguió la metodología del programa de bug bounty que había lanzado Netscape, sino que dio nacimiento a los Vulnerability Contributor Program (VCP) los cuales consistían en que "IDefense actuaba entonces como intermediario entre el investigador y los proveedores de software, ofreciendo hasta 400 dólares por reportes aceptados" (Friis-Jensen, 2014). (Figura 8)

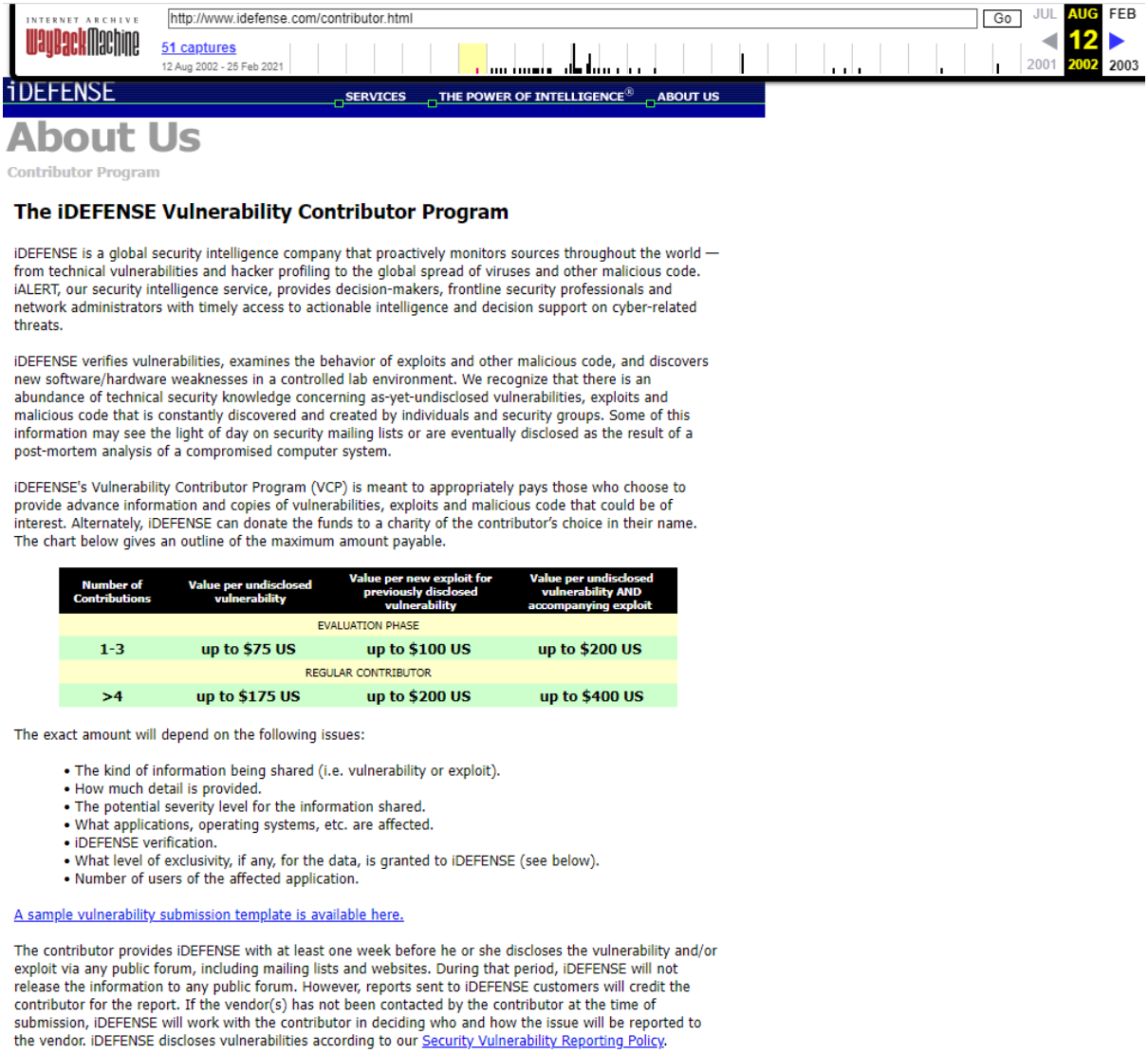


Figura 8 Vulnerability Contributor Program de iDefense.

Fuente *(iDefense, 2002)*

Dos años después, ya en el verano del 2004, otra compañía de navegadores web dio a conocer su programa de bug bounty, en esta oportunidad la empresa fue Mozilla Firefox con su Security Bug Bounty Program (Figura 9) en el cual ofrecía una recompensa de hasta 500 dólares a cualquier usuario que informara una vulnerabilidad de seguridad crítica en el software de Mozilla para usuarios finales. Mozilla Firefox hoy en día sigue manteniendo su programa de recompensas por errores, al cual destina una gran suma de dinero en efectivo anualmente,

los programas de recompensas por errores de Mozilla siguen funcionando con fuerza en la actualidad, ya que, se ha ampliado para cubrir la mayoría de sus productos.


mozillaZine

Mozilla Security Bugs Bounty Program Launched
Monday August 2nd, 2004

The Mozilla Foundation has announced a Security Bug Bounty Program. Under the new scheme, any user who reports a critical security vulnerability in end-user Mozilla software will receive a US$500 reward. The program is being funded by Linux distributor Linspire (formerly Lindows.com) and Internet entrepreneur and space tourist Mark Shuttleworth. The Mozilla Security Bug Bounty page has more details, including the process for reporting vulnerabilities and under what circumstances a report is eligible (unfortunately for sloppy developers, you cannot claim a bounty for a bug in your own code!). Netscape has run a bug bounty program in the past, though this latest Mozilla initiative is unrelated.

In addition, the Mozilla Foundation has updated the Mozilla Security Center with tips for safe browsing and information about how Mozilla keeps you secure.

Update: The article has been rewritten to include additional information. Thanks to CoffeeBreaks for his contributions to this report.

Figura 9 Security Bug Bounty Program de Mozilla.

Fuente *(mozillazine, 2004)*

En el año 2005 la empresa TippingPoint (actualmente parte de TrendMicro), en el blog de Cobalt dice “TippingPoint lanzó un programa "intermediario", llamado Zero Day Initiative (ZDI). Al igual que IDefense, TippingPoint conectaba a la comunidad de seguridad con los proveedores, ofreciendo recompensas en metálico por los informes sobre vulnerabilidades. La ZDI (Figura 10) sigue funcionando, ahora de la mano de Hewlett-Packard, que adquirió la empresa matriz de TippingPoint, 3Com, en 2010. David Endler, que ha trabajado tanto para IDefense como para TippingPoint y ha sido uno de los principales impulsores de ambos programas, ha escrito una bonita entrada en su blog, "Recordando cinco años de mercados de vulnerabilidad", en la que describe el periodo que va desde 2002 hasta el lanzamiento de ZDI.” (Friis-Jensen, 2014)

El director de investigación de vulnerabilidades de Trend Micro Brian Gorenc (2019) afirma

> Sabemos que las vulnerabilidades siguen siendo una de las mayores debilidades de seguridad de las organizaciones modernas, lo que permite a los hackers robar datos confidenciales e instalar malware que daña el resultado final y la reputación corporativa” y también que “ZDI ha liderado el mercado de la divulgación de vulnerabilidades durante casi 15 años, seguimos siendo el actor dominante en el mercado, como lo demuestra este informe. Esta es una noticia especialmente buena para

los clientes de Trend Micro TippingPoint, que están protegidos contra los ataques que aprovechan estos errores más de dos meses antes de que el parche público esté disponible.

Figura 10 Zero Day Initiative (ZDI).

Fuente *(Zero Day Initiative, 2005)*

El siguiente hito relevante en la historia del bug bounty ocurrió en el año 2007, con el surgimiento del concurso PWN20WN (Figura 11) según lo redacta Esben Friis-Jensen (2014) en el blog de Cobalt:

Tres semanas antes de la conferencia CanSecWest 2007, Dragos Ruiu anunció el concurso PWN2OWN, una caza de fallos de seguridad en Macs OSX. Esta era la forma en que Ruiu mostraba su frustración con la forma en que Apple manejaba la seguridad y la divulgación. El concurso se llevó a cabo en un plazo limitado, y el premio se anunció inicialmente como un ordenador portátil, pero más tarde se elevó a U$S10000 dólares de recompensa proporcionados por ZDI. PWN2OWN fue un gran éxito y se ha

convertido en un evento recurrente en CanSecWest. En 2014, se pagaron U$S850000 dólares en recompensas a investigadores cualificados. Este modelo de recompensas por errores al estilo de los concursos también ha sido utilizado recientemente por Stripe, en su concurso de captura de la bandera.

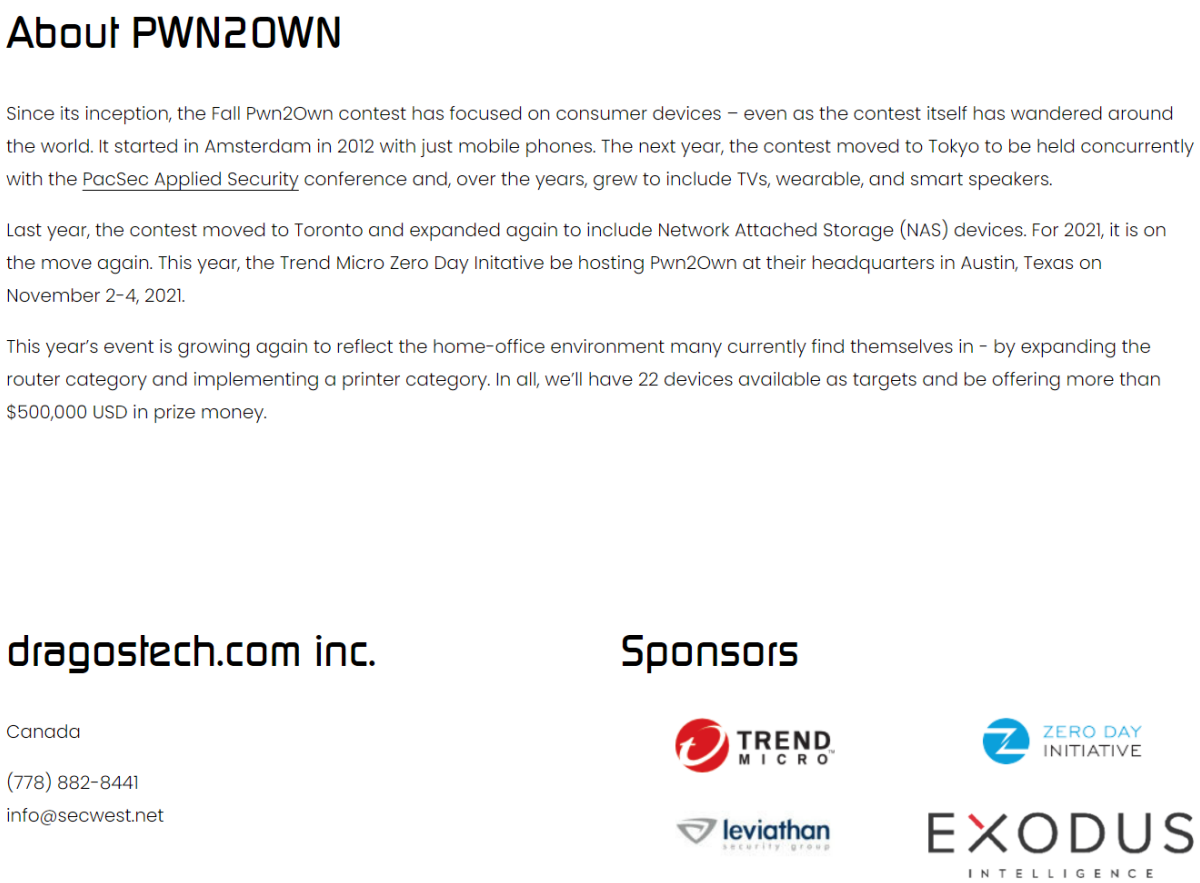


Figura 11 Página Oficial de la conferencia PWN20WN.

Fuente *(secwest, 2021)*

En la actualidad los Programas de Bug Bounty no paran de crecer año tras año, a partir de los casos que funcionan como precedente, el primero de ellos ocurrió en el año 2010 y fue de la mano de Google con su programa de vulnerability reward program y que rápidamente dio paso a otro programa para su proyecto open-source Chromium obteniendo excelentes resultados.

El segundo caso de éxito que abrió las puertas para que las empresas se sumen masivamente a los programas de bug bounty fue en el año 2011 con Facebook que vio el efecto que tuvieron los programas lanzados por Google, lo que trajo aparejado que otras empresas y organismos como Mozilla que decidió ampliar su programa a las aplicaciones web, Barracuda Networks lanzó una recompensa por fallos y Deutsche Post, el servicio postal federal alemán, lanzó una recompensa por fallos en su servicio de mensajería segura.

Hoy en día las empresas y organismos comenzaron a darse cuenta de los grandes beneficios de este tipo de iniciativa, lo que se debe a dos grandes razones:

- La primera, a la gran cantidad de bug hunters (como se los suele llamar a los hackers éticos que buscan vulnerabilidades por recompensas) que ven una gran oportunidad de obtener un rédito económico en corto plazo detectando vulnerabilidades y reportándolas, en base a la primera afirmación su justificación se debe a que ello es en muchos casos un sueldo extra a fin de mes, ya que complementan sus sueldos de trabajar día tras día sin tener que concurrir a una oficina entre ocho a nueve horas.
- La segunda, es la gran ventaja que trae a las organizaciones el tener un número muy grande de personas atacando a sus infraestructuras en busca de vulnerabilidades y solamente debiendo pagar en caso de reportes aceptados.

Entre las dos plataformas que concentran la mayor cantidad de programas activos de bug bounty, se encuentran HackerOne y Bugcrowd que, según sus informes cuentan con una cantidad de 1000 programas activos e incorporando cada día más.

A continuación, se presentan las plataformas web de HackerOne y Bugcrowd en donde se encuentran las listas de programas de bug bounty activos.

- https://hackerone.com/directory/programs
- https://www.bugcrowd.com/bug-bounty-list/

En el año 2023 y en pleno crecimiento de la inteligencia artificial, como Chat-GPT de la empresa OpenAI sacan un programa de bug bounty como se puede apreciar en la Figura 12

invitando a participar de la búsqueda de nuevas vulnerabilidades como lo indican en su propio comunicado según lo redactado en el blog de OpenAI (2023):

> La misión de OpenAI es crear sistemas de inteligencia artificial que beneficien a todos. Con ese fin, invertimos mucho en investigación e ingeniería para garantizar que nuestros sistemas de IA sean seguros y protegidos. Sin embargo, como ocurre con cualquier tecnología compleja, entendemos que pueden surgir vulnerabilidades y fallas.
>
> Creemos que la transparencia y la colaboración son cruciales para abordar esta realidad. Es por eso por lo que invitamos a la comunidad global de investigadores de seguridad, hackers informáticos éticos y entusiastas de la tecnología a ayudarnos a identificar y abordar las vulnerabilidades en nuestros sistemas. Estamos entusiasmados de aprovechar nuestros compromisos de divulgación coordinada ofreciendo incentivos para información calificada sobre vulnerabilidades. Su experiencia y vigilancia tendrán un impacto directo en mantener seguros nuestros sistemas y usuarios.

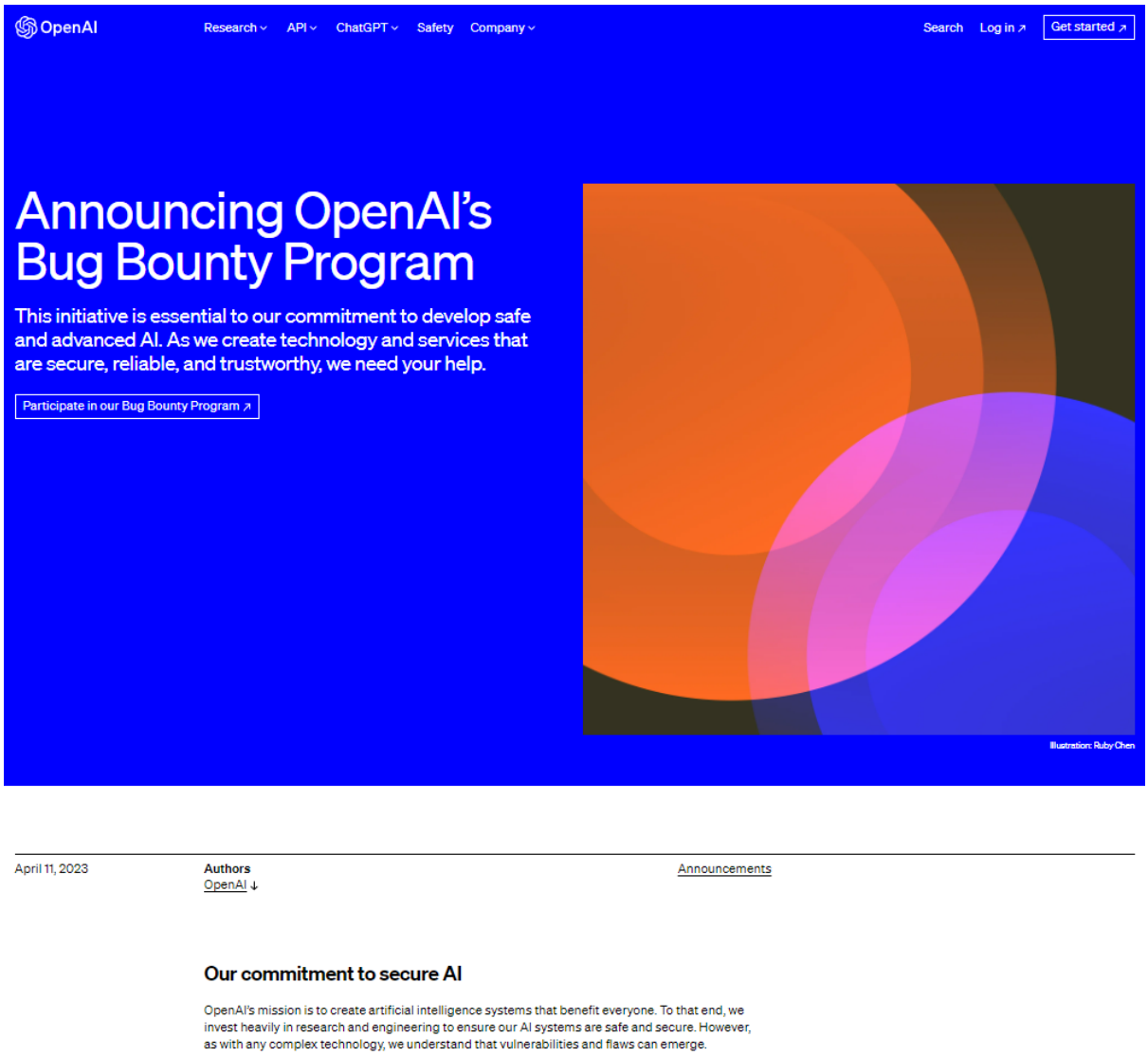


Figura 12 Página oficial de OpenAI anunciando programa de bug bounty.

Fuente (OpenAI, 2023)

La forma de implementación y articulación seleccionada por OpenAI para publicar sus programas de bug bounty es a través de la plataforma especializada Bugcrowd (https://bugcrowd.com/openai y se puede apreciar en la Figura 13) como ellos mismos lo anunciaron en su comunicado según lo redactado en el blog de OpenAI (2023)

> Nos hemos asociado con Bugcrowd, una plataforma líder de recompensas por errores, para gestionar el proceso de envío y recompensa, que está diseñado para garantizar una

experiencia optimizada para todos los participantes. Puede encontrar pautas y reglas de participación detalladas en nuestra página del Programa Bug Bounty.

Por último, resalta que según el tipo de criticidad e impacto que tenga las vulnerabilidades detectadas se podrán obtener recompensas que van desde los $200 hasta los $6500 dólares estadounidenses, pero también que en casos especiales de ser detectadas y reportadas vulnerabilidades excepcionales o que están fuera de los tipos enunciados en el propio programa como ellos mismos lo anunciaron en su comunicado según lo redactado en el blog de OpenAI (2023)

Para incentivar las pruebas y como muestra de nuestro agradecimiento, ofreceremos recompensas en efectivo según la gravedad y el impacto de los problemas informados. Nuestras recompensas van desde $200 por hallazgos de baja gravedad hasta $20,000 por descubrimientos excepcionales. Reconocemos la importancia de sus contribuciones y nos comprometemos a reconocer sus esfuerzos.

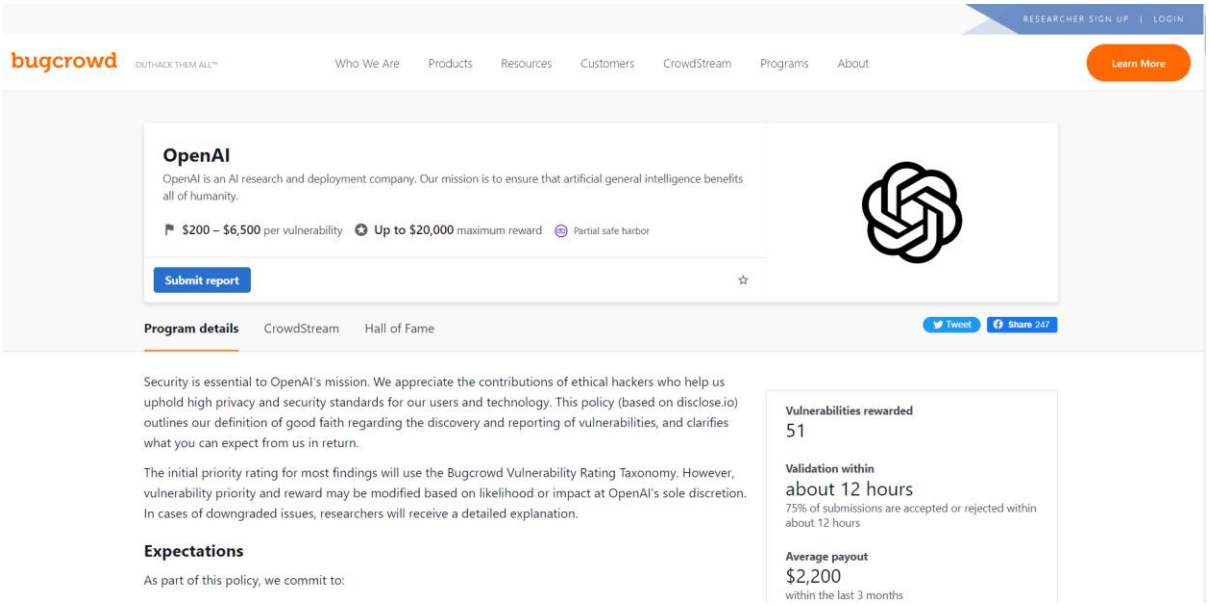


Figura 13 Página oficial de Bugcrowd programa de bug bounty de OpenAI.

Fuente (bugcrowd, 2023)

2.6 Los Bug Bounty Programs Gubernamentales

En el apartado anterior se expuso sobre los bugs bounty programs en el sector privado y cómo surgió el término bug bounty, también se comentó como fueron evolucionando las metodologías y creciendo los bugs bounty programs junto a las ventajas que generan en las organizaciones este tipo de prácticas.

En este apartado se comentarán los Programas de Bug Bounty más emblemáticos a nivel gubernamental en los diferentes países del mundo.

Se puede tomar como un punto de partida la década de los años 90, en la cual los gobiernos pagaban a personas que se especializaban en la búsqueda de vulnerabilidades en los sistemas y dispositivos, para con ello obtener una ventaja competitiva contra otros gobiernos del mundo.

Según lo explica la periodista en ciberseguridad y espionaje digital del diario New York Times Nicole Perlroth (2021) en su investigación This Is How They Tell Me the World Ends: The Cyberweapons Arms Race[7] (Figura 14)

> En los años 90, las agencias gubernamentales pagaban a contratistas como Sabien aproximadamente un millón de dólares por un conjunto de 10 exploits de día cero[8]. El equipo de Sabien destinaba la mitad de esa cantidad a la compra de bugs y luego los desarrollaba para convertirlos en exploits. Un fallo decente en un sistema ampliamente utilizado, como Windows, podría alcanzar los 50.000 dólares; un fallo en un sistema oscuro utilizado por un adversario clave podría alcanzar el doble. ¿Un fallo que permitiera a los espías del gobierno introducirse en el sistema de un adversario, sin ser detectado, y permanecer un tiempo? Fácilmente 150.000 dólares.

Según Lidia Castell García (2020) en su nota titulada ¿TIENEN FUTURO LOS PROGRAMAS "BUG BOUNTY" EN INSTITUCIONES PÚBLICAS? afirma que los

[7] https://www.youtube.com/watch?v=U8Tf29GHZ80 Consultado el 08/12/2021
[8] Una vulnerabilidad de día cero, también conocida como vulnerabilidad de día 0, es una falla de seguridad no intencionada en una aplicación de software o un sistema operativo (SO) desconocido para la parte o el proveedor responsable de corregir la falla. Permanecen sin revelarse y sin parches, lo cual deja brechas para los atacantes mientras el público sigue sin darse cuenta del riesgo. (manageengine.com, n.d.)

programas de empresas privadas cada día son más habituales, pero que no sucede lo mismo a nivel gubernamental, en el contexto que lo plantea ella haciendo referencia a los países europeos

> A nivel mundial, es bastante habitual que empresas privadas como Google, Facebook y Yahoo tengan sus propios programas de "Bug Bounty". Sin embargo, son muy pocas las instituciones públicas europeas que han hecho uso de ellos o que lo hayan manifestado. Algunos de los pocos casos conocidos son: la financiación de 14 programas de Bug Bounty de código abierto por parte de la Comisión Europea; en el sistema de voto electrónico suizo; el proyecto gubernamental "StopCovid France" para gestionar la emergencia sanitaria; y, en los Centros Nacionales de Seguridad Cibernética de Reino Unido y Holanda." Y también que "En definitiva, la creciente popularidad de los programas de recompensas y su mayor demanda en empresas privadas debería incentivar a que las instituciones públicas apostaran más por estos programas. Su rápido aumento e integración en la industria de la seguridad de la información, provocará que estos programas sean cada vez más usados en el futuro.

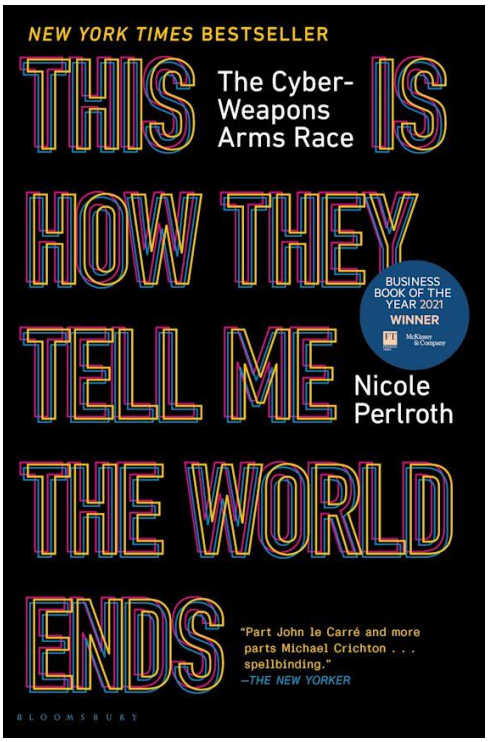


Figura 14 Portada del libro escrito por Nicole Perlroth.

Fuente (Perlroth, 2021)

En el año 2015 en el sitio web oficial de Cyber Defense Review se redacta por parte del CPT Michael Weigand y del CPT Rock Stevens (2015) un post titulado Army Vulnerability Response Program: A Critical Need in the Defense of our Nation que exponía como el secretario de Defensa Ashton Carter proponía y notaba la necesidad de que

> El Ejército de los EE.UU.. Necesita con urgencia poner en marcha un programa de respuesta y divulgación de vulnerabilidades que permita a su personal informar de manera responsable los hallazgos a una entidad centralizada que ayudaría a rastrear y resolver problemas. El Ejército podría construir una entidad de este tipo dentro de los marcos y regulaciones existentes con una sobrecarga mínima, mientras fortalece drásticamente nuestras defensas digitales. Un programa exitoso dentro del Ejército inevitablemente resultaría en una adopción a gran escala en el Departamento de Defensa y el Gobierno de los Estados Unidos.

Tras ello en el año 2016 se publica el programa piloto en la página oficial de HackerOne llamado Hack The Pentagon que estuvo activo desde el día 18 de abril del 2016 hasta el día 12 de mayo del 2016, resultando un caso de éxito para el Gobierno de los EE. UU. (Figura 15).

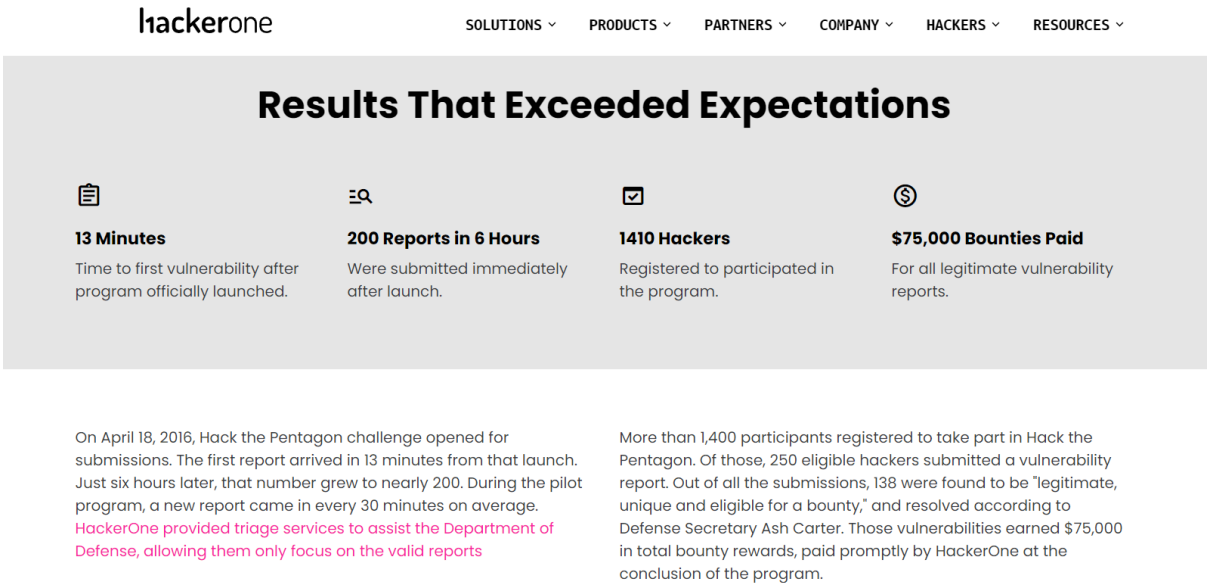


Figura 15 Página Oficial de HackerOne Programa “Hack The Pentagon”.

Fuente (hackerone, n.d.)

Tras el caso de éxito del Programa “Hack The Pentagon”, en el mes de noviembre del mismo año el Departamento de Defensa de los EE.UU. publica un comunicado anunciando su Política de Divulgación de Vulnerabilidades además que se creara el segundo Programa de Bug Bounty denominado “Hack the Army,” en la Figura 16 se pueden apreciar los hechos en una línea de tiempo. (U.S. Department of Defense, www.defense.gov, 2016)

En el año 2017 se anunciaba en el sitio web oficial de HackerOne que se habían resuelto más de 3000 vulnerabilidades, ello era un gran logro para el programa que había nacido como solo un piloto y luego fue ampliando la cartera con otros organismos del estado de EE.UU.

¡Grandes noticias para los ciudadanos estadounidenses! Se han resuelto más de 3.000 vulnerabilidades de seguridad válidas con el programa de seguridad impulsado por hackers del Departamento de Defensa de EE.UU. "Hack the Pentagon".

Hace poco más de un año, tras el éxito del programa piloto, anunciamos que el Departamento de Defensa de EE.UU. estaba ampliando sus iniciativas de " Hack the Pentagon". Hasta la fecha, HackerOne y el Departamento de Defensa han llevado a cabo retos de recompensas por errores para Hack the Pentagon, Hack the Army y Hack the Air Force. (johnk, www.hackerone.com, 2017)

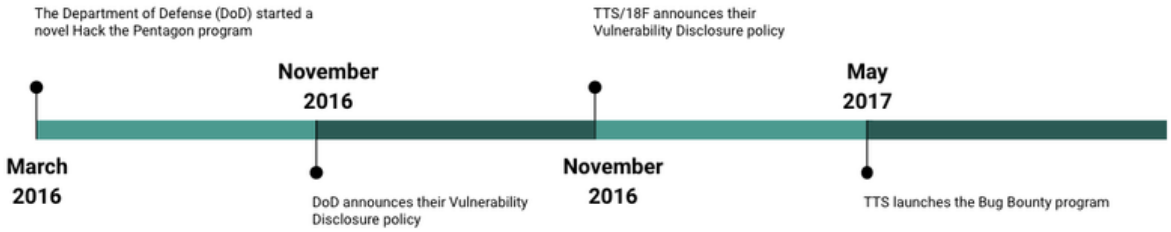


Figura 16 Página Línea de Tiempo BBP y VDP del DoD EE.UU.

Fuente (Feldman & Feola, 2020)

A mediados del año 2021 a través de otro comunicado oficial en el sitio oficial del Departamento de Defensa de los EE.UU. como se puede apreciar en la Figura 17, nuevamente vuelve a ampliar el alcance del Programa original comunicando

La política original se limitaba a los sitios web y aplicaciones de acceso público del Departamento de Defensa. La ampliación anunciada hoy permite investigar y notificar las vulnerabilidades relacionadas con todas las redes de acceso público del Departamento de Defensa, la comunicación basada en frecuencias, el Internet de las Cosas, los sistemas de control industrial, etc., dijo Goldstein. "Esta ampliación es un testimonio de la transformación del enfoque gubernamental en materia de seguridad y de la superación del estado actual de la tecnología dentro del Departamento de Defensa", dijo. (U.S. Department of Defense, www.defense.gov, 2021)

Figura 17 Página Oficial DoD EE.UU. Ampliación del Programa de VDP.

Fuente (U.S. Department of Defense, www.defense.gov, 2021)

Actualmente se están creando Programas de Bug Bounty oficiales de gobiernos de muchos países.

Se presentan tres programas de bug bounty que fueron publicados en octubre de 2021, el primero de ellos del Ministerio de Relaciones Exteriores de Finlandia, el segundo correspondiente a la Administración de servicios generales de EE.UU. (GSA) y por último el de La Agencia de Tecnología del Gobierno (GovTech) de Singapur.

El Ministerio de Relaciones Exteriores de Finlandia público en la página oficial Hackrfi como se puede apreciar en la Figura 18, según dice en el sitio web oficial de Hackrfi “HACKRFI ES EL PRIMER SERVICIO DEL MERCADO NÓRDICO EN COORDINAR Y GESTIONAR ACTIVAMENTE PROGRAMAS DE BUG BOUNTY” (Hackr.fi, 2021) un

programa de bug bounty público con una recompensa que puede ser de entre los €100 y alcanzar los €5000 según la criticidad de la vulnerabilidad reportada.

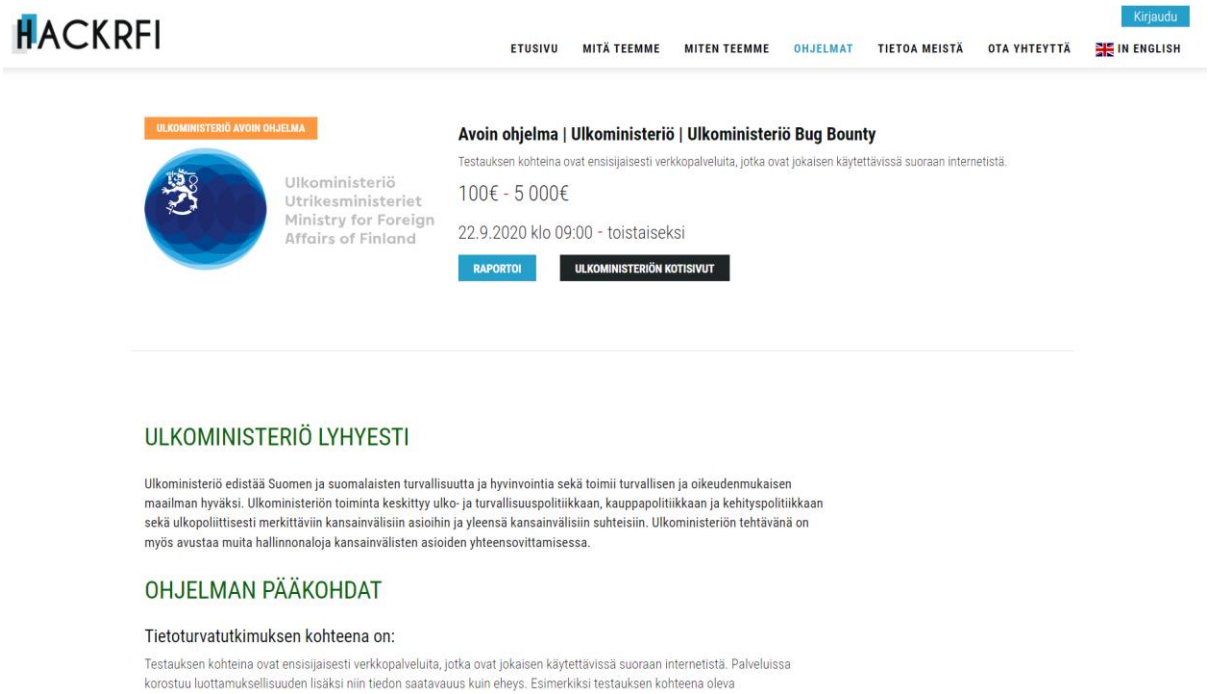


Figura 18 Página Oficial de Hackrfi Programa Finland Ministry of Foreign Affairs. Fuente (Hackr.fi, 2021)

La Administración de servicios generales de EE.UU. (GSA) es una agencia del gobierno de EE.UU. que apoya a otras agencias federales, cuenta con 47 activos gigantescos mediante la construcción y gestión de edificios gubernamentales, el desarrollo de políticas gubernamentales y la adquisición de productos y servicios.

En este contexto decide publicar un programa de bug bounty público en el cual "espera evolucionar su estructura con el tiempo y agradece la retroalimentación sobre las áreas de mejora". Los bugs hunters que reporten errores de gravedad críticos[9] recibirán hasta U$S 3000

[9] El programa de Bug Bounty de La Administración de servicios generales de EE.UU. (GSA) publicado en la plataforma https://hackerone.com/, clasifica los bugs en 4 niveles según la gravedad: Low $250, Medium $500, High $1,000 y Critical $3,000. (HackerOne, hackerone, 2020) Consultado el 29/05/2023

mil dólares, mientras que los defectos de alta gravedad recibirán recompensas de hasta U$S 1000 mil dólares.

Por último, se presenta el programa de bug bounty que fue publicado por la Agencia de Tecnología del Gobierno de Singapur (GovTech).

Según escribe Jessica Haworth (2021) en el blog de portswigger

> El brazo digital del gobierno de Singapur ha lanzado un nuevo programa de recompensas por errores que ofrece hasta U$S150000 para informes "excepcionales".
>
> La Agencia de Tecnología del Gobierno (GovTech) anunció ayer (31 de agosto) que se había asociado con HackerOne para ofrecer a los investigadores de seguridad seleccionados la oportunidad de buscar errores en un programa privado.
>
> En el comunicado, GovTech dijo que ofrecerá entre U$S250 y U$S5000 por informes de errores y asignará una bonificación de U$S150000 por "vulnerabilidades que podrían causar un impacto excepcional en sistemas y datos seleccionados".

Según dice en la nota, “es el segundo programa que publica el Gobierno de Singapur, el primero fue publicado en el año 2018, y esto se debe al gran esfuerzo que está realizando por mantener su país ciberseguro.” (Haworth, 2021)

Cerrando la nota informa que “el Gobierno de Singapur firmó un acuerdo con los EE.UU. para mejorar la cooperación y el intercambio de conocimientos sobre las amenazas cibernéticas dirigidas a las agencias financieras.” (Haworth, 2021)

2.7 Principales Plataformas de Bug Bounty

En este apartado se van a comentar las principales plataformas de programas de bug bounty que hoy en día crecen en cantidad de programas creados, empresas y organismos que se suman a ellas, y bug hunters que los utilizan para aportar sus reportes y obtener una recompensa por ello, estas plataformas las podemos dividir en tres categorías: las plataformas desarrolladas de empresas u organismos que ponen a disposición sus propios programas de bug bounty, las plataformas de programas de bug bounty que hacen de nexo entre las empresas y los bug hunters y por último los portales de compra de Zero-Days, de los cuales en este apartado nos centraremos en las plataformas de programas de bug bounty nexo entre las empresas y los bug hunters.

Muchos son los sitios en los cuales se pueden encontrar programas de bug bounty activos, tanto de organizaciones privadas como de Organismos Gubernamentales, en ellos los bugs hunters pueden reportar diferentes tipos de vulnerabilidades catalogadas según su severidad y de ello dependerá el pago que van a percibir.

Se va a desarrollar brevemente en este apartado la historia de las siguientes plataformas: HackerOne, Bugcrowd y YesWeHack (por ser las más significativas en base al criterio del maestrando), así también, al final se dejará una lista de las plataformas recomendadas por el maestrando que permitirán a los lectores conocer más plataformas disponibles.

HackerOne

Según definen Carlos A. Lozano y Shahmeer Amir (2018)

> HackerOne es una plataforma de colaboración en materia de vulnerabilidad y de caza de errores que conecta empresas con los hackers. Fue una de las primeras empresas emergentes en comercializar, utilizar seguridad y hackers como parte de su modelo de negocio, y es la mayor empresa de ciberseguridad de este tipo. (p. 5)

La plataforma HackerOne (Figura 19) tiene su origen en el año 2012, la idea surgió de la

> mano de Michael Prins, Jobert Abma y Merijn Terheggen después de llevar años reportando vulnerabilidades de seguridad a grandes compañías tecnológicas como Apple, Microsoft o Google, sin que ninguna de ellas les recompensase por ello. La mayoría de las veces era completamente ignorada. (derechodelared, 2019)

Esta plataforma desde sus origines fue sumando clientes y bug hunters, en el último reporte oficial que fue redactado por la empresa y puesto a disposición para su consulta, el cual muestra cómo se han incrementado las cifras desde el reporte anterior correspondiente al año 2019, en el documento se puede leer

Desde la publicación del Informe Hacker 2019 hace dos años, la comunidad HackerOne ha duplicado su tamaño hasta superar el millón de hackers registrados. Aunque gran parte de la comunidad todavía ha estado explorando y aprendiendo, se produjo un aumento del 63% en el número de hackers que envían informes durante el 2020. Eso es un aumento del 143% desde 2018, lo que demuestra que los hackers están aumentando sus habilidades y experiencia a medida que las organizaciones e industrias de todo el mundo invierten en soluciones impulsadas por hackers.

Los hackers ganaron 40 millones de dólares solo en 2020, contribuyendo a alcanzar el hito de 100 millones de dólares pagados a los hackers en la plataforma HackerOne. Nueve hackers han ganado más de 1 millón de dólares en la plataforma desde 2019, y un hacker superó la marca de 2 millones de dólares en 2020. (HackerOne Team, 2021, p. 2)

haciendo referencia al caso del hacker Argentino Santiago López que con tan solo 19 años en el año 2019 logrando reportar más de 1.670 vulnerabilidades únicas válidas a empresas como Verizon Media Company, Twitter, Wordpress, Automattic y HackerOne, así como a programas privados, consiguió ganar la suma de 1 millón de dólares como se comenta en el blog de la propia plataforma HackerOne. (johnk, www.hackerone.com, 2019)

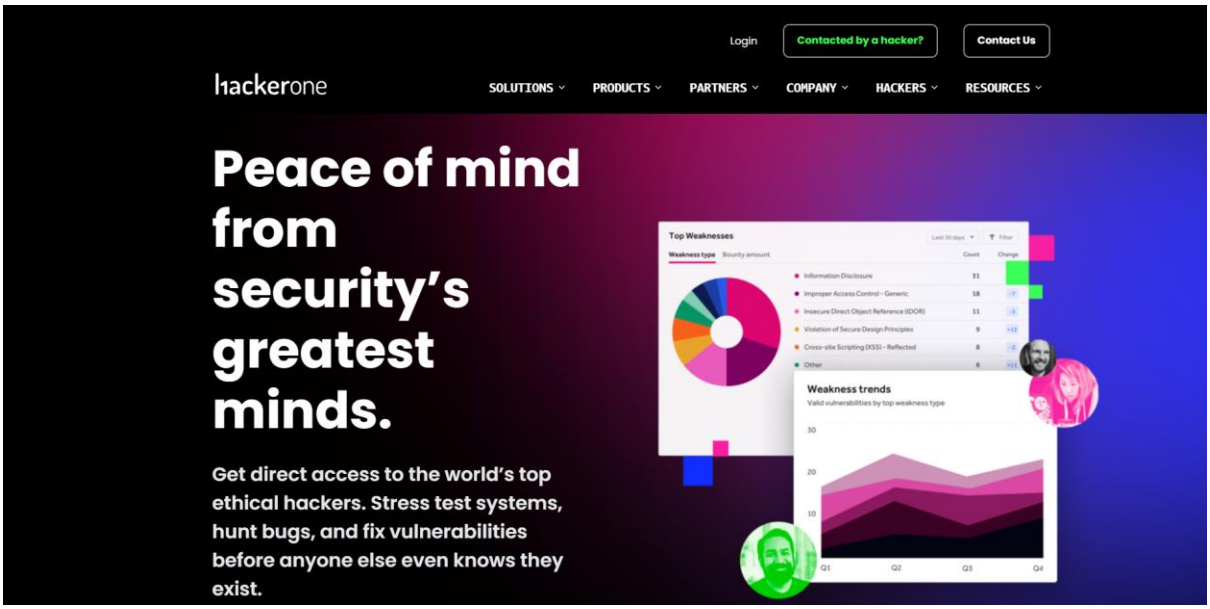


Figura 19 Página Oficial HackerOne.

Fuente *(HackerOne, www.hackerone.com, 2021)*

Bugcrowd

Bugcrowd es una plataforma (Figura 20) que también vio su nacimiento en el año 2012 como HackerOne, Bugcrowd se presenta en su página web oficial como

> Más organizaciones empresariales confían en Bugcrowd para gestionar sus programas de pen test, bug bounty, divulgación de vulnerabilidades y gestión de la superficie de ataque. Combinando el mayor y más experimentado equipo de triaje con los hackers de mayor confianza en todo el mundo, Bugcrowd genera mejores resultados, reduce el riesgo y permite a las organizaciones lanzar productos seguros al mercado más rápidamente, sin cargos ocultos. Con sede en San Francisco, Bugcrowd está respaldada por Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally Ventures, Salesforce Ventures y Triangle Peak Partners. (RELEASE, n.d.)

Entre las empresas que están dadas de alta en la plataforma de Bugcrowd se pueden encontrar a NETGEAR, LastPass, Samsung que ponen a disposición hardware y software para

que sea auditado por los bugs hunters, estas auditorías pueden ser realizadas sobre servicios web, APIs, etc.

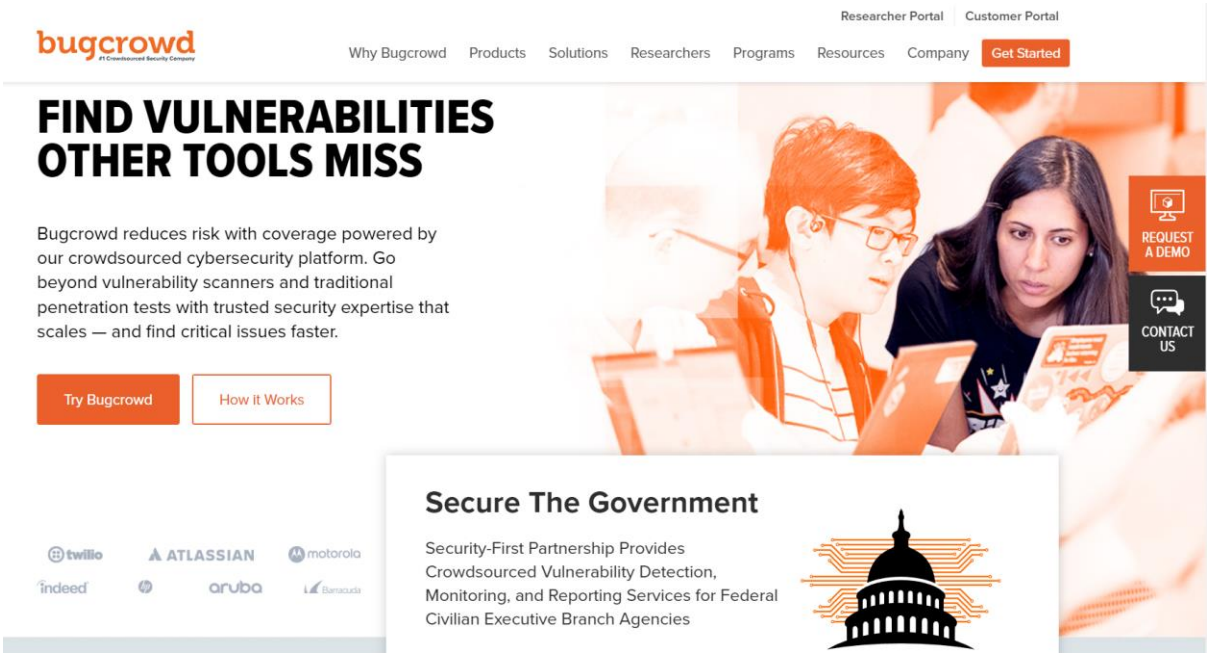


Figura 20 Página Oficial Bugcrowd.

Fuente *(Bugcrowd, www.bugcrowd.com, 2021)*

YesWeHack

YesWeHack es una plataforma española global de recompensas de errores (Figura 21), que ofrece divulgación de vulnerabilidades y seguridad de colaboración colectiva en muchos países, como Francia, Alemania, Suiza y Singapur. Proporciona una solución disruptiva de Bug Bounty para hacer frente a las amenazas que crecen año tras año con el aumento de la transformación digital de las empresas donde las herramientas tradicionales ya no cumplen con las expectativas.

Según Louise Bautista (2019) quien es Account Executive de YesWeHack la define como

YesWeHack, es la primera plataforma de Bug Bounty en Europa, estamos extendiéndonos internacionalmente con despachos en Singapur y Suiza. Hacemos Bug Bounty privado, pero también; tenemos 8000 hackers que están escritos en la

plataforma y son de varios países, tenemos 120 países en la plataforma, en principio tenemos en la plataforma todos los programas que se pueden publicar, ayudamos a las empresas a hacer los programas en las empresas privadas y los ayudamos a escoger personal, con una serie de recompensas fijadas con el consejo de YesWeHack.

Ahora, trabajamos con instituciones que son muy diferentes, como el Spotify francés, o como el Ministerio de Defensa en Francia.

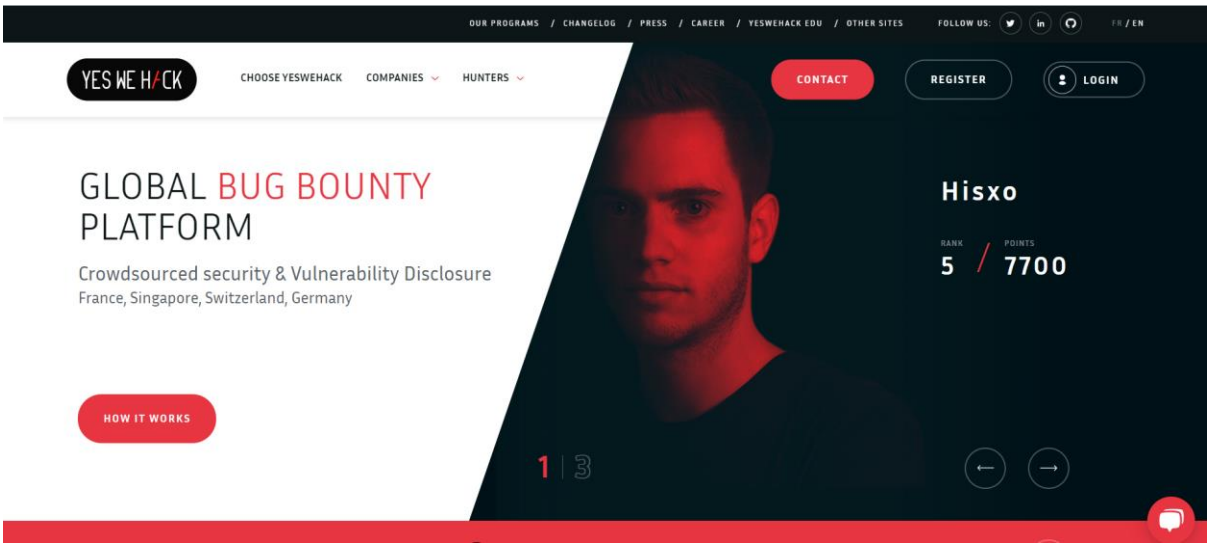


Figura 21 Página Oficial YesWeHack.

Fuente *(YesWeHack, 2021)*

La siguiente lista es de plataformas de programas de bug bounty (derechodelared, 2019) que el maestrando recomienda para continuar investigando.

- Intel: https://security-center.intel.com/BugBountyProgram.aspx
- Pentágono: https://www.hackerone.com/resources/hack-the-pentagon
- Apple: https://support.apple.com/en-au/HT201220
- Google: https://www.google.com/about/appsecurity/reward-program/
- Facebook: https://www.facebook.com/whitehat/
- Mozilla: https://www.mozilla.org/en-US/security/bug-bounty/
- Microsoft: https://technet.microsoft.com/en-us/library/dn425036.aspx

- GitHub: https://bounty.github.com/
- Uber: https://eng.uber.com/bug-bounty/
- Tor Project: https://hackerone.com/torproject
- Netflix: https://bugcrowd.com/netflix
- WordPress: https://hackerone.com/wordpress
- LinkedIn: https://security.linkedin.com/posts/2015/private-bug-bounty-program
- Paypal: https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues
- Avast: https://www.avast.com/bug-bounty

2.8 Principales Ciberataques a Organismos Gubernamentales de Argentina

En este último apartado del Capítulo II: Historia de los Bugs y Bugs Bounty se desarrollarán los hechos más relevantes en materia de ciberdelitos, ocurridos en los últimos siete años (2017-2023) en el ámbito local (Figura 22) y (Figura 23), particularmente ciberataques a organismos gubernamentales de la República Argentina.

Figura 22 Representación Propia. Línea de tiempo Ciberataques Argentina entre 2017-2021.

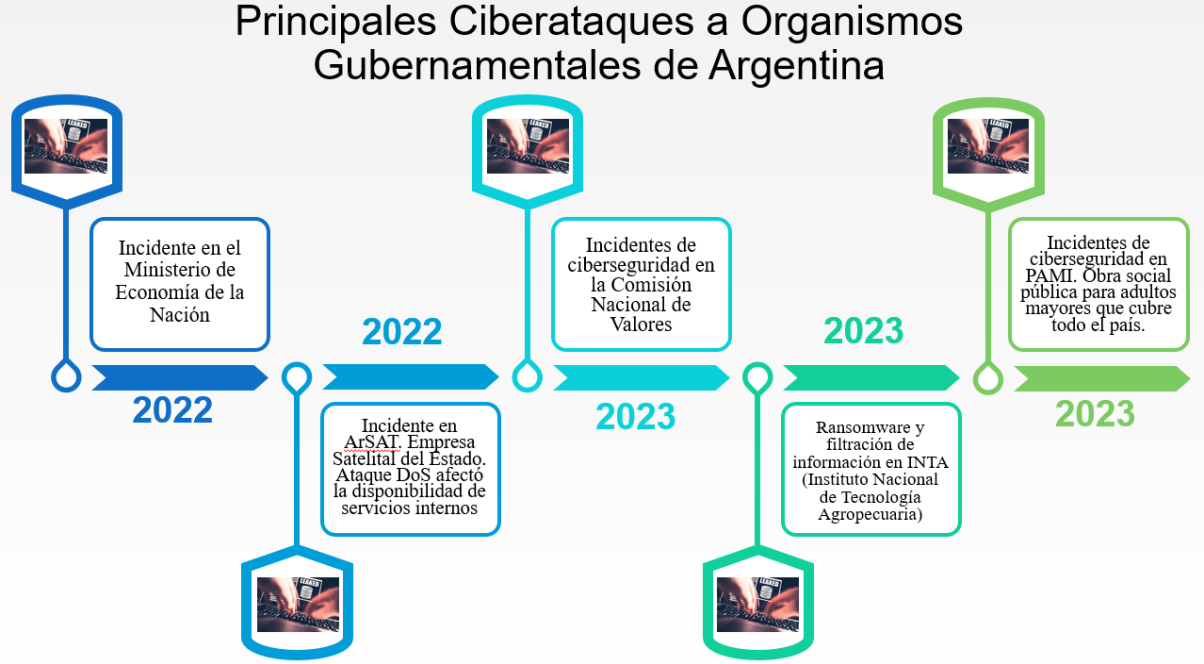


Figura 23 Representación Propia. Línea de tiempo Ciberataques Argentina entre 2022-2023.

Durante el verano del año 2017 más precisamente en el mes de enero ocurrió un hecho que puso en alerta al Ministerio de Seguridad de la Nación Argentina, tras sufrir un ciberataque la propia ministra que en ese momento era la Dr. Patricia Bullrich.

El día 26 de enero del año 2017 la cuenta oficial de Twitter de la ministra sufrió un ciberataque, en el cual ciberdelincuentes después de obtener el acceso a la cuenta escribieron los siguientes tweets “matan personas todos los días, la gente se siente insegura cuando sale a la calle, a los que roban, matan o violan los dejan libres”, decía en uno de los tuits. También hubo insultos hacia el presidente y reclamos por la gestión: “Macri gato. Hacé una bien y dejale el puesto a alguien que tenga HUEVOS u OVARIOS para tomar medidas drásticas si es necesario”. "Soy una borracha inútil que le queda grande este cargo igual que al presidente @mauriciomacri el cargo de presidente", siguió la cuenta de Bullrich durante el ciberataque. (Figura 24)

El hackeo a la ministra se produjo a través de un correo electrónico enviado desde una cuenta falsa -a nombre de la Embajada de Bolivia en Argentina- y a través de un documento ejecutable que permite acceder a las contraseñas del titular de la cuenta que recibe el correo.

En este mismo acto se detectó que hubo alrededor de 30 cuentas de diferentes agentes del Ministerio de Seguridad de la Nación involucradas que fueron afectadas en el hackeo sumada a la de la ministra, lo que luego se amplió a que en realidad no fueron solo 30 mails, sino que más de 200 como se publicaba en la nota del diario Noticias

> Según papeles a los que pudo acceder Noticias de fuentes cercanas a los hechos, no fueron treinta correos los afectados por el ataque, tal como le informó la Policía Federal al juez Sebastián Ramos, sino más de doscientos mails. Algunos corresponden al personal policial de Jujuy, Chubut y Río Negro, entre otras provincias. Los correos habrían sido sustraídos del Sistema Nacional de Información Criminal (SNIC), que depende del ministerio de Seguridad (Catalán, 2017).

Y también que hubo más ataques en el mes de diciembre del año 2016 a otros dos organismos, el Ministerio de Producción

> a cargo de Francisco Cabrera, le hackearon 18.000 cuentas que exponían datos personales, correos, teléfonos, perfiles en redes y documentos privados. Este ataque ha sido atribuido, en sitios especializados en temática hacker, a un extranjero cuyo nombre "artístico" es Kapustkiy. En un intercambio de mails con NOTICIAS, el señalado Kapustkiy reconoció -en su ciberjerga- su intervención. "Fue un ataque por fuerza bruta con un toque de ingeniería social en el que probé diferentes combinaciones para vulnerar el sistema", dijo.
>
> Por otro lado, el Ministerio de Salud, a cargo de Jorge Lemus, vio inutilizadas sus computadoras por un virus que infectó el sistema. En las últimas semanas los empleados y funcionarios de la Jefatura de Gabinete, a cargo de Marcos Peña, tuvieron inconvenientes con sus cuentas y el acceso al sistema. Si bien estas situaciones no fueron denunciadas, la información fue reconocida por fuentes allegadas a los ministerios de Modernización y de Justicia (Catalán, 2017).

Figura 24 Tweets de la Cuenta Hackeada de la ministra Dr. Patricia Bulrrich.

Fuente *(Denuncia, 2017)*

En el año 2018 ocurrieron otros ciberataques a varios organismos gubernamentales de la República Argentina entre ellos el ciberataque a la página oficial de la Policía de la Ciudad a la cual le realizaron un Defacement (Figura 25), procedimiento que consiste en realizar un cambio de la página de inicio del sitio web para con ello lograr que el visitante del sitio vea esta página adulterada en vez de ver la página original, según una nota del diario Clarín de esa fecha el ciberdelincuente

> se identificó como "[S]" para pedir por la libertad de Emanuel Velez Cheratto, un joven cordobés procesado por el ciberataque al sitio del diario El Litoral de Santa Fe.
>
> En el mensaje que subieron a la web de la fuerza porteña, también colgaron dos links con archivos de 3.6 GB de bases de datos que había en el servidor. Fuentes de la fuerza informaron a Clarín que esos archivos no pertenecen a policías, si no a "datos viejos de inscripciones por la web al instituto" (Policiales, 2018).

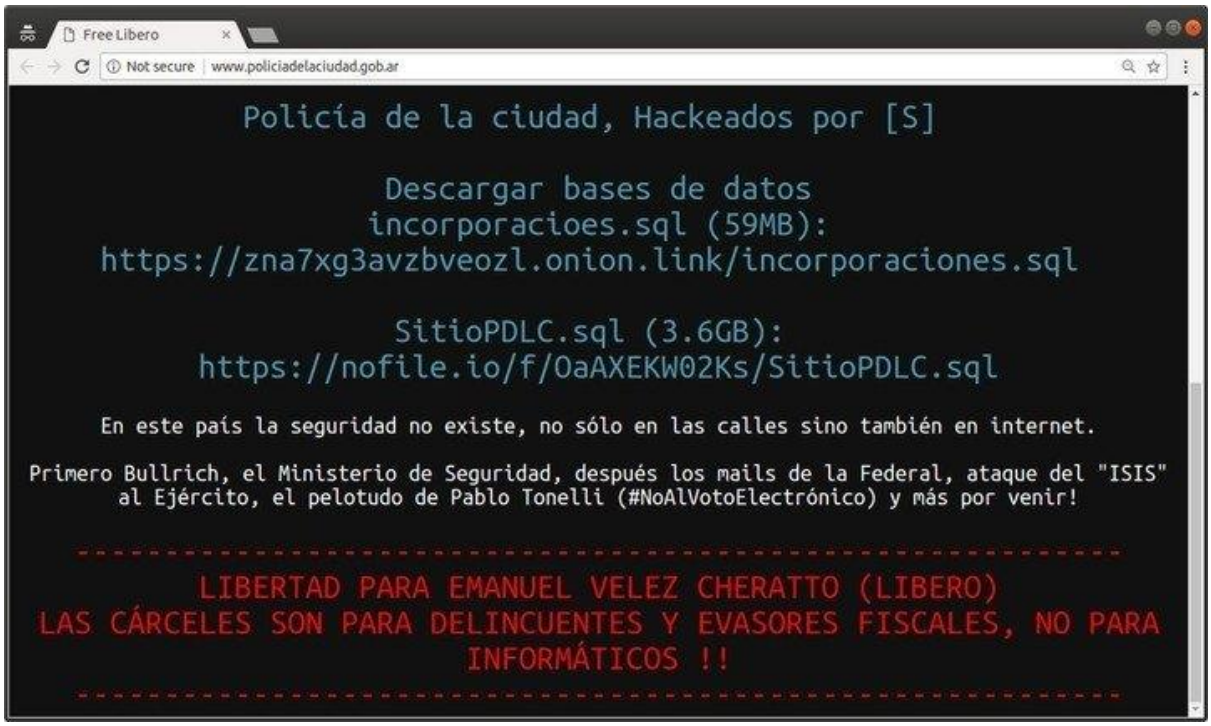


Figura 25 Página Oficial de la Policía de la Ciudad Hackeada

Fuente *(Policiales, 2018)*

En el año 2019

un usuario de Twitter llamado @lagorraleaks (luego suspenderían su cuenta), se adjudicó el hackeo a la Policía Federal Argentina ocurrido el día 12 de agosto de 2019 a través del tweet que se puede apreciar en la Figura 26 en la cual indicaba que iba a subir 700 GB de información de la Policía Federal Argentina y de la Ciudad a la Deep Web. (LA NACIÓN, 2019)

Según se plantea en una nota del diario la nación de la época

Las hipótesis son dos: una venganza por la detención de los dos hackers que se habían infiltrado en la cuenta oficial de la ministra Bullrich y de la Policía de Seguridad Aeroportuaria (PSA), hechos ocurridos en enero de 2017. La otra pista que analizamos es que @lagorraleaks sea un funcionario policial infiel", afirmó una alta fuente oficial. (Nicola, 2019)

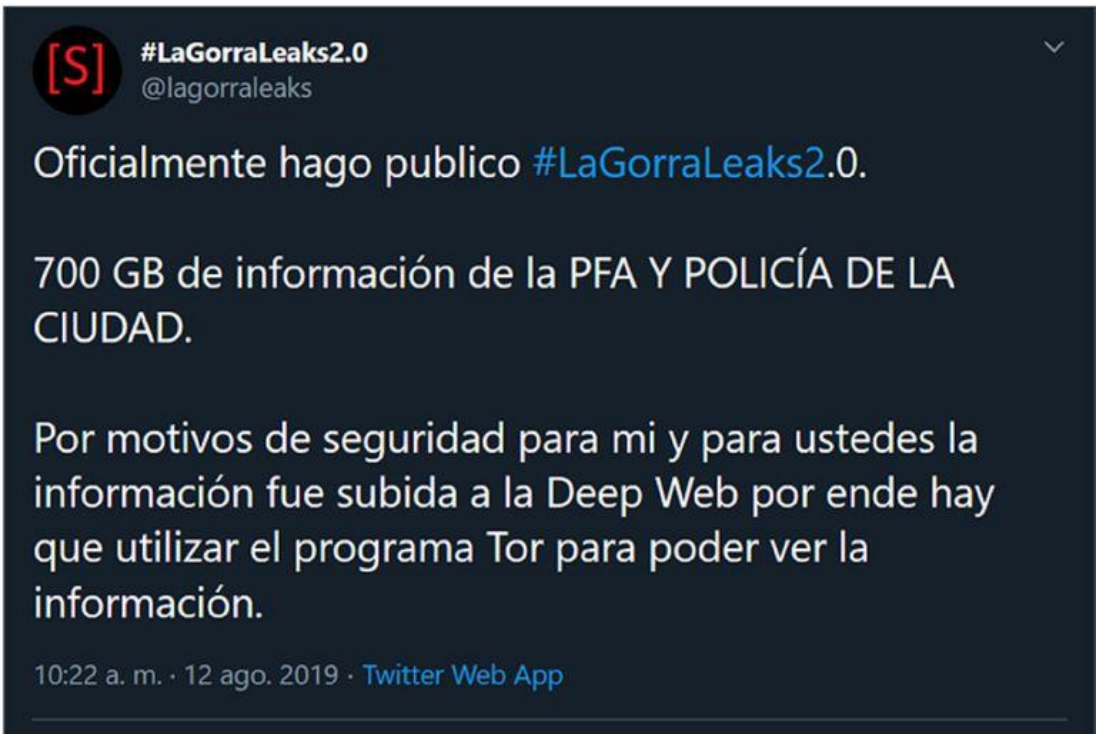


Figura 26 Twitter Oficial de la LaGorraLeaks2.0 Policía Federal Argentina Hackeada

Fuente *(Nicola, 2019)*

En el año 2020 ocurrió otro ciberataque que impactó mucho en la Administración Pública Nacional, fue el ataque recibido a través de una infección por ransomware en la Dirección Nacional de Migraciones (DNM) dependiente del Ministerio del Interior.

Según fue informado por la propia cuenta oficial de Twitter de la DNM (Figura 27) el Sistema Integral de Captura Migratoria (SICaM) también fue afectado por el ransomware ocasionando retrasos en los pasos fronterizos, este ciberataque también derivó en que solicitaban los ciberdelincuentes un rescate de plata por la no divulgación de información del organismo

Un ataque de ransomware conocido como NetWalker secuestró información de la Dirección Nacional de Migraciones (DNM) y amenaza con publicar esos datos de la dependencia del Ministerio del Interior si no se efectúa un pago millonario. Se habla de US$ 76 millones, pero las autoridades confirmaron que son US$ 4 millones (a pagar en Bitcoins). El plazo vence hoy miércoles. Los datos que se publicaron en este caso se difundieron a través de una captura de pantalla donde se ven carpetas que hacen referencia a la Agencia Federal de Inteligencia (AFI), consulados, embajadas e informes de flujos migratorios. Allí también se ve el lapso de tiempo en el que la información será publicada (infotechnology, 2020). (Figura 28)

Figura 27 Twitter Oficial Dirección Nacional de Migraciones.

Fuente *(@Migraciones_AR, 2020)*

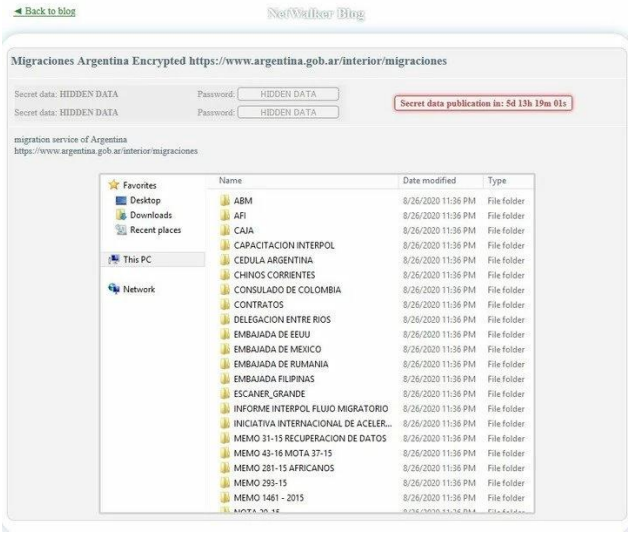


Figura 28 Twitter Oficial Dirección Nacional de Migraciones.

Fuente *(infotechnology, 2020)*

Se presentará un caso que ocurrió en septiembre del año 2021 cuando el Instituto de Obra Social de las Fuerzas Armadas y la Seguridad (IOSFA) recibió un ciberataque que afectó la base de datos de sus afiliados, ello, aunque en su sitio oficial a través de un comunicado oficial (Figura 29) afirman la existencia del ataque, lo minimizaron diciendo que se trata de una base de datos obsoleta e incompleta.

Figura 29 Página Oficial IOSFA Informando Hackeo.
Fuente *(IOSFA, 2021)*

Por último, en los últimos dos años (2022-2023) se fueron intensificando los ciberataques a diferentes organismos del Estado Nacional Argentino, esto pone de manifiesto como es exponencial su crecimiento año tras año como se comentó en la introducción.

Durante el transcurso del año 2022 se comentan los ciberataques:

- Incidente en el Ministerio de Economía de la Nación: Durante el mes de septiembre circuló en Twitter que el Grupo de hackers, Everest, habría anunciado en su sitio web la venta de los accesos al Ministerio de Economía y Finanzas Públicas de Argentina. Ante la noticia, se le solicitó a la Justicia que investigue el posible hackeo. (RM/fl, 2022)
- Incidente en ArSAT. Empresa Satelital del Estado. Ataque DoS afectó la disponibilidad de servicios internos: ARSAT INFORMA: En el día de hoy sufrimos una caída en el área de sistemas corporativos que afectó sólo a los sistemas internos de la empresa. En este momento nos encontramos aplicando procedimientos de prevención. (@ARSATSA, 2022)

Durante el transcurso del año 2023 se comentan los ciberataques:

- Incidentes de ciberseguridad en la Comisión Nacional de Valores: El grupo de ransomware Medusa difundió una lista con 1,5 TB de información al vencer el plazo de pago. Pedían un rescate de 500 mil dólares. (Brodersen, 2023)
- Ransomware y filtración de información en INTA (Instituto Nacional de Tecnología Agropecuaria): La infraestructura tecnológica del INTA fue hackeado, por lo que pidieron u$s2,5 millones a cambio. La red brinda servicios a más de siete mil personas en el país. (ámbito, 2023)
- Incidentes de ciberseguridad en PAMI. Obra social pública para adultos mayores que cubre todo el país: Un virus informático afectó el sistema de PAMI. El grupo ransomware Rhysida que se adjudicó el ataque dijo tener un TB de información, a su vez el 19/08/2023 se publicaron 831 GB de datos. (Assalian, 2023)

Conclusiones del capítulo

En conclusión, la historia de los bugs y los programas de recompensas por encontrarlos, conocidos como bug bounty, es un claro ejemplo del poder de la colaboración entre hackers éticos y organizaciones privadas y organismos de diferentes estados, a lo largo de este capítulo hemos podido apreciar cómo el descubrimiento y reporte responsable de vulnerabilidades en sistemas informáticos ha evolucionado desde prácticas ilegales a una actividad legítima que beneficia tanto a las organizaciones como a los investigadores.

Se pudo presentar esta historia pasando desde los sistemas analógicos del Siglo XIX así también por los sistemas digitales Siglo XX más precisamente en la década de 1940 cuando surgen las primeras computadoras.

Los bugs han existido desde los primeros días de la informática, pero con el crecimiento exponencial de las tecnologías digitales se han convertido en una preocupación cada vez mayor para empresas e individuos. La amenaza que representan para la seguridad cibernética ha llevado a muchas compañías a establecer programas de bug bounty, ofreciendo recompensas económicas o reconocimiento público por encontrar y reportar fallas en sus sistemas.

Estos programas no solo brindan incentivos financieros para que expertos en seguridad dediquen su tiempo y talento al descubrimiento activo de vulnerabilidades, sino que también fomentan una cultura más segura dentro del mundo digital. Al premiar el comportamiento responsable y ético, se crea un ambiente propicio para compartir conocimientos e información valiosa sobre ciberseguridad.

Además, estos programas ayudan a reducir drásticamente el riesgo potencialmente dañino asociado con las vulnerabilidades desconocidas al permitir que sean identificadas antes de ser explotadas por actores maliciosos. Esto resulta especialmente crucial considerando el panorama actual donde ataques cibernéticos sofisticados son cada vez más comunes.

Se pudieron repasar los principales bugs que ocurrieron en la historia y que dejaron una huella por su magnitud o impacto como ser el caso del fallo de la sonda Mariner I enviada por la NASA para explorar Marte y debió ser derriba apenas fue lanzada por un bug que desviaba su trayectoria, otro caso emblemático fue el del Gusano de Morris que afectó un número significativo de computadoras para la época y dio nacimiento al primer CERT de EE.UU., también se tuvieron fallos por bugs no tan críticos pero si chistosos como el ocurrido en el

lanzamiento del sistema operativo Windows 98 por Microsoft en el cual un fallo en los drivers de una scanner hizo sorprender a Bill Gates ante su jefe de ingenieros, y el famoso Y2K o fallo del siglo 2000 cuando se pensó que las computadoras no iba a poder soportar el cambio de numeración de siglo pasando del 1999 al 2000 y lo cual fue superado.

Por su parte también se pudo realizar un recorrido por varios programas de bug bounty gubernamentales, pasando por el programa Hack The Pentagon del DoD de los EEUU y que al ser un éxito se fue extendiendo a diferentes organismos de los Estados Unidos y que llega hasta nuestros dias, también programas como el de Finlandia a través de la página de HackRFI.

En resumen, la historia detrás de los bugs y bug bounty ha sido un viaje desde el anonimato y la ilegalidad hacia una colaboración ética y beneficiosa para todas las partes involucradas. A medida que continuamos avanzando en nuestra dependencia de la tecnología, es fundamental seguir promoviendo este tipo de programas para garantizar un entorno digital más seguro y protegido tanto para organizaciones privadas como para los organismos públicos.

“Mi mensaje para las empresas que piensan que no han sido atacadas es: no estás buscando lo suficiente”
James Snook

Capítulo III: Encuesta

Introducción

El capítulo presenta el armado y análisis de los datos obtenidos en la encuesta que se mantuvo activa entre los días 12/11/2021 y el 01/12/2021 y que se volvió a abrir para conseguir el número necesario para la muestra el día 04/06/2023 y se cerró el 29/06/2023. La finalidad buscada fue la de recolectar información de la población objetivo en base a respuestas sobre la utilización de programas de bug bounty en el Estado Nacional Argentino, esta población objetivo fueron las Áreas de Tecnología, Seguridad de la Información o de Ciberseguridad de los Organismos de la Administración Pública Nacional (APN).

Como una fuente de información fidedigna el maestrando tomo al Instituto Nacional de Estadística y Censos (INDEC) quien es el encargado de recolectar y analizar los datos sobre los agentes de la Administración Pública Nacional (APN) en su sitio oficial se puede leer

> La Secretaría de Gestión y Empleo Público de la Jefatura de Gabinete de ministros estableció, a través de las resoluciones 194/2022 y 196/2022, la obligatoriedad de informar mensualmente la dotación de recursos humanos de las jurisdicciones y entidades comprendidas en los incisos a) y c) del artículo 8° de la Ley Nº 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.
>
> Incluye a las empresas del Estado, las sociedades del Estado, las sociedades anónimas con participación estatal mayoritaria, las sociedades de economía mixta y todas aquellas organizaciones empresarias en las cuales el Estado Nacional tiene participación mayoritaria en el capital o en la formación de las decisiones societarias, como así también a los Fondos Fiduciarios total o mayoritariamente integrados con

bienes y/o fondos del Estado nacional comprendidos en los incisos b) y d) del mencionado artículo. (Indec, n.d.)

Según los datos obtenidos desde el sitio oficial del INDEC en su informe correspondiente a la Dotación de personal de la administración pública nacional, empresas y sociedades del mes de mayo de 2023 (2023) dice que el número total de agentes de la APN es de 339.756 agentes siendo este número la población potencial.

Los criterios de selección para obtener la población objetivo fueron tomados de la población potencial que fueron definidos como los agentes de toda la APN pero tomando solo los que pertenecen a las áreas de Tecnología, Seguridad de la Información o de Ciberseguridad de los Organismos de la APN. (Figura 30)

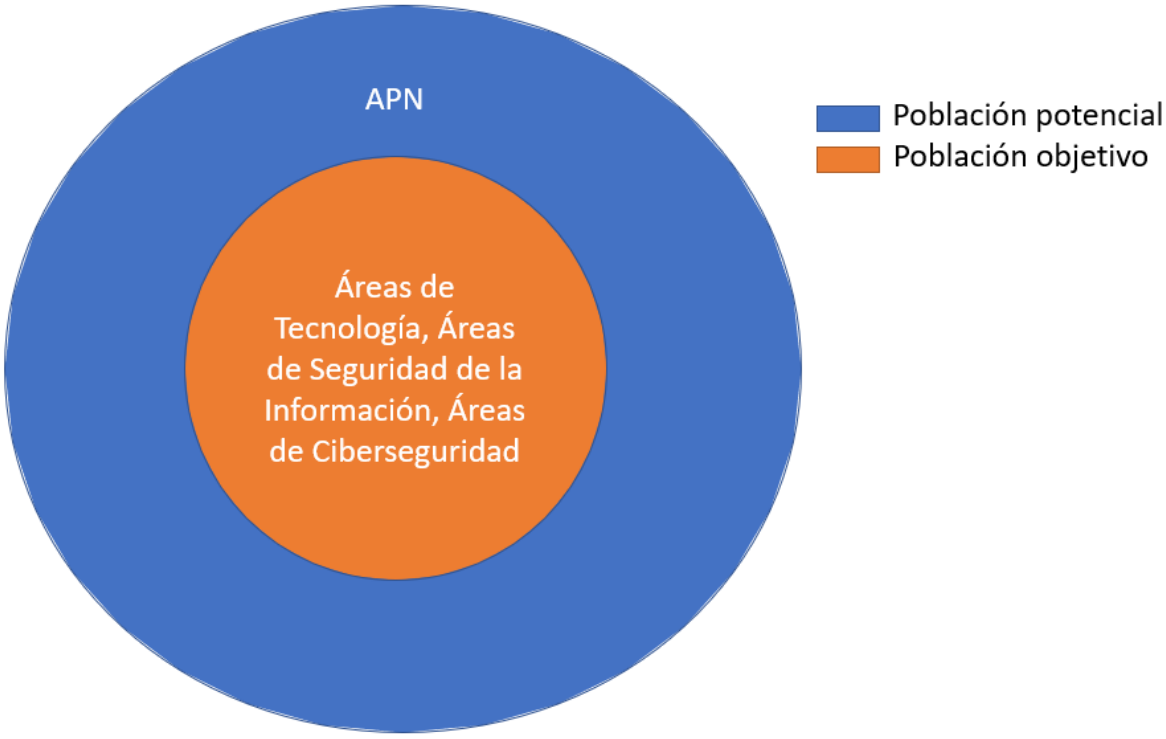


Figura 30 Representación propia. Población potencial y población objetivo.

Al no contar el maestrando con el total de agentes que componen la población objetivo (agentes que pertenecen a la APN y que pertenecen a las áreas de tecnología, áreas de seguridad de la información o áreas de ciberseguridad) se calculará el tamaño de la muestra necesaria con

la fórmula del cálculo del tamaño de muestra infinita para variables cuantitativas con un nivel de confianza del 90% y un margen de error del 10%.

$$n = \frac{Z_{\alpha}^{2} * p * q}{e^{2}}$$

n = Tamaño de muestra buscado.

z = parámetro estadístico que depende el Nivel de Confianza (NC).

e = Margen de error máximo aceptado.

p = Probabilidad de que ocurra el evento estudiado (éxito).

q = Probabilidad de que no ocurra el evento estudiado (fracaso).

Por lo tanto, las variables que se utilizarán para obtener el tamaño de la muestra para esta tesis serán de un nivel de confianza del 90% y de un margen de error del 10%:

n = Tamaño de muestra buscado.

z = 90% = 1, (Según tabla).

e = 10% = 1, (Según tabla).

p = 50% = 0,5.

q = 50% = 0,5.

Se reemplazan los valores en la ecuación:

$$n = \frac{(1{,}645)^{2} * 0{,}5 * 0{,}5}{(0{,}10)^{2}}$$

$$n = 68$$

Por lo tanto, luego de aplicada la fórmula se llegó al resultado que se deben obtener 68 muestras para tener un nivel de confianza del 90% y de un margen de error del 10%.

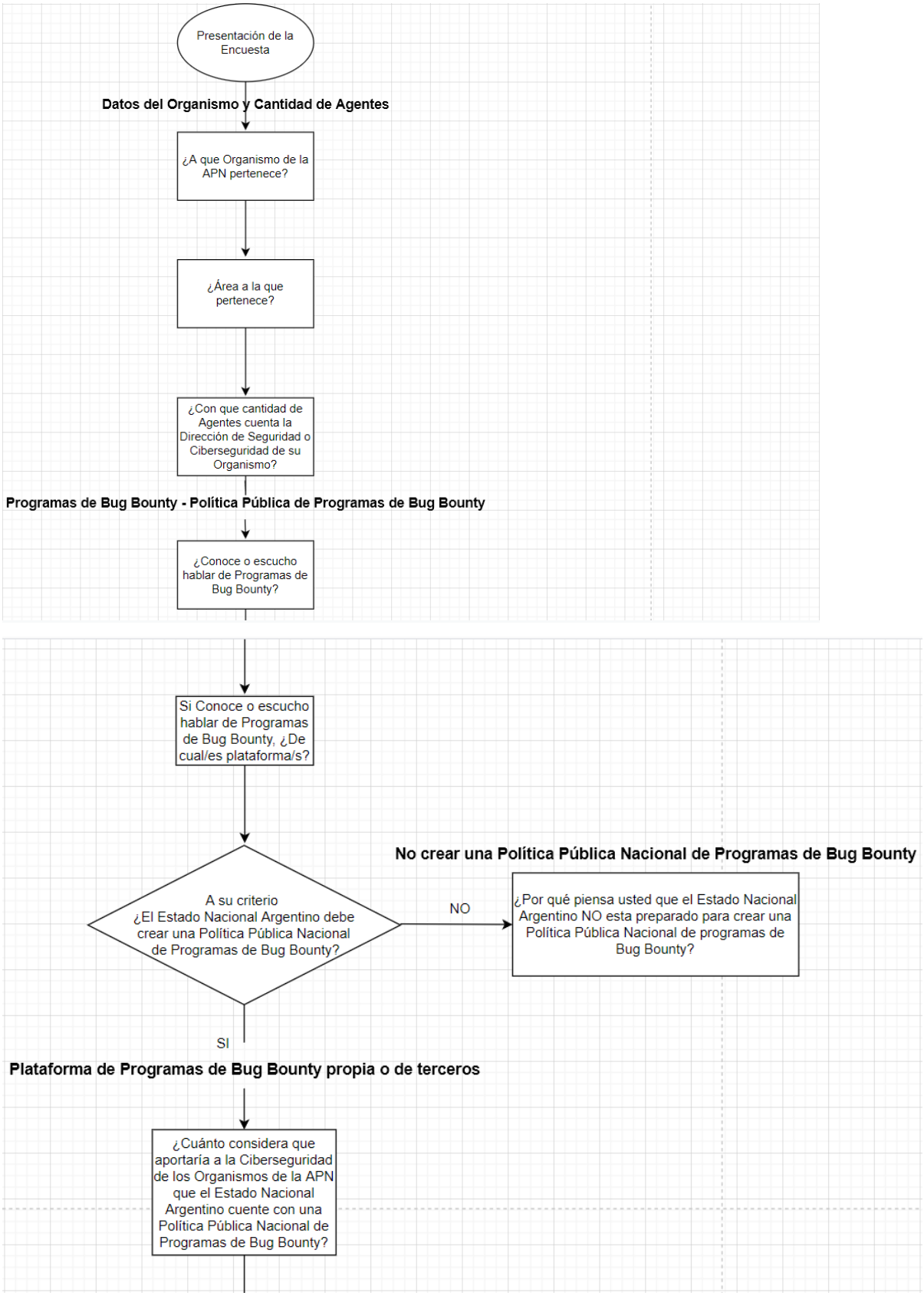
3.1 Presentación de la Encuesta

La encuesta tuvo un enfoque cuantitativo, según la definición de los Doctores Sampieri, Collado y Baptista (2006) el "Enfoque cuantitativo usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías."

La encuesta se compuso de siete secciones divididas de la siguiente manera:

- **Sección 1**: Presentación de la Encuesta.
- **Sección 2**: Datos del Organismo y Cantidad de Agentes.
- **Sección 3**: Programas de Bug Bounty – Política Pública de Programas de Bug Bounty.
- **Sección 4**: No crear una Política Pública Nacional de Programas de Bug Bounty.
- **Sección 5**: Plataforma de Programas de Bug Bounty propia o de terceros.
- **Sección 6**: Infraestructura Crítica.
- **Sección 7**: Recompensas.

Además, contó con la siguiente lógica, que se presenta en el flujograma de la (Figura 31), habiéndose elaborado al momento de la creación de la encuesta.


Presentación de la Encuesta
Datos del Organismo y Cantidad de Agentes
¿A que Organismo de la APN pertenece?
¿Área a la que pertenece?
¿Con que cantidad de Agentes cuenta la Dirección de Seguridad o Ciberseguridad de su Organismo?
Programas de Bug Bounty - Política Pública de Programas de Bug Bounty
¿Conoce o escucho hablar de Programas de Bug Bounty?
Si Conoce o escucho hablar de Programas de Bug Bounty, ¿De cual/es plataforma/s?
No crear una Política Pública Nacional de Programas de Bug Bounty
A su criterio ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty?
NO
¿Por qué piensa usted que el Estado Nacional Argentino NO esta preparado para crear una Política Pública Nacional de programas de Bug Bounty?
SI
Plataforma de Programas de Bug Bounty propia o de terceros
¿Cuánto considera que aportaría a la Ciberseguridad de los Organismos de la APN que el Estado Nacional Argentino cuente con una Política Pública Nacional de Programas de Bug Bounty?

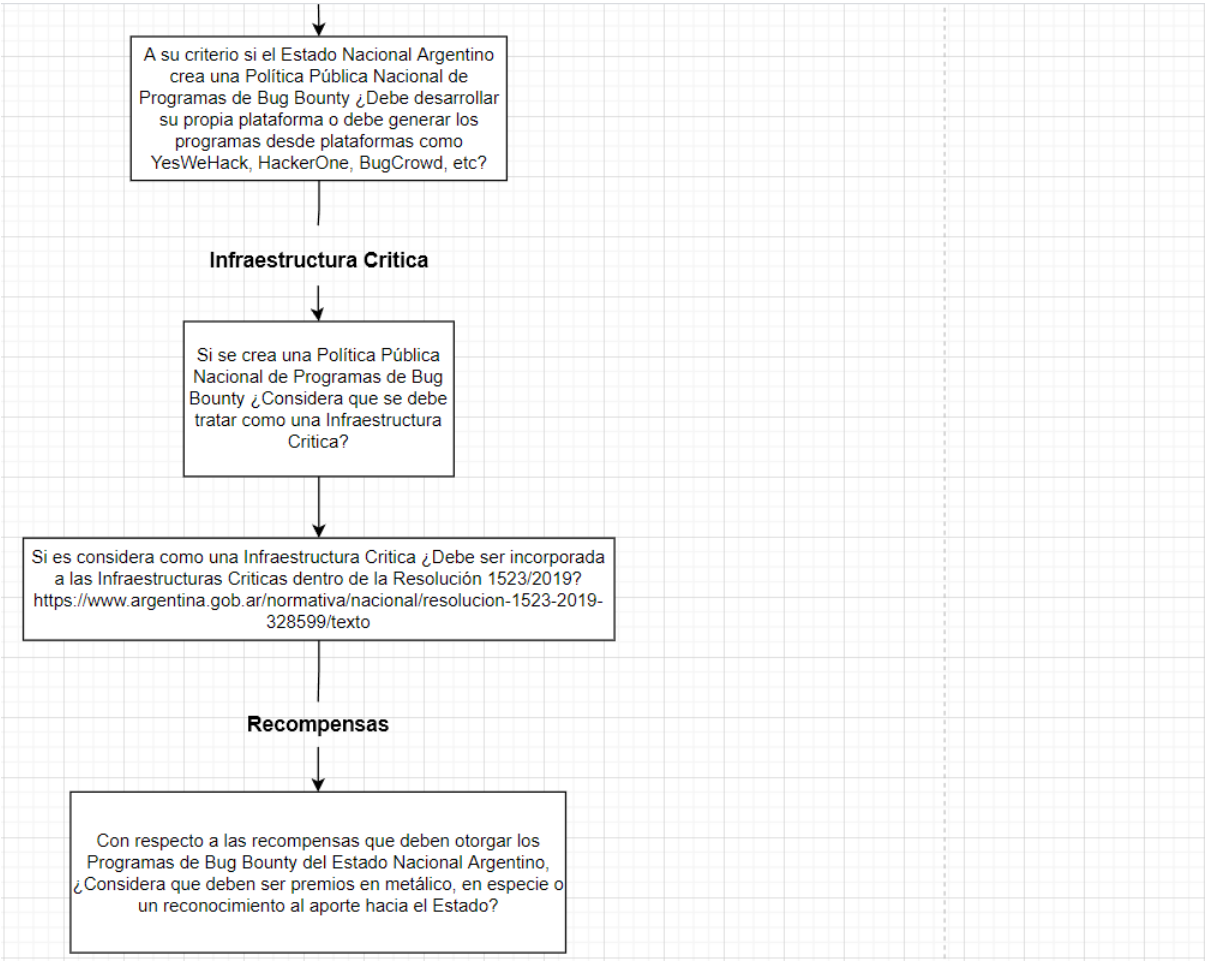


Figura 31 Representación Propia. Flujograma de Encuesta.

3.2 Análisis de los datos

A continuación, se realiza el análisis de los datos obtenidos, la encuesta se compartió por diferentes medios los cuales fueron: correo electrónico, telegram, whatsapp y signal a diferentes Agentes de la Administración Pública Nacional en los días que estuvo disponible la misma.

Tras llegar al número de 69 de respuestas y teniendo como resultado de la fórmula que se debían obtener 68 para alcanzar el nivel de confianza necesario para poder comenzar a realizar un análisis objetivo de los datos, se decidió cerrar la misma y pasar al análisis de datos, de todos los formularios obtenidos fueron respondidos de forma completa 51, y había una respuesta que no era mandatorio el ser respondida, por lo tanto 18 agentes decidieron dejarla sin responder.

Sección 1: Presentación de la Encuesta

Se presenta la encuesta al público objetivo que fue seleccionado, para ello se escribió un texto en el cual se le avisó la finalidad y el uso que se le iba a brindar a los datos obtenidos de las respuestas a las preguntas de la encuesta. (Figura 32)

Figura 32 Representación Propia. Presentación de Encuesta.

Sección 2: Datos del Organismo y Cantidad de Agentes

En la primera sección se buscó conocer el Organismo en el cual trabaja el encuestado y la cantidad de agentes que componen la Dirección de Seguridad de la Información, Ciberseguridad o similar de su Organismo.

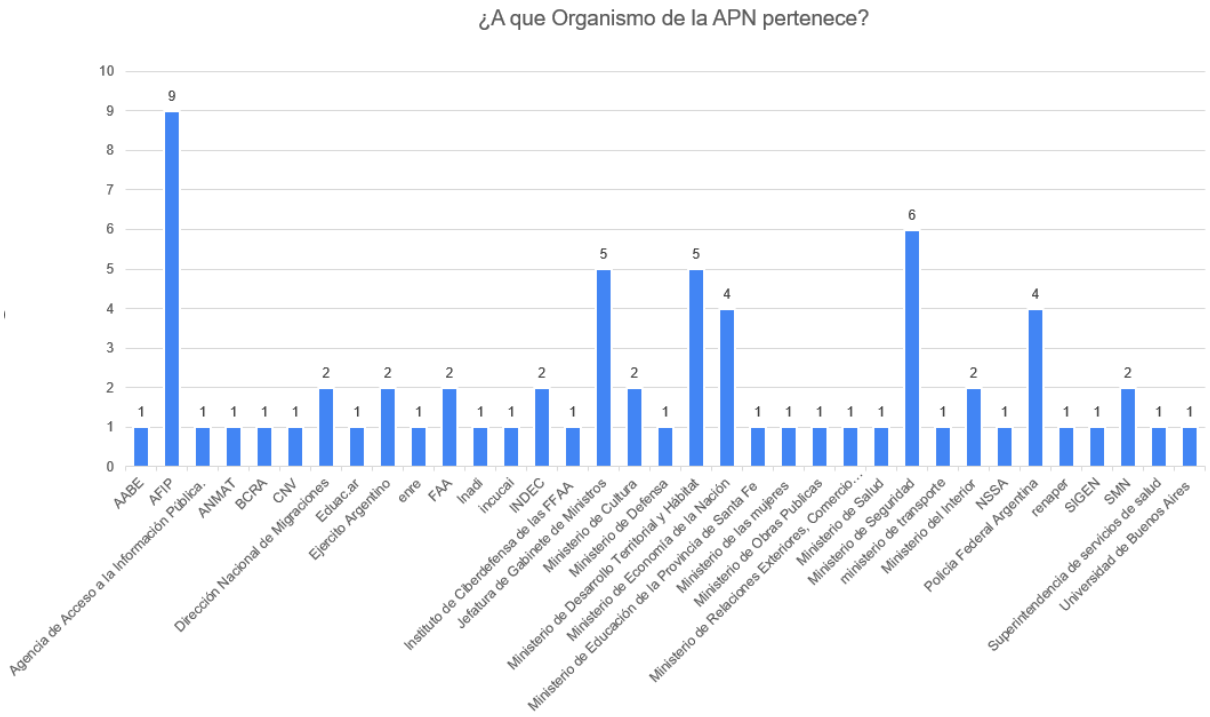


Figura 33 Representación Propia. Respuesta Pregunta 1.

De las 69 respuestas obtenidas en 13 casos respondieron agentes del mismo Organismo, todos los restantes agentes fueron de distintos Organismos de la Administración Pública Nacional. (Figura 33)

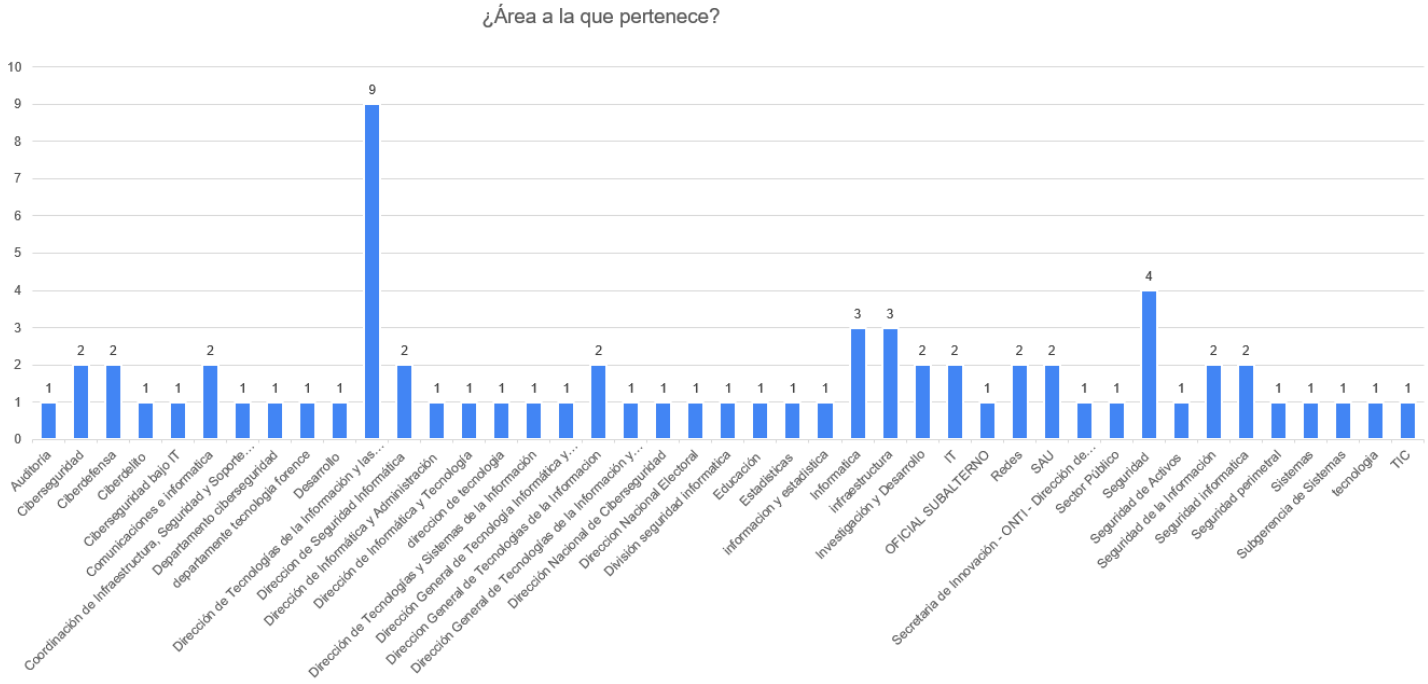


Figura 34 Representación Propia. Respuesta Pregunta 2.

Se obtuvieron 9 respuestas de agentes pertenecientes a la Dirección de Tecnologías de la Información y las Comunicaciones seguida por seguridad que tuvo 4 agentes que respondieron la encuesta, y distribuyendo el resto entre diferentes áreas como informática e infraestructura, pero también se destacan el resto como áreas más específicas entre ellas ciberdelito o ciberdefensa. (Figura 34)

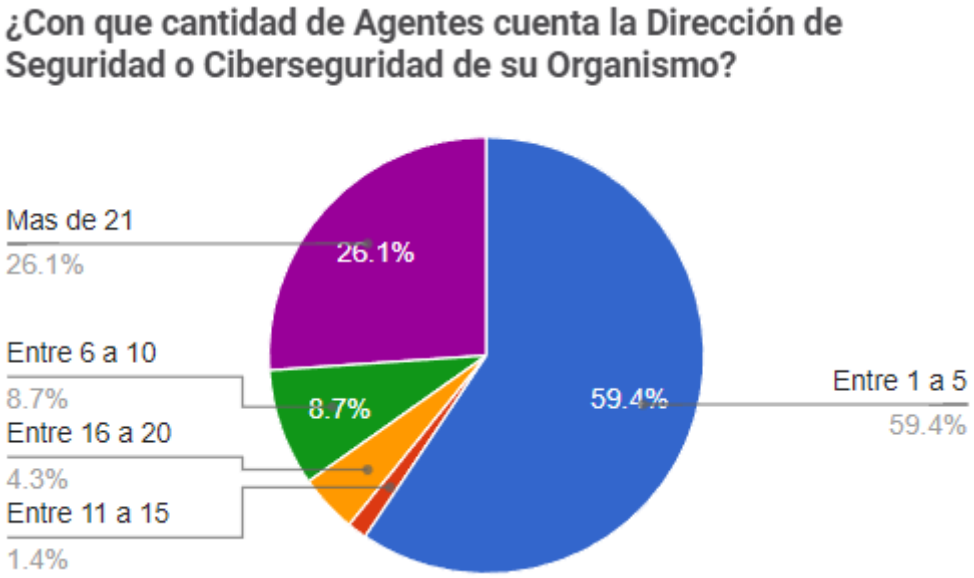


Figura 35 Representación Propia. Respuesta Pregunta 3

La respuesta obtenida a la pregunta no sorprende ya que al ver los resultados se nota la disparidad entre unos Organismos y otros, 41 (59,4%) de entre 69 respuestas cuentan con "entre 1 a 5 agentes", lo que quiere decir que con esa cantidad tiene que desempeñar sus funciones un área de Seguridad de la Información o Ciberseguridad, entre las restantes respuestas, 18 (26,1%) deben desempeñar sus tareas con "más de 21" agentes en sus áreas de Seguridad de la Información o Ciberseguridad, lo que es todo lo contrario y por último de las demás respuestas obtenidas 6 (8,7%) respuestas de ellas cuenta con un área de Seguridad de la Información o Ciberseguridad que tiene "Entre 6 a 10" agentes, 1 (1,4%) respuesta se respondió que cuenta con un área de Seguridad de la Información o Ciberseguridad que tiene "Entre 11 a 15" agentes y por último 3 respuestas (4,3%) "Entre 16 a 20" agentes. (Figura 35)

Sección 3: Programas de Bug Bounty - Política Pública de Programas de Bug Bounty

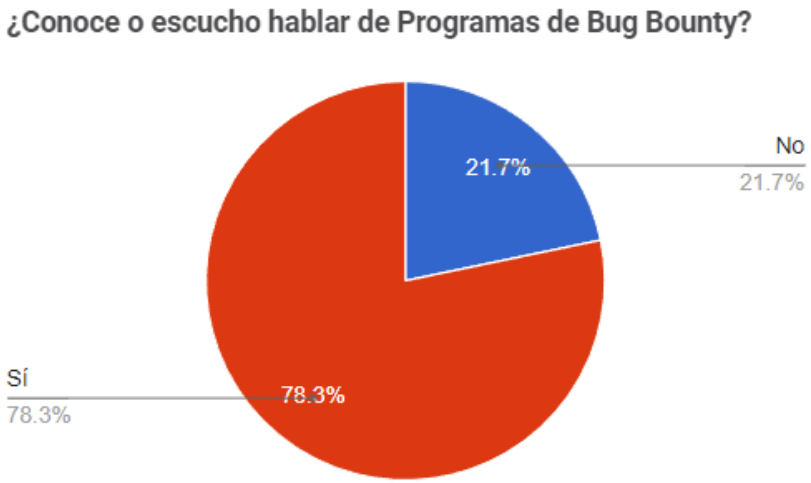


Figura 36 Representación Propia. Respuesta Pregunta 4

Cuando fueron consultados para entender si conocían o habían escuchado hablar del término bug bounty de los 69 encuestados 54 (78,3%) respondieron que sí conocían y 15 (21,7%) que no conocían o habían escuchado hablar del término. (Figura 36)

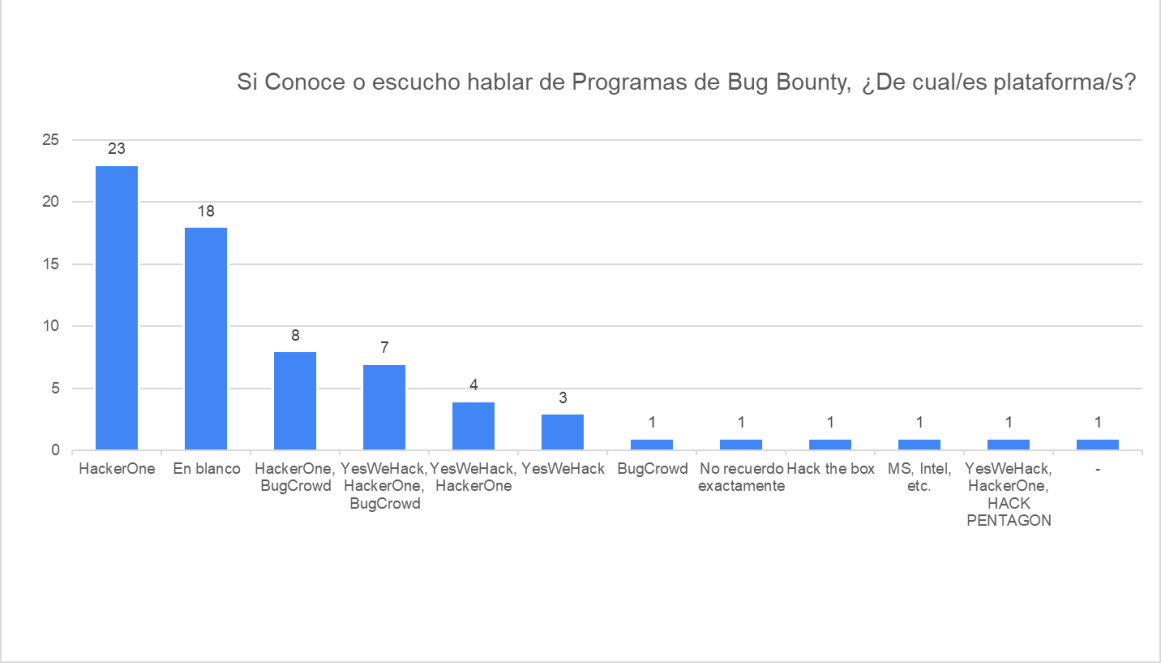


Figura 37 Representación Propia. Respuesta Pregunta 5

A la pregunta de si conocía o si había escuchado hablar sobre plataformas de bug bounty, la misma se generó de forma que no era mandatorio responder (se brindó la opción de poder responder o no, pero la encuesta continuaba igual), se podían seleccionar múltiples opciones y hasta generar sus propias opciones si no aparecía la que necesitaba para poder responder.

La mayoría de los agentes encuestados que respondieron esta pregunta, fueron 51, conocía a HackerOne y BugCrowd principalmente. (Figura 37)

Figura 38 Representación Propia. Respuesta Pregunta 6

A la pregunta de si ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty? de las 69 respuestas, 60 (87%) agentes estuvieron de acuerdo con que SI se debe crear y solo 9 (13%) de los agentes cree que NO. Ello sorprendió al ver la respuesta a la consulta si se conocía o se había escuchado hablar de Programas de Bug Bounty y en las respuestas se había obtenido un 21,7% que no lo habían hecho, pero sin embargo igual estuvieron de acuerdo en que si se debe tener una Política Pública Nacional de Programas de Bug Bounty. (Figura 38)

Sección 4: No crear una Política Pública Nacional de Programas de Bug Bounty

Figura 39 Representación Propia. Respuesta Pregunta 7

La sección 4 en la cual se consulta ¿Por qué piensa usted que el Estado Nacional Argentino NO está preparado para crear una Política Pública Nacional de Programas de Bug Bounty? se obtuvieron 9 (100%) respuestas, porque se respondieron negativamente a la pregunta anterior ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty?, los agentes respondieron que piensan que NO se debe crear una Política Pública Nacional de Programas de Bug Bounty "Porque no cuenta con la madurez necesaria". (Figura 39)

Sección 5: Plataforma de Programas de Bug Bounty propia o de terceros

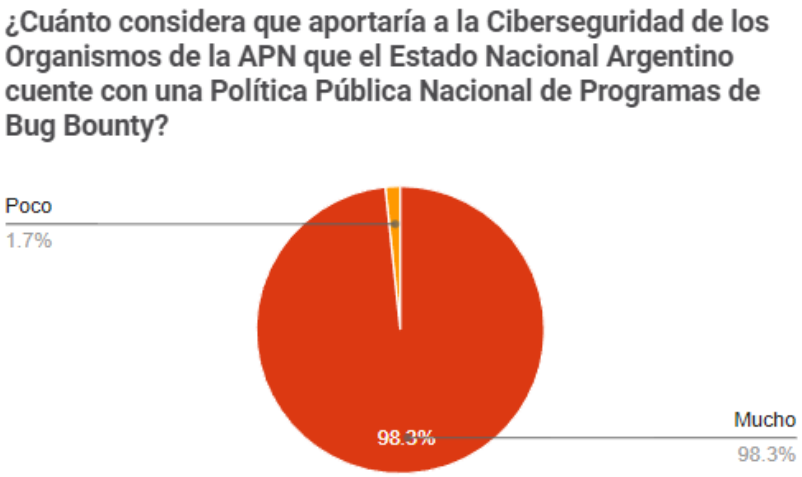


Figura 40 Representación Propia. Respuesta Pregunta 8

A la primera pregunta de la sección 5 ¿Cuánto considera que aportaría a la ciberseguridad de los Organismos de la APN que el Estado Nacional Argentino cuente con una Política Pública Nacional de Programas de Bug Bounty? se obtuvo que 59 (98,3%) de los agentes encuestados consideran que aportaría mucho la creación de una Política Pública de Programas de Bug Bounty, siendo un encuestado (1,7%) el que considera que aportaría poco y quedando los restantes 9 encuestados los que no respondieron esta pregunta ya que respondieron negativamente a la respuesta ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty? de la sección 4 del formulario. (Figura 40)

Figura 41 Representación Propia. Respuesta Pregunta 9

Y a la segunda pregunta de la sección 5 en la cual se desea conocer qué piensan los agentes de la Administración Pública Nacional, a su criterio si el Estado Nacional Argentino crea una Política Pública Nacional de Programas de Bug Bounty ¿Debe desarrollar su propia plataforma o debe generar los programas desde plataformas como YesWeHack, HackerOne, BugCrowd, etc? Se obtuvo que 54 (90 %) de los 60 agentes consideran que el Estado Nacional Argentino debe desarrollar su propia plataforma si se crea una Política Pública Nacional de

Programas de Bug Bounty y solo 6 (10%) que no les importaría perder la soberanía de la información realizando los programas a través de una plataforma de terceros. (Figura 41)

Sección 6: Infraestructura Crítica

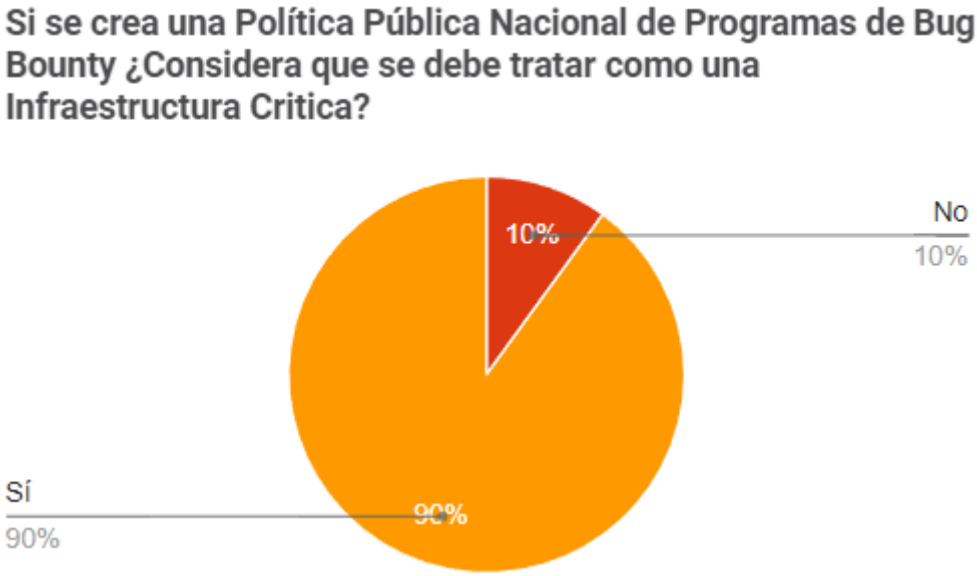


Figura 42 Representación Propia. Respuesta Pregunta 10

En la primera pregunta de la sección 6 interesa conocer si los agentes encuestados consideran que la plataforma que se desarrolle de Programas de Bug Bounty debe considerarse como una infraestructura crítica del país, donde, de los 60 agentes 55 respondieron que sí (90%) y 5 agentes (10%) no lo considera necesario. (Figura 42)

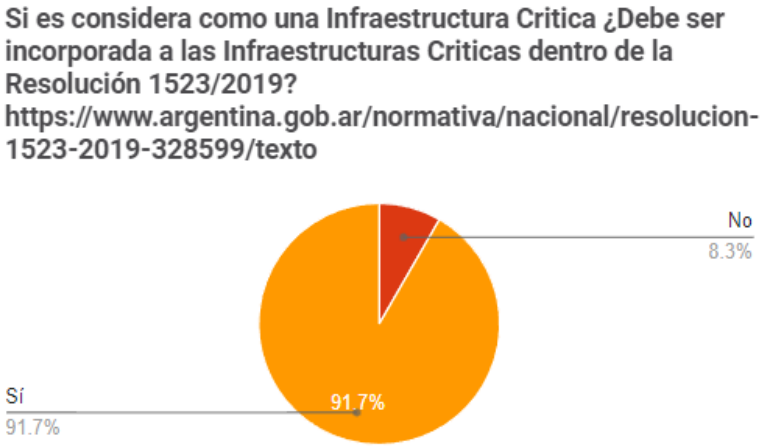


Figura 43 Representación Propia. Respuesta Pregunta 11

La segunda pregunta que se les realizó en esta sección 6 a los agentes encuestados pretende dar a conocer si ellos piensan que si es considerada una infraestructura crítica la plataforma desarrollada por el Estado Nacional Argentino de Programas de Bug Bounty debería ser agregada al catálogo de infraestructuras críticas del país y de los 60 agentes que respondieron, 55 (91,7%) de ellos respondieron que sí y sólo 5 (8,3%) agentes no lo considera necesario. (Figura 43)

Sección 7: Recompensas

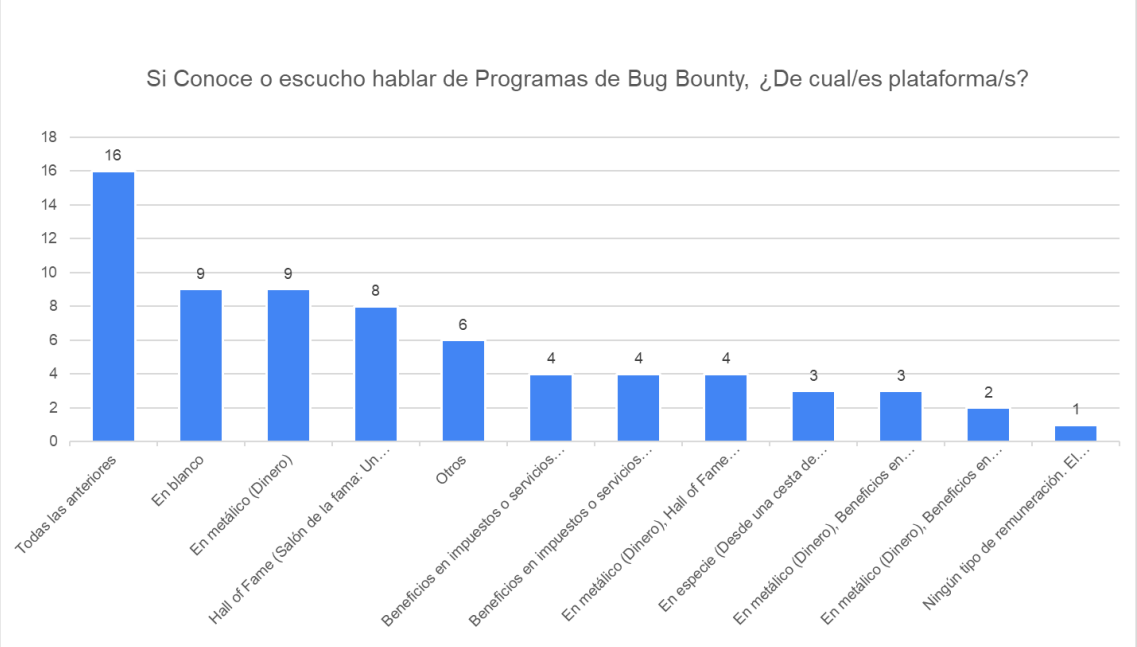


Figura 44 Representación Propia. Respuesta Pregunta 12

En la última pregunta se les consultó a los agentes cuál consideraban que era la mejor recompensa que deben entregar los Programas de Bug Bounty del Estado Nacional Argentino.

De lo cual en esta respuesta los encuestados podían elegir múltiples opciones simultáneas, de ellas la que mayor cantidad de respuestas obtuvo fue “Todas las anteriores” con 16 (23,2%), la segunda fue “En metálico (Dinero)” con 9 (13%) respuestas y la tercera opción con 8 (11,6%) respuestas fue “Hall of Fame (Salón de la fama: Un reconocimiento por su aporte al Estado Nacional Argentino)”, también 9 (13%) de los agentes al responder que no se debería crear una política pública de bug bounty no recibieron la pregunta. (Figura 44)

Por último, sobre las preguntas:

- ¿Conoce o escucho hablar de Programas de Bug Bounty?
- A su criterio ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty?
- ¿Cuánto considera que aportaría a la ciberseguridad de los Organismos de la APN que el Estado Nacional Argentino cuente con una Política Pública Nacional de Programas de Bug Bounty?
- A su criterio si el Estado Nacional Argentino crea una Política Pública Nacional de Programas de Bug Bounty ¿Debe desarrollar su propia plataforma o debe generar los programas desde plataformas como YesWeHack, HackerOne, BugCrowd, etc?
- Si se crea una Política Pública Nacional de Programas de Bug Bounty ¿Considera que se debe tratar como una Infraestructura Crítica?
- Si es considerada como una Infraestructura Crítica ¿Debe ser incorporada a las Infraestructuras Críticas dentro de la Resolución 1523/2019? https://www.argentina.gob.ar/normativa/nacional/resolucion-1523-2019-328599/texto

Se utilizó una escala de Likert, para determinar la conformidad de los encuestados con el tema planteado, la escala de Likert es un método de investigación que utiliza una escala de calificación para conocer el nivel de acuerdo y desacuerdo de las personas sobre un tema.

Creada en 1932 por el psicólogo americano Rensis Likert, la escala pretende no limitar las respuestas a “sí” o “no”. Así, en la escala Likert, el encuestado califica sus respuestas al “estar de acuerdo o no” con la situación. Por lo tanto, lo que esta escala determina es la conformidad de las personas y resulta útil cuando necesitas una opinión detallada sobre un tema en particular. La encuesta de Likert ofrece un resultado cualitativo, a pesar de fundarse en respuestas cuantitativas.

Para el estudio se obtuvieron las frecuencias numéricas, así como las frecuencias porcentuales que se pueden consultar en el Anexo I. La escala de Likert utilizada fue:

1) De acuerdo
2) Neutrales
3) En desacuerdo

Donde 1 corresponden a valores positivos, el número 2 corresponde a los agentes que no supieron polarizarse y se mantienen neutrales, y el número 3 son en consecuencia negativos.

También se debe comentar cómo fueron tabuladas cada una de las variables

Variable P1 = Pregunta 1 ¿A qué Organismo de la APN pertenece?

Abierta

Variable P2 = Pregunta 2 ¿Área a la que pertenece?

Abierta

Variable P3 = Pregunta 3 ¿Con qué cantidad de Agentes cuenta la Dirección de Seguridad o Ciberseguridad de su Organismo?

1 - Entre 1 a 5

2 - Entre 6 a 10

3 - Entre 11 a 15

4 - Entre 16 a 20

5 - Más de 21

Variable P4 = Pregunta 4 ¿Conoce o escuchó hablar de Programas de Bug Bounty?

1 - No

2 - Si

Variable P5 = Pregunta 5 Si Conoce o escuchó hablar de Programas de Bug Bounty, ¿De cual/es plataforma/s?

Multiple Choice - Abierta

Variable P6 = Pregunta 6 su criterio ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty?

1 - No

2 - Si

Variable P7 = Pregunta 7 ¿Por qué piensa usted que el Estado Nacional Argentino NO está preparado para crear una Política Pública Nacional de programas de Bug Bounty?

Pregunta que no se toma en cuenta ya que en la P6 se responde por sí o se debe crear una política pública de Bug Bounty, en esta pregunta sólo se justifica el por qué no.

Variable P8 = Pregunta 8 ¿Cuánto considera que aportaría a la ciberseguridad de los Organismos de la APN que el Estado Nacional Argentino cuente con una Política Pública Nacional de Programas de Bug Bounty?

0 - 0

1 - No aportaría nada

2 - Poco

3 - Mucho

Variable P9 = Pregunta 9 A su criterio si el Estado Nacional Argentino crea una Política Pública Nacional de Programas de Bug Bounty ¿Debe desarrollar su propia plataforma o debe generar los programas desde plataformas como YesWeHack, HackerOne, BugCrowd, etc?

0 - 0

1 - Podría utilizar una plataforma de terceros (aunque los datos perderían Soberanía Nacional)

2 - Debe desarrollar su propia plataforma

Variable P10 = Pregunta 10 Si se crea una Política Pública Nacional de Programas de Bug Bounty ¿Considera que se debe tratar como una Infraestructura Crítica?

0 - 0

1 - No

2 - Si

Variable P11 = Pregunta 11 Si es considerada como una Infraestructura Crítica ¿Debe ser incorporada a las Infraestructuras Críticas dentro de la Resolución 1523/2019? https://www.argentina.gob.ar/normativa/nacional/resolucion-1523-2019-328599/texto

0 - 0

1 - No

2 - Si

Variable P12 = Pregunta 12 Con respecto a las recompensas que deben otorgar los Programas de Bug Bounty del Estado Nacional Argentino, ¿Considera que deben ser premios en metálico, en especie o un reconocimiento al aporte hacia el Estado?

Multiple Choice - Abierta

Con lo cual el valor máximo que se puede conseguir de las variables analizadas es

P4 + P6 + P8 + P9 + P10 + P11 = 2 + 2 + 3 + 2 + 2 + 2 = 13

Y el valor mínimo que se puede conseguir de las variables analizadas es

P4 + P6 + P8 + P9 + P10 + P11 = 1 + 1 + 0 + 0 + 0 + 0 = 2

Por lo tanto, ahora se puede sacar el baremo que va a tener el rango entre el valor mínimo 2 y el valor máximo 13.

$13 - 2 = 11$ $11 / 3 = 3{,}66$

Como se comentó se va a tener una escala 1) De acuerdo 2) Neutrales 3) En desacuerdo que se corresponde con los siguientes rangos.

2 – 5,66 En desacuerdo

5,67 – 9,33 Neutrales

9,34 - 13 De acuerdo

Total (Agrupada)

	N	%
En desacuerdo	9	13,0%
Neutrales	1	1,4%
De acuerdo	59	85,5%

Tabla 3 Representación Propia. Total (Agrupada) de los valores de acuerdo

Y se obtiene la siguiente representación gráfica

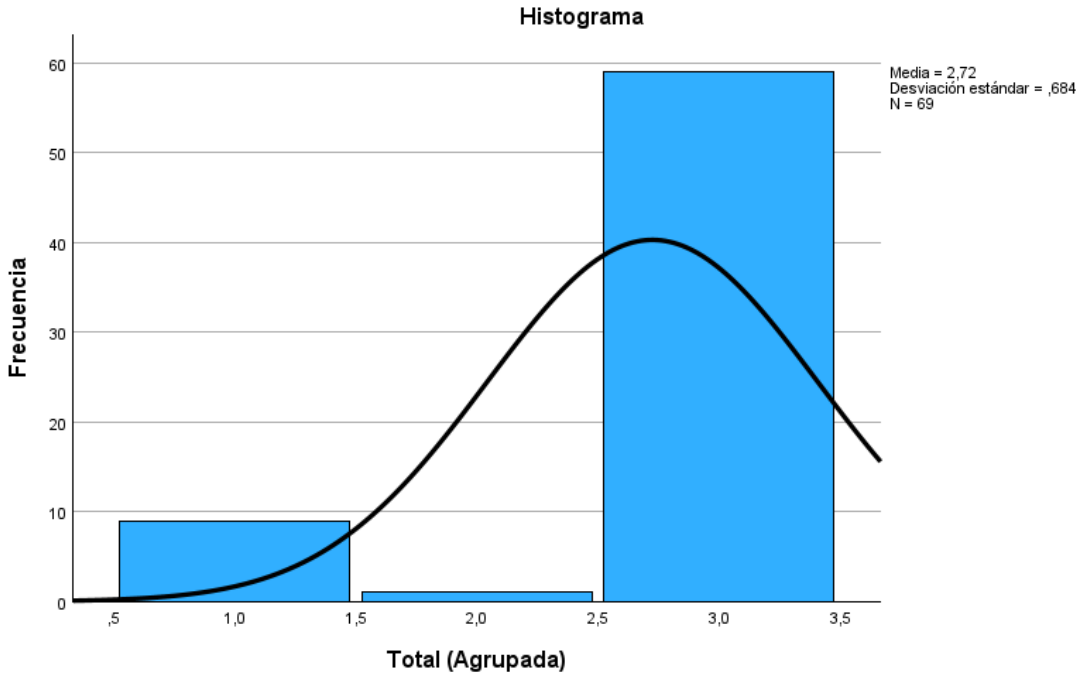


Figura 45 Representación Propia. Histograma Total (Agrupada) Nivel de Aceptación

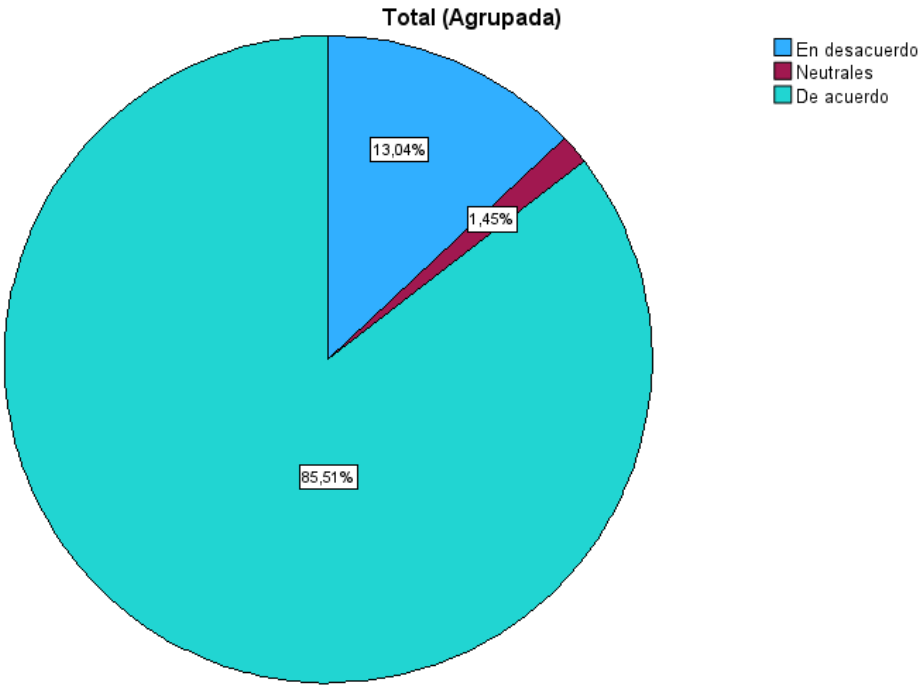


Figura 46 Representación Propia. Gráfico Circular Total (Agrupada) Nivel de Aceptación

Conclusiones del capítulo

Como conclusiones a las respuestas obtenidas en la encuesta realizada a los agentes que desempeñan funciones en la Administración Pública Nacional, los siguientes datos son muy reveladores para la hipótesis planteada en la obra.

- Se puede observar que los agentes de los Organismos de la Administración Pública Nacional participaron desde diferentes Organismos y Áreas, lo que permitió realizar el análisis de los datos sin sesgos de Organismos particulares.
- Con respecto a las Áreas a las cuales pertenecen los agentes también se consiguió que fueran diferentes, entre ellas las de Seguridad de la Información, Ciberseguridad, Infraestructura, Comunicaciones y hasta de la Dirección de Estándares Tecnológicos.
- Se pudo conocer que la mayoría de los Organismos cuenta con pocos Agentes (Entre 1 a 5) en sus áreas de Seguridad Informática, Seguridad de la Información o Ciberseguridad.
- En la sección 3 se pudo conocer que los encuestados en su gran mayoría (78,3%) conoce que es bug bounty, además que las páginas más conocidas por ellos son HackerOne y BugCrowd que es pertinente ya que son las que cuentan con mayor número de programas de bug bounty al día de la escritura de la obra, por último y más importante que se buscaba en esta sección era conocer si los encuestados piensan que el Estado Nacional Argentino debe crear una Política Pública de Programas de Bug Bounty a lo que su respuesta fue casi unánime que sí, ello está alineado con lo que plantea el maestrando en su hipótesis.
- La sección 4 solo pretendía obtener información del porque el encuestado piensa que no se debe crear una Política Pública Nacional de Programas de Bug Bounty y se obtuvo que solamente 9 respuestas a esa pregunta y habilitando a ese encuestado a responder la pregunta de esta sección, la misma resulta de utilidad para entender que piensa que el Estado no cuenta con la madurez necesaria para llevar adelante el proyecto de creación de este tipo de políticas públicas.
- Las preguntas que se realizaron en la sección 5 para conocer si los encuestados estaban de acuerdo con que el estado desarrolle su propia plataforma de

Programas de Bug Bounty, la cual fue respondida por la mayoría con un sí, lo cual atiende al resguardo de la soberanía nacional de los datos.

- Con respecto a las preguntas que se realizaron en la sección 6 para conocer si los encuestados estaban de acuerdo con que el estado desarrolle su propia plataforma de Programas de Bug Bounty considerándola una infraestructura crítica del país y deba ser sumada al catálogo de infraestructuras críticas casi por unanimidad respondieron que sí, resguardando la soberanía nacional sobre los datos del Estado y en caso de ser atacada responder ante las leyes vigentes creadas para la defensa de las Infraestructuras Críticas del País.
- La pregunta que se realizó en la sección 7, obtuvo una respuesta que conlleva un desembolsó de dinero por parte del estado, pero también varios de los encuestados estarían de acuerdo que la mejor recompensa para los Programas de Bug Bounty que puede poner en funcionamiento el Estado Nacional Argentino sea el Hall of Fame (Salón de la Fama en español) como reconocimiento por el aporte realizado al Estado.
- También aplicando una escala de Likert de tres niveles, se llegó a demostrar que la mayor cantidad de los encuestados están en un nivel de acuerdo de un 85,51% sobre un nivel de desacuerdo del 13%.

“La tarea del hacker no es destruir, sino utilizar sus conocimientos en favor de la libertad y la igualdad social."

Johan Manuel Méndez

Conclusiones

Las siguientes son las conclusiones obtenidas del aporte teórico que se realizó en la presente tesis de final de magíster.

Como primera conclusión se puede apreciar gracias a la investigación que la hipótesis planteada como objetivo general de la tesis pudo ser respondida de forma satisfactoria en base a lo que pensaba el maestrando y los datos obtenidos en la encuesta que fue respondida por los agentes de varios Organismos del Estado Nacional Argentino.

Sobre la primera parte de la hipótesis planteada ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de programas de bug bounty?

La respuesta fue claramente que ¡Sí!, esto en base a los antecedentes que se pudieron presentar a través de todo el Capítulo II: Historia de los Bugs y Bugs Bounty y con el respaldo de las respuestas obtenidas en Capítulo 3 Encuesta, en el que se realizó el análisis de las respuestas obtenidas y se alineaban al pensamiento del maestrando.

Sobre la segunda parte de la hipótesis que plantea si el Estado Nacional Argentino ¿Debe contar con su propia plataforma de programas de bug bounty o puede utilizar una plataforma de terceros? se llegó a la conclusión por parte del maestrando que, aunque muchos países como los casos de Estados Unidos de Norte América, Francia, Singapur o Israel por citar solo algunos que sus programas de bug bounty los realizan a través de la página HackerOne, sería muy beneficioso para el Estado Nacional Argentino comenzar a desarrollar sus primeros programas de bug en una plataforma como HackerOne o BugCrowd, para tomarlo como un aprendizaje y poder obtener estadísticas como fue el caso de Hack The Pentagon, mientras en paralelo se realiza la planificación, desarrollo, implementación y puesta en marcha de su propia plataforma de programas de bug bounty a la cual luego migrar y que la misma pueda ser declarada e incorporada al catálogo de las infraestructuras críticas del país como fue el caso de la plataforma de Gestión Documental Electrónica (GDE).

Así también en el trabajo final de maestría se pudo brindar como aporte los primeros lineamientos de una metodología de programas de bug bounty para que el Estado Nacional

Argentino los pueda incorporar a la creación de la primera Política Pública Nacional de Programas de Bug Bounty como una ventaja estratégica que otorga mayor resiliencia al Estado Nacional Argentino.

Como conclusión final tomando lo investigado y redactado se espera que el Estado Nacional Argentino pueda tener en cuenta la tesis final de maestría escrita por él maestrando y en base a la misma analizar el colocar el tema en la agenda de las políticas públicas del Estado, la creación de una Política Pública Nacional de Programas de Bug Bounty sería muy beneficioso no solo para el Estado sino también para todos los ciudadanos que en definitiva son los verdaderos afectados con la perdida de sus datos por parte del Estado, esto sería una excelente iniciativa para la soberanía nacional en los años en que la información es la moneda de cambio de todos los países, ya lo vemos con el avance del análisis de big data, ello hará que el Estado Nacional Argentino comience a ser más proactivo en la toma de decisiones y no ocurra como con la Disposición 8/2021 " Ciberseguridad: crearon una guía de buenas prácticas para el desarrollo de aplicaciones web" publicada en el Boletín Oficial de la República Argentina (JEFATURA DE GABINETE DE MINISTROS, Boletin Oficial de la Republica Argentina, 2021), lo cual aconteció luego de que sucedieran los eventos de ciberataques a los sitios oficiales de IOSFA, PFA, Ministerio de Seguridad de la Nación, entre otros, como se desarrolló en el apartado "2.8 Principales Ciberataques a Organismos Gubernamentales de Argentina" del Capítulo II: Historia de los Bugs y Bugs Bounty.

Aportes propuestos

En este capítulo se presentan los aportes propuestos por el maestrando, las respuestas a la hipótesis planteada serán tomadas como el desencadenante de las ideas que darán desarrollo al sustento del aporte innovador.

De la información obtenida en el apartado "2.5 Los Bug Bounty Programs de Empresas Privadas" del Capítulo II: Historia de los Bugs y Bugs Bounty, donde se recorrió la historia en la cual se pudo observar que los programas de bug bounty nacieron en el año 1995 con la compañía Netscape, o sea hace 26 años atrás se acuñaba el término bug bounty, todos ellos de empresas privadas y que algunas hasta continúan utilizando esta práctica en la actualidad para

mejorar la seguridad de sus infraestructuras y de su información, lo cual no es un dato menor, estos programas fueron evolucionando en las metodologías utilizadas a través de los años.

También cabe aclarar que tras la investigación que se realizó y se expuso en el Capítulo II: Historia de los Bugs y Bugs Bounty no se encontró antecedentes de Políticas Públicas Nacionales de Programas de Bug Bounty que se hayan propuesto por parte de la Subsecretaría de Ciberdefensa del Ministerio de Defensa de la Nación ni de la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública, pero si se tomaran los casos aportados en el apartado "2.6 Los Bug Bounty Programs Gubernamentales" en el cual se realizó un recorrido a través de los casos de creación de Políticas Nacionales de Programas de Bug Bounty en países como EE.UU., Holanda, Finlandia y Singapur, solo por citar algunos de ellos.

También es relevante el sustentar este capítulo con los resultados y las conclusiones aportadas en los apartados "3.2 Análisis de los datos" y "Conclusiones del capítulo" del Capítulo III: Encuesta en el cual se obtuvieron resultados positivos a favor de la hipótesis planteada por el maestrando tanto a favor de que el Estado Nacional Argentino debe Crear una Política Pública Nacional de Programas de Bug Bounty, como así también que sería muy propicio que se genere un proyecto para el desarrollo de su propia Plataforma de Programas de Bug Bounty y adicionalmente que se declare a la misma como una infraestructura crítica de la República Argentina.

En el caso del aporte que se quiere realizar desde esta obra se considera por el maestrando que la Política Pública Nacional de programas de Bug Bounty que se debe crear para el Estado Nacional Argentino debe seguir los lineamientos que se proponen en forma teórica a continuación.

Quizás sería recomendable para el Estado Nacional Argentino el comenzar con un programa de divulgación de vulnerabilidades (del inglés vulnerability disclosure program, VDP) para luego ir gradualmente creando la Política Pública Nacional de Programas de Bug Bounty, lo más complejo, ya que se tiene que tener en cuenta las recompensas que se van a brindar, si se va a utilizar programas privados en un principio (sería lo recomendable) y luego pasar a crear programas públicos en los casos que sea pertinente.

Según la investigadora Katie Moussouris[10] fundadora y CEO de Luta Security en su presentación Bug Bounties & VDPs Lessons Learned From Industry NIST muestra que se

[10] https://www.youtube.com/watch?v=hvLorE8sjcc Consultado el 08/12/2021

debería comenzar implementando, siguiendo los estándares ISO 29147 & 30111 sobre Vulnerability Disclosure y Vulnerability Handling Processes respectivamente. Se puede ver un gráfico donde se describen los estándares ISO 29147 & 30111 en la Figura 47.

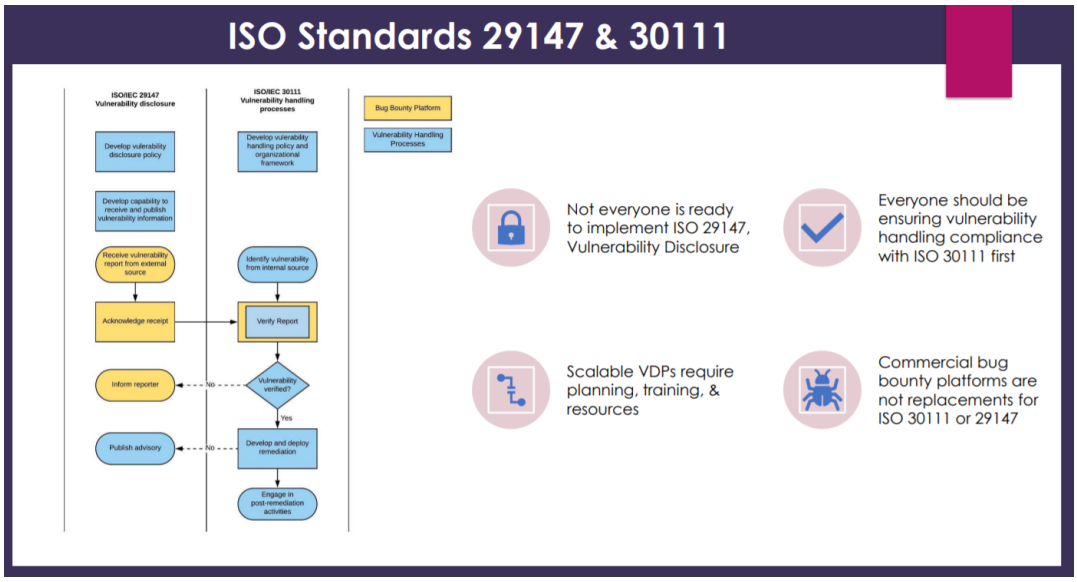


Figura 47 ISO Standards 29147 & 30111

Fuente *(Moussouris, 2020)*

Katie Moussouris también recomienda el tiempo mínimo que se debe desarrollar el Vulnerability Disclosure Program (VDP) como dos años para luego, con el estado de madurez adquirido pasar a un programa de Bug Bounty Program. Se puede apreciar un gráfico donde se describe el tiempo mínimo recomendado para un VDP y sus fases en la Figura 48.

Figura 48 Tiempo mínimo recomendado para un VDP

Fuente *(Moussouris, 2020)*

Según se presenta en la página oficial de HackerOne se proponen cinco componentes claves y su detalle que deben tener los VDP: “

- Declaración de propósitos/promesas: La declaración de apertura de un PDV debe incluir las razones por las que tiene un PDV y por qué es importante tenerlo.

  Esto es para demostrar su compromiso con los clientes y otras partes interesadas que están potencialmente afectadas por sus vulnerabilidades de seguridad.
- Alcance: Indica qué propiedades, productos y tipos de vulnerabilidad están disponibles para encontrar vulnerabilidades. Esto ayuda a los buscadores en lo que respecta a los activos en los que deben o no centrar su atención.
- Resguardo seguro: Una declaración que asegura a los buscadores que no serán penalizados ni se emprenderán acciones legales contra ellos por las vulnerabilidades que encuentren.
- Descripción del proceso: Una descripción del proceso de cómo los buscadores deben presentar informes y qué información se requiere en una presentación.
  Cómo se evaluarán los informes

  Un esquema descriptivo que establezca las expectativas sobre cómo se evaluarán los informes.

  Puede incluir:
- El tiempo que se espera que los buscadores esperen entre el envío y la primera respuesta.
- Cómo variarán los tiempos de respuesta en función de la gravedad y del activo afectado.
- Cuando los descubridores pueden revelar públicamente sus vulnerabilidades encontradas.
- Si los descubridores pueden esperar un correo electrónico de confirmación o no.”

Para la Política Pública Nacional de Programas de Bug Bounty se podrían definir los siguientes componentes claves que se detallan a continuación.

- Los reportes de hallazgos de errores deberán ser enviados a través de la plataforma en un formato predefinido.
- Los reportes deberán contener las correspondientes PoC que puedan ser replicables por el equipo de seguridad responsable de validar los errores reportados.
- Se deberá utilizar un framework como el del NIST (National Institute of Standards and Technology) llamado CVSS (Common Vulnerability Scoring System Calculator) para el cálculo de la ponderación para las vulnerabilidades reportadas.
- Se deberá fijar un alcance de los sitios que serán los únicos habilitados como objetivos válidos para la búsqueda de vulnerabilidades.
- Se deberá fijar las recompensas basadas en las ponderaciones de las vulnerabilidades reportadas.
- Se deberán establecer las reglas (Bases y Condiciones) por escrito, en las cuales se brindarán los lineamientos y penalidades en caso de incumplimientos.

Con respecto a la plataforma, la misma debe ser centralizada pudiendo ser el dueño la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública, en la cual se puedan concentrar los programas generados por cada uno de los Organismos de la Administración Pública Nacional, pero delegando en administradores locales para cada Organismo que lo solicite y se vaya sumando en la generación de los programas de bug bounty.

Esta propuesta de aporte planteada por el maestrando como un aporte para la ciberseguridad y la resiliencia de los servicios del Estado Nacional Argentino también se encuentra totalmente alineada a la "**SEGUNDA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA**" que fue publicada el día 1 de septiembre de 2023 en el BORA[11] bajo la resolución 44/2023 (RESOL-2023-44-APN-SIP#JGM) como se puede apreciar en la Figuras 49 y la Figura 50.

[11] BORA: Boletín Oficial de la República Argentina (https://www.boletinoficial.gov.ar) es el diario oficial de la República Argentina, es decir, el medio de comunicación escrito que el Estado argentino utiliza para publicar sus normas jurídicas (tales como leyes, decretos y reglamentos) y otros actos de naturaleza pública, tanto del poder legislativo como del ejecutivo y el judicial. (Wikipedia, 2023) Consultado el 10/09/2023

Figura 49 Anuncio de la aprobación de la Segunda Estrategia Nacional de Ciberseguridad en el sitioArgentina.gob.ar

Fuente *(Argentina.gob.ar, 2023)*

Esta estrategia busca jerarquizar la importancia de que los Estados incorporen la problemática de la ciberseguridad a la agenda gubernamental y otorgar un contexto seguro para que los avances tecnológicos y de innovación puedan ser aprovechados por todos los actores de la sociedad. (Argentina.gob.ar, 2023)

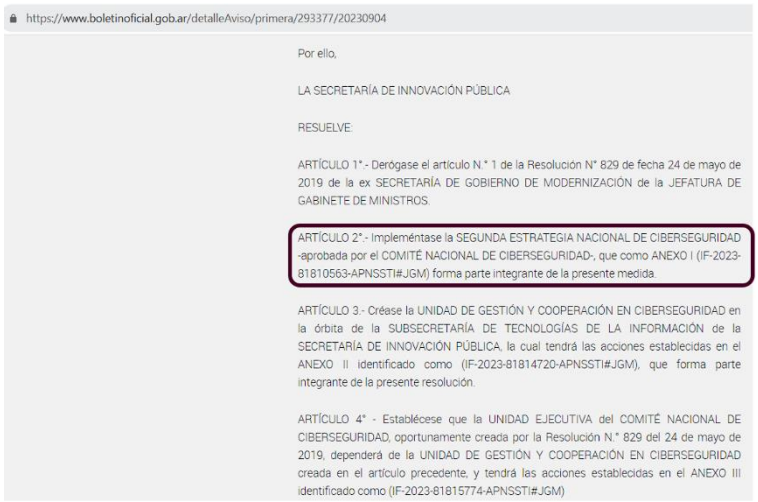


Figura 50 Segunda Estrategia Nacional de Ciberseguridad y ANEXO I

Fuente *(Técnica, 2023)*

Y también busca que

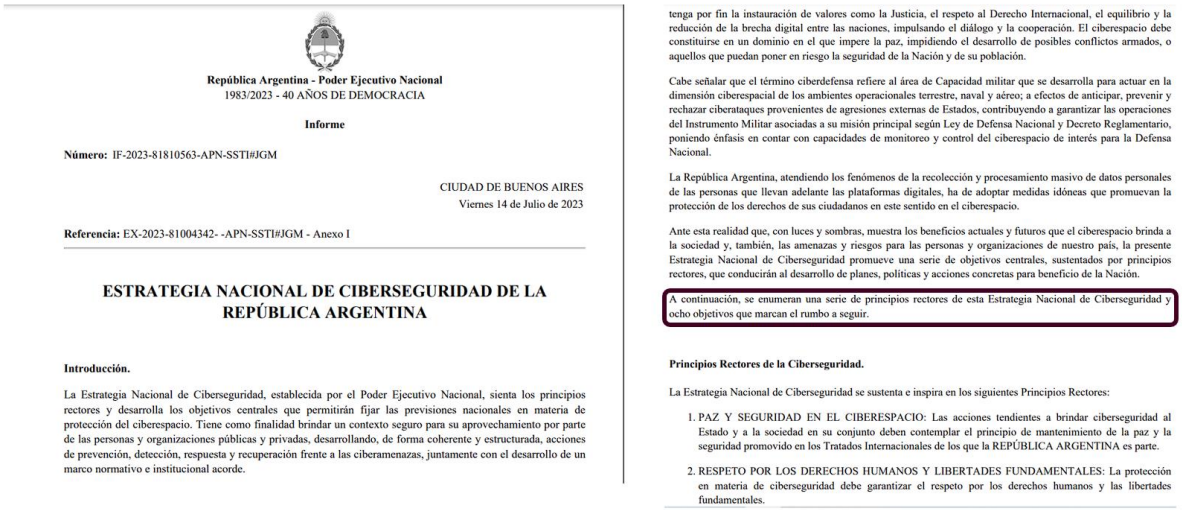
> En el marco de dar cumplimiento a los objetivos de la Segunda Estrategia Nacional de Ciberseguridad se convocarán a las distintas empresas, universidades y actores del ecosistema de ciberseguridad para impulsar compromisos y actividades con el objetivo de dar cumplimiento a los 8 principios rectores, los 8 objetivos concretos y las 42 acciones. (Argentina.gob.ar, 2023)

Dentro de la definición de sus: "Objetivos la Estrategia Nacional de Ciberseguridad." indica en su Objetivo tres lo siguiente:

> Objetivo 3. Protección y recuperación de los sistemas de información del Sector Público.
>
> Adoptar las medidas necesarias para que los sistemas de información que utiliza el Sector Público, incluyendo todos sus poderes y organismos, posean un adecuado nivel de seguridad y recuperación.
>
> Para ello será necesario:
>
> Diseñar e implementar las políticas públicas basadas en mejores prácticas internacionales necesarias para fortalecer la seguridad y resiliencia de los sistemas de información del Sector Público, incluyendo los mecanismos de control para la aplicación de las Políticas de Seguridad de la Información.

Como se ve en la Figura 51 y Figura 52

Anexo I



República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Informe

Número: IF-2023-81810563-APN-SSTI#JGM

CIUDAD DE BUENOS AIRES
Viernes 14 de Julio de 2023

Referencia: EX-2023-81004342- -APN-SSTI#JGM - Anexo I

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DE LA REPÚBLICA ARGENTINA

Introducción.

La Estrategia Nacional de Ciberseguridad, establecida por el Poder Ejecutivo Nacional, sienta los principios rectores y desarrolla los objetivos centrales que permitirán fijar las previsiones nacionales en materia de protección del ciberespacio. Tiene como finalidad brindar un contexto seguro para su aprovechamiento por parte de las personas y organizaciones públicas y privadas, desarrollando, de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, juntamente con el desarrollo de un marco normativo e institucional acorde.

tenga por fin la instauración de valores como la Justicia, el respeto al Derecho Internacional, el equilibrio y la reducción de la brecha digital entre las naciones, impulsando el diálogo y la cooperación. El ciberespacio debe constituirse en un dominio en el que impere la paz, impidiendo el desarrollo de posibles conflictos armados, o aquellos que puedan poner en riesgo la seguridad de la Nación y de su población.

Cabe señalar que el término ciberdefensa refiere al área de Capacidad militar que se desarrolla para actuar en la dimensión ciberespacial de los ambientes operacionales terrestre, naval y aéreo; a efectos de anticipar, prevenir y rechazar ciberataques provenientes de agresiones externas de Estados, contribuyendo a garantizar las operaciones del Instrumento Militar asociadas a su misión principal según Ley de Defensa Nacional y Decreto Reglamentario, poniendo énfasis en contar con capacidades de monitoreo y control del ciberespacio de interés para la Defensa Nacional.

La República Argentina, atendiendo los fenómenos de la recolección y procesamiento masivo de datos personales de las personas que llevan adelante las plataformas digitales, ha de adoptar medidas idóneas que promuevan la protección de los derechos de sus ciudadanos en este sentido en el ciberespacio.

Ante esta realidad que, con luces y sombras, muestra los beneficios actuales y futuros que el ciberespacio brinda a la sociedad y, también, las amenazas y riesgos para las personas y organizaciones de nuestro país, la presente Estrategia Nacional de Ciberseguridad promueve una serie de objetivos centrales, sustentados por principios rectores, que conducirán al desarrollo de planes, políticas y acciones concretas para beneficio de la Nación.

A continuación, se enumeran una serie de principios rectores de esta Estrategia Nacional de Ciberseguridad y ocho objetivos que marcan el rumbo a seguir.

Principios Rectores de la Ciberseguridad.

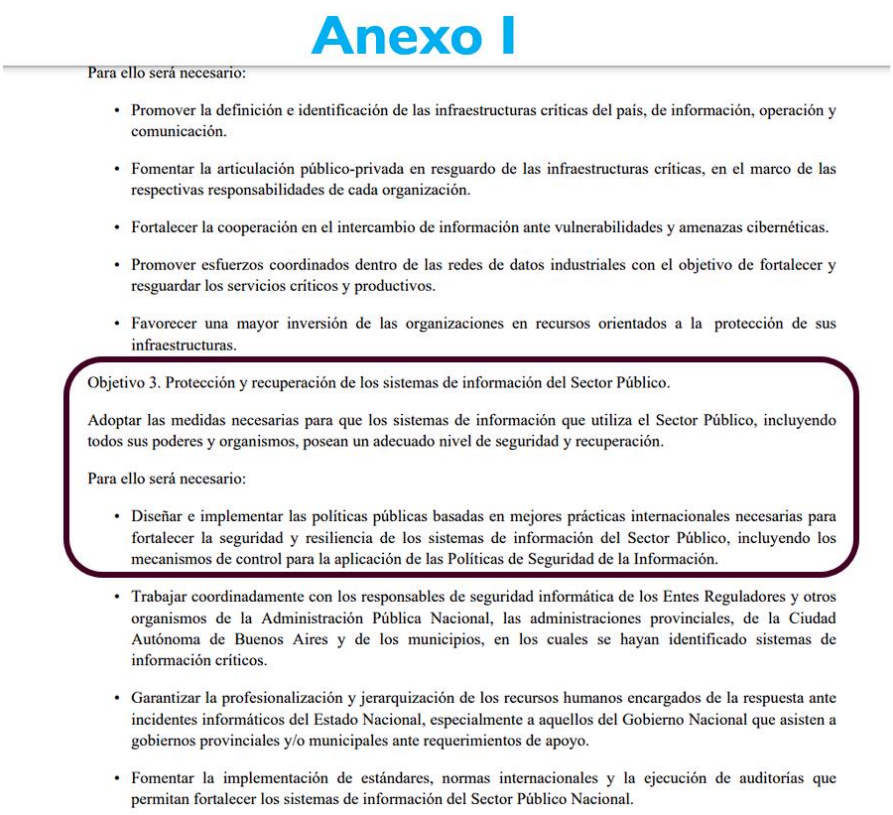
La Estrategia Nacional de Ciberseguridad se sustenta e inspira en los siguientes Principios Rectores:

1. PAZ Y SEGURIDAD EN EL CIBERESPACIO: Las acciones tendientes a brindar ciberseguridad al Estado y a la sociedad en su conjunto deben contemplar el principio de mantenimiento de la paz y la seguridad promovido en los Tratados Internacionales de los que la REPÚBLICA ARGENTINA es parte.
2. RESPETO POR LOS DERECHOS HUMANOS Y LIBERTADES FUNDAMENTALES: La protección en materia de ciberseguridad debe garantizar el respeto por los derechos humanos y las libertades fundamentales.

Figura 51 ANEXO I principios rectores y objetivos de la Segunda Estrategia Nacional de Ciberseguridad

Fuente *(Técnica, 2023)*

Anexo I



Para ello será necesario:

- Promover la definición e identificación de las infraestructuras críticas del país, de información, operación y comunicación.
- Fomentar la articulación público-privada en resguardo de las infraestructuras críticas, en el marco de las respectivas responsabilidades de cada organización.
- Fortalecer la cooperación en el intercambio de información ante vulnerabilidades y amenazas cibernéticas.
- Promover esfuerzos coordinados dentro de las redes de datos industriales con el objetivo de fortalecer y resguardar los servicios críticos y productivos.
- Favorecer una mayor inversión de las organizaciones en recursos orientados a la protección de sus infraestructuras.

Objetivo 3. Protección y recuperación de los sistemas de información del Sector Público.

Adoptar las medidas necesarias para que los sistemas de información que utiliza el Sector Público, incluyendo todos sus poderes y organismos, posean un adecuado nivel de seguridad y recuperación.

Para ello será necesario:

- Diseñar e implementar las políticas públicas basadas en mejores prácticas internacionales necesarias para fortalecer la seguridad y resiliencia de los sistemas de información del Sector Público, incluyendo los mecanismos de control para la aplicación de las Políticas de Seguridad de la Información.
- Trabajar coordinadamente con los responsables de seguridad informática de los Entes Reguladores y otros organismos de la Administración Pública Nacional, las administraciones provinciales, de la Ciudad Autónoma de Buenos Aires y de los municipios, en los cuales se hayan identificado sistemas de información críticos.
- Garantizar la profesionalización y jerarquización de los recursos humanos encargados de la respuesta ante incidentes informáticos del Estado Nacional, especialmente a aquellos del Gobierno Nacional que asisten a gobiernos provinciales y/o municipales ante requerimientos de apoyo.
- Fomentar la implementación de estándares, normas internacionales y la ejecución de auditorías que permitan fortalecer los sistemas de información del Sector Público Nacional.

Figura 52 ANEXO I Objetivo 3 de la Segunda Estrategia Nacional de Ciberseguridad

Fuente *(Técnica, 2023)*

Por lo tanto, está diciendo que la propuesta de poner en la agenda de las políticas públicas del Estado Nacional Argentino una Política Pública de programa de Bug Bounty tomando como referencia los programas como Hack the Pentagon impulsado por el Departamento de Defensa de los EE. UU. (DoD) y los estándares de referencias como la Norma ISO/IEC 29147: Divulgación de vulnerabilidad y la Norma ISO/IEC 30111: Los procesos de manejo de vulnerabilidad.

Trabajo Futuro

Como trabajo futuro se deja la inquietud para futuros investigadores, así como para él propio maestrando que escribe esta obra en tomar los aportes realizados y conclusiones para llevar desde la teoría presentada hacia la propuesta de colocar en agenda e implementación empírica del proyecto de la creación de una Política de Programas de Bug Bounty por parte del Estado Nacional Argentino y el desarrollo de una plataforma web con carácter de infraestructura crítica del país.

Por lo expuesto en el párrafo anterior se considera que los pasos a seguir como trabajo futuro deben ser los siguientes:

- Realizar una investigación sobre el marco normativo de los Programas de Bug Bounty que den los paraguas legales tanto a los Organismos de la Administración Pública Nacional como a los ciudadanos que se inscriban en los programas y suban sus reportes de vulnerabilidades, ya que no fue tratado al no ser del alcance de esta tesis.
- Realizar una nueva encuesta, pero teniendo como público objetivo a las comunidades de Bug Bounty, Ethical Hackers, Pentesters, etc para poder conocer su opinión y si estuvieran dispuestos a inscribirse en un programa de Bug Bounty del Estado Nacional de la República Argentina en el caso hipotético de la creación de una Política Pública de Programas de Bug Bounty. En el alcance de esta tesis sólo se pretendió conocer la opinión de los agentes de la Administración Pública Nacional.

Bibliografía

(INDEC), I. N. (Abril de 2023). *Dotación de personal de la administración pública nacional, empresas y sociedades.* Obtenido de https://www.indec.gob.ar/ftp/cuadros/economia/dotacion_personal_apn_05_234BEFA7D474.pdf

@ARSATSA. (30 de 11 de 2022). *twitter.com*. Recuperado el 10 de 09 de 2023, de twitter: https://twitter.com/ARSATSA/status/1598078467140378625

@Migraciones_AR. (27 de Agosto de 2020). *twitter.com*. Obtenido de https://twitter.com: https://twitter.com/Migraciones_AR/status/1299126157418336262

@senorarroz. (04 de Octubre de 2016). *twitter.com*. Obtenido de https://twitter.com: https://twitter.com/senorarroz/status/783385066390982658?s=20

abc tecnología. (26 de Febrero de 2015). *ABC Consultorio*. Obtenido de ABC Consultorio: https://www.abc.es/tecnologia/consultorio/20150226/abci--201502252129.html

Aberouch, A. (02 de Noviembre de 2015). *www.bbvaopenmind.com*. Obtenido de https://www.bbvaopenmind.com/: https://www.bbvaopenmind.com/tecnologia/innovacion/5-bugs-informaticos-que-marcaron-la-historia/

Aguilar Villanueva, L. F. (1992). *Colección antologías de política pública* (1 ed.). España: Grupo Editorial Miguel Angel Porrua.

Agulló, J., & Rico, R. (02 de Junio de 2009). *¿Distopía en la red? Conocimiento (libre) y propiedad (intelectual), sociología de una confrontación (mundial) silenciosa. "La política es la guerrilla por los medios" (Subcomandante Marcos).* Obtenido de XXVII Congreso de la Asociación Latinoamericana de Sociología. VIII Jornadas de Sociología de la Universidad de Buenos Aires. Asociación Latinoamericana de Sociología, Buenos Aires.: https://www.aacademica.org/000-062/65

Aleph1. (08 de Noviembre de 1996). *phrack.org*. Obtenido de http://phrack.org: http://phrack.org/issues/49/14.html

ámbito. (03 de 05 de 2023). *www.ambito.com*. Recuperado el 10 de 09 de 2023, de ambito.com: https://www.ambito.com/informacion-general/hackearon-al-inta-y-piden-mas-us2-millones-devolver-el-sistema-n5713388

Argentina.gob.ar. (05 de 09 de 2023). *www.argentina.gob.ar*. Recuperado el 10 de 09 de 2023, de Argentina.gob.ar: https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad#:~:text=Esta%20estrategia%20busca%20jerarquizar%20la,los%20actores%20de%20la%20sociedad.

Assalian, M. (23 de 08 de 2023). *Security Advisor*. Recuperado el 10 de 09 de 2023, de Security Advisor Su defensa digital: https://sadvisor.com/ciberdelincuentes-exponen-datos-sensibles-tras-ataque-a-pami/

Aybar, R. D. (2020). *Automatización de Pruebas de Seguridad en el Ciclo de Vida del Desarrollo de Software. (Trabajo Final de Posgrado. Universidad de Buenos Aires.).* Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1631_AybarRD.pdf

Bannister, A. (30 de Noviembre de 2021). *portswigger.net*. Obtenido de https://portswigger.net: https://portswigger.net/daily-swig/bug-bounty-radar-the-latest-bug-bounty-programs-for-december-2021

Boehm, B. (Septiembre de 1987). Industrial Metrics Top 10 List. *Computer Magazine - IEEE*, 84-85.

Boehm, B., & Basili, V. R. (01 de 01 de 2001). Software Defect Reduction Top 10 List. *Computer Magazine - IEEE, V. 34*, 135-137.

Brodersen, J. (01 de 07 de 2023). *www.clarin.com*. Recuperado el 10 de 09 de 2023, de clarin.com: https://www.clarin.com/tecnologia/publicaron-archivos-robados-comision-nacional-valores-informacion-sensible-datos-privados_0_4EL06yMc7u.html

Bugcrowd. (07 de Diciembre de 2021). *www.bugcrowd.com*. Obtenido de https://www.bugcrowd.com/: https://www.bugcrowd.com/

Bugcrowd. (28 de Enero de 2021). *www.bugcrowd.com*. Obtenido de https://www.bugcrowd.com: https://www.bugcrowd.com/blog/illustrated-guide-to-bug-bounties-step-1-planning/

bugcrowd. (2023). *bugcrowd.com*. Recuperado el 10 de 09 de 2023, de bugcrowd: https://bugcrowd.com/openai

Caryl-Sue. (15 de 07 de 2020). *National Geographic*. Obtenido de National Geographic: https://www.nationalgeographic.org/thisday/sep9/worlds-first-computer-bug/

Catalán, G. (05 de Febrero de 2017). *noticias.perfil.com/noticias*. Obtenido de https://noticias.perfil.com/noticias: https://noticias.perfil.com/noticias/politica/2017-02-05-el-gobierno-muy-vulnerable-a-los-hackers-hubo-ataques-en-cuatro-ministerios.phtml

Catalinas, Á. (04 de Junio de 2019). *www.ciberseguridadpyme.es*. Obtenido de https://www.ciberseguridadpyme.es: https://www.ciberseguridadpyme.es/destacado/yeswehack-bugbounty-europa/

Chen, R. (10 de Septiembre de 2014). *Microsoft*. Obtenido de https://devblogs.microsoft.com: https://devblogs.microsoft.com/oldnewthing/?p=44113

clarin.com. (26 de 04 de 2018). *www.clarin.com*. Obtenido de https://www.clarin.com: https://www.clarin.com/policiales/hackearon-web-policia-ciudad-amenazaron-ciberataques_0_HymuVFkTf.html

Córdoba, R. P. (02 de 08 de 2023). *www.perfil.com*. Recuperado el 10 de 09 de 2023, de perfil.com: https://www.perfil.com/noticias/cordoba/un-virus-informatico-afecta-el-sistema-de-pami-es-un-problema-grave.phtml

Denuncia. (27 de Enero de 2017). *crimenyrazon.com*. Obtenido de https://crimenyrazon.com: https://crimenyrazon.com/el-hackeo-de-la-cuenta-de-twitter-de-bullrich-y-la-vulnerabilidad-del-voto-electronico/

derechodelared. (25 de Agosto de 2019). *derechodelared.com*. Obtenido de derechodelared.com: https://derechodelared.com/bug-bounty-programs/

diarioti.com. (30 de Diciembre de 2019). *diarioti.com*. Obtenido de https://diarioti.com: https://diarioti.com/zero-day-initiative-de-trend-micro-lidera-en-inteligencia-sobre-vulnerabilidades/111261

Dirección Nacional de Migraciones. (27 de Agosto de 2020). *twitter.com*. Obtenido de twitter.com: https://twitter.com/Migraciones_AR/status/1299126157418336262

Director. (20 de Diciembre de 2016). *www.elciudadano.com*. Obtenido de https://www.elciudadano.com/: https://www.elciudadano.com/ciencia-tecnologia/el-uso-de-armas-ciberneticas-de-usa-desde-1982-sobre-rusia-y-el-mundo/12/20/

Dowd, M., McDonald, J., & Schuh, J. (2019). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities* (Vol. 1). Addison-Wesley Professional; 1er edición (1 Enero 2006).

Feldman, A., & Feola, A. (14 de Diciembre de 2020). *digital.gov*. Obtenido de https://digital.gov: https://digital.gov/2020/12/14/tts-bug-bounty-program-3-year-review/

Florêncio, R. (Agosto de 2020). Permissão para Atacar: Como Melhorar a Cibersegurança de Portugal através de Um Programa de Bug Bounty Governamental. *idn Nação e Defesa*(156), 79-102. Obtenido de http://hdl.handle.net/10400.26/35920

Friis-Jensen, E. (11 de Abril de 2014). *cobalt.io*. Obtenido de cobalt.io: https://cobalt.io/blog/the-history-of-bug-bounty-programs

Fundeu. (4 de Noviembre de 2011). *fundeu.es*. Obtenido de https://www.fundeu.es: https://www.fundeu.es/recomendacion/crowdsourcing

fyccorp.com. (10 de Noviembre de 2020). Obtenido de https://www.fyccorp.com: https://www.fyccorp.com/articulo-10-grandes-errores-de-software#:~:text=Se%20colapsa%20el%20aeropuerto%20de,sus%20destinos%20durante%209%20horas.

GARCÍA, L. C. (23 de Julio de 2020). *periciatecnologica.org*. Obtenido de https://periciatecnologica.org: https://periciatecnologica.org/tienen-futuro-los-programas-bug-bounty-en-instituciones-publicas/

hackerone. (s.f.). Obtenido de hackerone: https://www.hackerone.com/hack-the-pentagon

HackerOne. (29 de Septiembre de 2020). *hackerone*. Recuperado el 20 de Mayo de 2023, de https://hackerone.com: https://hackerone.com/gsa_bbp?type=team

HackerOne. (07 de Diciembre de 2021). *www.hackerone.com*. Obtenido de https://www.hackerone.com: https://www.hackerone.com/

HackerOne. (s.f.). *Hackerone*. Obtenido de https://docs.hackerone.com: https://docs.hackerone.com/programs/vdp-vs-bbp.html

HackerOne Team. (2021). *The 2021 Hacker Report.*

HackerOne. (s.f.). *www.hackerone.com*. Obtenido de https://www.hackerone.com/: https://www.hackerone.com/hack-the-pentagon

Hackr.fi. (08 de Diciembre de 2021). *https://hackr.fi*. Obtenido de https://hackr.fi: https://hackr.fi/

Haworth, J. (01 de Septiembre de 2021). *portswigger.net*. Obtenido de https://portswigger.net: https://portswigger.net/daily-swig/singapore-government-launches-bug-bounty-program-for-digital-services

Hill, M., & Hupe, P. (2002). *Implementing Public Policy: Governance in Theory and in Practice.*

iDefense. (12 de Agosto de 2002). *web.archive.org*. Obtenido de web.archive.org: https://web.archive.org/web/20020812035333/www.idefense.com/contributor.html

Indec. (s.f.). *www.indec.gob.ar*. Obtenido de www.indec.gob.ar: https://www.indec.gob.ar/indec/web/Nivel4-Tema-3-10-102

infotechnology. (09 de Agosto de 2020). *www.infotechnology.com*. Obtenido de https://www.infotechnology.com: https://www.infotechnology.com/online/Hackearon-Migraciones-y-el-gobierno-no-quiere-pagar-piden-us-4-M-para-no-liberar-los-datos-de-millones-de-argentinos-20200909-0006.html

Intel. (s.f.). *Intel.la*. Obtenido de Intel.la: https://www.intel.la/content/www/xl/es/silicon-innovations/moores-law-technology.html

Interpol. (s.f.). *www.interpol.int*. Obtenido de www.interpol.int: https://www.interpol.int/es/Delitos/Ciberdelincuencia

IOSFA. (29 de Septiembre de 2021). *iosfa.gob.ar*. Obtenido de iosfa.gob.ar: https://iosfa.gob.ar/novedades/132/informacion-sobre-base-de-datos-de-afiliados

JEFATURA DE GABINETE DE MINISTROS. (18 de Septiembre de 2019). *www.argentina.gob.ar*. Obtenido de www.argentina.gob.ar: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1523-2019-328599/texto

JEFATURA DE GABINETE DE MINISTROS. (10 de Noviembre de 2021). *Boletin Oficial de la Republica Argentina*. Obtenido de https://www.boletinoficial.gob.ar/: https://www.boletinoficial.gob.ar/detalleAviso/primera/252690/20211111

Jefatura de Gabinete de Ministros. (29 de Octubre de 2021). *mapadelestado.jefatura.gob.ar.* Obtenido de mapadelestado.jefatura.gob.ar: https://mapadelestado.jefatura.gob.ar

johnk. (09 de Noviembre de 2017). *www.hackerone.com*. Obtenido de https://www.hackerone.com/: https://www.hackerone.com/ethical-hacker/hack-pentagon-turns-one-hackerone

johnk. (01 de Marzo de 2019). *www.hackerone.com*. Obtenido de https://www.hackerone.com: https://www.hackerone.com/company-news/trytohack-makes-history-first-bug-bounty-hacker-earn-over-1-million

LA NACIÓN. (13 de agosto de 2019). *Ola de intrusiones en cuentas de las fuerzas federales de seguridad*. Obtenido de La Nación: https://www.lanacion.com.ar/seguridad/ola-de-intrusiones-en-cuentas-de-las-fuerzas-federales-de-seguridad-nid2276919/

Lahera, E. (Agosto de 2004). *REPOSITORIO DIGITAL Comisión Económica para América Latina y el Caribe.* (N. Unidas, Ed.) Recuperado el 3 de Julio de 2023, de https://repositorio.cepal.org/bitstream/handle/11362/6085/S047600_es.pdf?sequence=1&isAllowed=y

Landry, J. (s.f.). *SecureOps*. Obtenido de SecureOps: https://secureops.com/blog/bug-bounty-programs/

Li, V. (2021). *Bug bounty bootcamp : the guide to finding and reporting web vulnerabilities.* San Francisco: No Starch Press, Inc.

López, M. S. (2016). 'Bug bounty': evoluciona tu inversión en ciberseguridad. *Red Seguridad*, 74-75.

Lozano, C. A., & Shahmmer, A. (2018). *Bug Bounty Hunting Essentials: Quick-paced guide to help white-hat hackers get through bug bounty programs.* Packt Publishing Ltd.

Magoun, A. B., & Israel, P. (01 de Agosto de 2013). *IEEE Spectrum*. Obtenido de IEEE Spectrum: https://spectrum.ieee.org/did-you-know-edison-coined-the-term-bug

manageengine.com. (s.f.). Obtenido de https://www.manageengine.com: https://www.manageengine.com/latam/vulnerability-management/vulnerabilidad-dia-cero-zero-day.html

Mendez, M. H. (14 de Octubre de 2018). *www.tekcrispy.com*. Obtenido de www.tekcrispy.com: https://www.tekcrispy.com/2018/10/14/bugs-errores-de-software/

Missillier, M. (14 de Septiembre de 2017). *BSSI*. Obtenido de BSSI: https://blog.bssi.fr/le-bug-bounty/

Moreno, P. H. (Enero - Junio de 1993). *Instituto Nacional de Administración Pública.* (E. R. INAP, Ed.) Recuperado el 06 de 07 de 2023, de http://historico.juridicas.unam.mx/publica/librev/rev/rap/cont/84/pr/pr1.pdf

Moussouris, K. (2020). *csrc.nist.gov.* Obtenido de https://csrc.nist.gov: https://csrc.nist.gov/CSRC/media/Presentations/industry-bug-bounty-implementations-lessons/images-media/Industry%20Bug%20Bounty%20Implementations%20Lessons.pdf

mozillazine. (02 de Agosto de 2004). *www.mozillazine.org*. Obtenido de www.mozillazine.org: http://www.mozillazine.org/talkback.html?article=5121

NASA. (s.f.). *www.jpl.nasa.gov*. Obtenido de https://www.jpl.nasa.gov/: https://www.jpl.nasa.gov/missions/mariner-1

National Museum of American History. (s.f.). *National Museum of American History*. Obtenido de National Museum of American History: https://americanhistory.si.edu/collections/search/object/nmah_334663

Netscape. (10 de Octubre de 1995). *web.archive.org*. Obtenido de web.archive.org: https://web.archive.org/web/19970501041756/www101.netscape.com/newsref/pr/newsrelease48.html

NETSCAPE ANNOUNCES "NETSCAPE BUGS BOUNTY" WITH RELEASE OF NETSCAPE NAVIGATOR 2.0 BETA. (s.f). Obtenido de Wayback Machine: https://web.archive.org/web/19970501041756/http://www3.netscape.com:80/newsref/pr/newsrelease48.html

Nicola, G. D. (13 de Agosto de 2019). *Las dos hipótesis sobre el hackeo a la Policía Federal*. Obtenido de La Nación: https://www.lanacion.com.ar/seguridad/las-hipotesis-del-hackeo-policia-federal-nid2277076/

Nirenberg, O., Brawerman, J., & Ruiz, V. (2003). *Programación y Evaluación de Proyectos Sociales. Aportes para la racionalidad y la transparencia.* Argentina: Paidos.

Omer Akgul, T. E. (2020). *The Hackers' Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs.*

OpenAI. (11 de 04 de 2023). *openai.com*. Recuperado el 10 de 09 de 2023, de openai.com: https://openai.com/blog/bug-bounty-program

Ozlak, O., & O'Donnell, G. A. (1995). Estado y políticas estatales en América Latina: hacia una estrategia de investigación. *Redes, 2(4)*, 99-128. Recuperado el 04 de 07 de 2023, de https://www.redalyc.org/articulo.oa?id=90711285004

Pastor, J. (23 de Abril de 2018). *xataka*. Obtenido de https://www.xataka.com/: https://www.xataka.com/historia-tecnologica/hace-20-anos-windows-98-debutaba-y-lo-hacia-con-bsod-incluida-delante-de-bill-gates

perfil.com. (26 de 01 de 2017). Obtenido de https://www.perfil.com: https://www.perfil.com/noticias/politica/patricia-bullrich-confirmo-que-fue-hackeada-y-advirtio-que-investigaran-el-ciberataque.phtml

Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race.* New York: Bloomsbury Publishing.

Policiales, C. (26 de Abril de 2018). *www.clarin.com*. Obtenido de https://www.clarin.com: https://www.clarin.com/policiales/hackearon-web-policia-ciudad-amenazaron-ciberataques_0_HymuVFkTf.html

Pressman, J. L., & Wildavsky, A. (1998). *Implementación. Cómo grandes expectativas concebidas en Washington se frustran en Oakland.* Fondo de Cultura Económica.

PÚBLICA, S. D. (04 de Junio de 2020). *www.argentina.gob.ar*. Obtenido de www.argentina.gob.ar: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-36-2020-338378/texto

Ramírez, F. (07 de Julio de 2020). *Una al Día*. Obtenido de Una al Día: https://unaaldia.hispasec.com/2020/07/en-auge-los-programas-de-bug-bounty.html

RELEASE, P. (s.f.). *Bugcrowd University Opens Its Doors to the Crowd*. Obtenido de www.bugcrowd.com: https://www.bugcrowd.com/press-release/bugcrowd-university-opens-its-doors-to-the-crowd/

Rizzo, D. O. (2020). *Marco de referencia de ciberseguridad para infraestructuras críticas. (Trabajo Final de Posgrado. Universidad de Buenos Aires.)*. Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1603_RizzoDO.pdf

RM/fl. (22 de 09 de 2022). *perfil.com*. Recuperado el 10 de 09 de 2023, de perfil: https://www.perfil.com/noticias/economia/investigan-un-posible-hackeo-al-ministerio-de-economia.phtml

Rutledge, K., Ramroop, T., Boudreau, D., McDaniel, M., Teng, S., Sprout, E., . . . Hunt, J. (21 de Enero de 2011). *nationaleographic.org*. Obtenido de https://www.nationalgeographic.org/: https://www.nationalgeographic.org/encyclopedia/Y2K-bug/

Sáenz, T. (1997). El análisis de las políticas públicas, en Bañon, R. y Carrillo, E. (comp.) La Nueva Administración Pública. Alianza Editorial S.A.

Sampieri , R. H., Collado, C. F., & Baptista Lucio, P. (2006). *Metodología de la investigación* (Cuarta ed.). Mexico: McGraw-Hill.

Scalzo, E. L. (02 de Agosto de 2013). *fundeuRAE*. Obtenido de fundeuRAE: https://www.fundeu.es/recomendacion/bug-alternativas-en-espanol/

secwest. (08 de Diciembre de 2021). *www.secwest.net*. Obtenido de https://www.secwest.net: https://www.secwest.net/pwn2ownaustin2021

Técnica, S. L. (01 de 09 de 2023). *Boletín Oficial de la República Argentina*. Recuperado el 10 de 09 de 2023, de Boletín Oficial de la República Argentina: https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904

U.S. Department of Defense. (21 de Noviembre de 2016). *www.defense.gov*. Obtenido de https://www.defense.gov: https://www.defense.gov/News/Releases/Release/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/

U.S. Department of Defense. (04 de Mayo de 2021). *www.defense.gov*. Obtenido de https://www.defense.gov: https://www.defense.gov/News/News-Stories/Article/Article/2595294/dod-expands-hacker-program-to-all-publicly-accessible-defense-information-syste/

Velis, R. (25 de Septiembre de 2017). *elcorreoweb.es*. Obtenido de https://elcorreoweb.es: https://elcorreoweb.es/sevilla/los-fallos-clave-del-accidente-mortal-del-a400m-XL3368624

Vulnerability Management. (09 de Noviembre de 2021). *HackerOne*. Obtenido de https://www.hackerone.com/: https://www.hackerone.com/vulnerability-management/what-bug-bounty-should-you-offer-one-and-how-do-it

Vuusteri. (15 de Abril de 2021). Windows 98 presentation fail (HQ) [vídeo]. Youtube. Obtenido de https://www.youtube.com: https://www.youtube.com/watch?v=yeUyxjLhAxU

Webster, M. (s.f.). *Merriam Webster*. Obtenido de Merriam Webster: https://www.merriam-webster.com/dictionary/bug

Weigand, C., & Stevens, C. (23 de Octubre de 2015). *https://cyberdefensereview.army.mil*. Obtenido de https://cyberdefensereview.army.mil: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136015/army-vulnerability-response-program-a-critical-need-in-the-defense-of-our-nation/

welivesecurity. (9 de Abril de 2014). *welivesecurity.com*. Obtenido de https://www.welivesecurity.com: https://www.welivesecurity.com/la-es/2014/04/09/5-cosas-debes-saber-sobre-heartbleed/#:~:text=Se%20trata%20de%20una%20vulnerabilidad%20(CVE%2D2014%2D0160),de%20ah%C3%AD%20proviene%20su%20nombre.

wikipedia. (10 de 09 de 2023). *es.wikipedia.org*. Obtenido de wikipedia.org: https://es.wikipedia.org/wiki/Bolet%C3%ADn_Oficial_de_la_Rep%C3%BAblica_Argentina

Williams, D. D. (28 de Octubre de 2021). *https://nssdc.gsfc.nasa.gov*. Obtenido de https://nssdc.gsfc.nasa.gov: https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=MARIN1

Williams, D. D. (s.f.). *National Aeronautics and Space Administration*. Obtenido de National Aeronautics and Space Administration: https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=MARIN1

Winchester, L. (14 a 25 de 11 de 2011). Recuperado el 06 de 07 de 2023, de https://gc.scalahed.com/recursos/files/r161r/w25351w/M1AP113_S4_WINCHESTER.pdf

www.defense.gov. (21 de Diciembre de 2016). Obtenido de web.archive.org: https://web.archive.org/web/20161221090829/http://www.defense.gov/Portals/1/Documents/Fact_Sheet_Hack_the_Pentagon.pdf

YesWeHack. (07 de Diciembre de 2021). *www.yeswehack.com*. Obtenido de https://www.yeswehack.com/: https://www.yeswehack.com/

Zero Day Initiative. (25 de Julio de 2005). *www.zerodayinitiative.com*. Obtenido de https://www.zerodayinitiative.com: https://www.zerodayinitiative.com/about/

Zuckerman, L. (22 de Abril de 2000). *The New York Times*. Obtenido de The New York Times: https://www.nytimes.com/2000/04/22/arts/think-tank-if-there-s-a-bug-in-the-etymology-you-may-never-get-it-out.html

Anexo I

A continuación, se comparten las tablas de distribución de los resultados de las preguntas P4, P6, P8, P9, P10 y P11.

Tablas de Frecuencia

¿Conoce o escucho hablar de Programas de Bug Bounty?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	15	21,7	21,7	21,7
	Si	54	78,3	78,3	100,0
	Total	69	100,0	100,0	

Tabla 4 Representación Propia. Frecuencia, Porcentaje de Respuesta Pregunta 4

A su criterio ¿El Estado Nacional Argentino debe crear una Política Pública Nacional de Programas de Bug Bounty?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No	9	13,0	13,0	13,0
	Si	60	87,0	87,0	100,0
	Total	69	100,0	100,0	

Tabla 5 Representación Propia. Frecuencia, Porcentaje de Respuesta Pregunta 6

¿Cuánto considera que aportaría a la Ciberseguridad de los Organismos de la APN que el Estado Nacional Argentino cuente con una Política Pública Nacional de Programas de Bug Bounty?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	0	9	13,0	13,0	13,0
	Poco	1	1,4	1,4	14,5
	Mucho	59	85,5	85,5	100,0
	Total	69	100,0	100,0	

Tabla 6 Representación Propia. Frecuencia, Porcentaje de Respuesta Pregunta 8

A su criterio si el Estado Nacional Argentino crea una Política Pública Nacional de Programas de Bug Bounty ¿Debe desarrollar su propia plataforma o debe generar los programas desde plataformas como YesWeHack, HackerOne, BugCrowd, etc?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	0	9	13,0	13,0	13,0
	Podría utilizar una plataforma de terceros (aunque los datos perderían Soberanía Nacional)	6	8,7	8,7	21,7
	Debe desarrollar su propia plataforma	54	78,3	78,3	100,0
	Total	69	100,0	100,0	

Tabla 7 Representación Propia. Frecuencia, Porcentaje de Respuesta Pregunta 9

Si se crea una Política Pública Nacional de Programas de Bug Bounty ¿Considera que se debe tratar como una Infraestructura Critica?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	0	9	13,0	13,0	13,0
	No	6	8,7	8,7	21,7
	Si	54	78,3	78,3	100,0
	Total	69	100,0	100,0	

Tabla 8 Representación Propia. Frecuencia, Porcentaje de Respuesta Pregunta 10

Si es considera como una Infraestructura Critica ¿Debe ser incorporada a las Infraestructuras Criticas dentro de la Resolución 1523/2019?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	0	9	13,0	13,0	13,0
	No	5	7,2	7,2	20,3
	Si	55	79,7	79,7	100,0
	Total	69	100,0	100,0	

Tabla 9 Representación Propia. Frecuencia, Porcentaje de Respuesta Pregunta 11

Y también los datos descriptivos obteniendo el rango, el máximo y el mínimo de la suma de todas las variables.

Estadísticos descriptivos

	N	Rango	Mínimo	Máximo	Media	Desv. estándar
SUMA	69	6,00	11,00	17,00	13,2174	1,14878
N válido (por lista)	69					

Tabla 10 Representación Propia. Datos Descriptivos Suma de Variables