Proyecto: Grupo 2 - DevForge

| **Producto:** | AuditForge |
| --- | --- |
| **Descripción breve:** | El producto AuditForge está orientado a auditores y empresas de seguridad informática, que enfrentan el problema del gran consumo de tiempo que implica la creación de informes, lo que limita el tiempo del auditor para poder realizar pruebas y explotar vulnerabilidades de manera efectiva. Dicho problema se intensifica aún más cuando se debe trabajar colaborativamente, junto con la restricción de políticas anti nube (las cuales no permiten compartir datos de clientes con terceros). Esta problemática se resuelve mediante el uso de nuestro software, el cual brinda a los usuarios la posibilidad generar informes de forma automatizada sin la necesidad de utilizar servicios de internet y sin la preocupación de utilizar herramientas de terceros, resguardando así la confidencialidad de los datos manejados. Lo anterior permite la aceleración del proceso de generación de informes, reduciendo el tiempo total dedicado al proyecto, optimizando así el proceso y servicio de auditoría. Nuestra solución se diferencia de Dradis, Cyver Core y PwnDoc por proveer las funcionalidades de un Dashboard con información segregada por clientes, como también las recomendaciones de CWE automatizadas a través de IA, por otra parte posee un valor agregado relevante dentro del negocio, como lo es ser un software de código abierto. |
| **Líder del proyecto:** | Camilo Vera Vidales |
| **Campus:** | Casa Central |
| **Objetivos ODS:** |  |
| **Link a vídeo Pitch:** | <https://youtu.be/lE1Z4hyVsS8> |

**Equipo compuesto por:**

| Sebastián Alvarado Raimilla | [LinkedIn - Sebastián Alvarado](https://www.linkedin.com/in/sealrai) | +56 9 57031557 |
| --- | --- | --- |
| Julio Cerda Villablanca | [LinkedIn - Julio Cerda](http://www.linkedin.com/in/julio-cerda-villablanca-87b293258) | +56 9 45389525 |
| José Llanos Gaete | [LinkedIn - José Llanos](https://www.linkedin.com/in/jos%C3%A9-llanos-99b1801b6) | +56 9 64822666 |
| Maximiliano Ponce Abutter | [LinkedIn - Maximiliano Ponce](https://www.linkedin.com/in/maximiliano-ponce-abutter) | +56 9 45755274 |
| Ricardo Olalquiaga Ferreira | [LinkedIn - Ricardo Olalquiaga](https://www.linkedin.com/in/ricardo-olalquiaga) | +56 9 88962987 |
| Camilo Vera Vidales | [LinkedIn - Camilo Vera Vidales](https://www.linkedin.com/in/camilo-vera-vidales) | +56 9 82755636 |

**Descripción del problema**

El ***hacking* ético** es la práctica de identificar y explotar vulnerabilidades en sistemas informáticos de manera autorizada. A diferencia de los *hackers* maliciosos, los *hackers* éticos actúan de manera legal y ética. Bajo este contexto, hay empresas especializadas que realizan pruebas de seguridad mediante auditorías, con el fin de informar sobre debilidades que comprometen los sistemas del cliente. Así, los auditores de seguridad son los encargados de realizar las pruebas de vulnerabilidad y culminan el proceso de identificación de vulnerabilidades con un **reporte** que resume todos sus hallazgos.

El tiempo utilizado en la **generación de informes** de los auditores de seguridad resulta en un problema, ya que puede ocupar hasta el 40% del tiempo total dedicado al proyecto[[1]](#footnote-0). Esto hace que el proceso de *hacking* ético no sea óptimo, ya que resta tiempo útil a la realización de pruebas de seguridad adicionales en función del plazo establecido por el cliente. Este problema impacta negativamente al auditor y a la empresa de ciberseguridad, dado que reduce el tiempo que el auditor dedica a la búsqueda de vulnerabilidades y aumenta el tiempo destinado a la generación de reportes.

Actualmente, la generación de informes se realiza de manera **manual** a través de *LibreOffice* y el uso de plantillas. Por acuerdos de confidencialidad, no se pueden utilizar otras herramientas como *Microsoft Word* o *Google Docs*, porque estas herramientas no son *open source*. Esto implica que, al ser código cerrado, se desconoce el funcionamiento interno y el procesamiento de los datos dentro de sus aplicaciones. Adicionalmente, existen clientes que establecen no utilizar programas con participación de terceros, por lo cual se restringe el uso de herramientas que no sean locales.

El uso de herramientas locales provoca una falta de trabajo colaborativo entre auditores de seguridad, porque estas no permiten que varios auditores puedan generar un reporte cooperativamente de forma rápida y eficiente.

En el **Anexo 1** se detalla el proceso generalizado de auditoría, y se destaca el cuello de botella que se produce en la generación de informes.

Esto es un problema complejo de ingeniería, ya que se debe crear y diseñar una solución que cumpla varios requisitos técnicos que puedan coexistir entre sí. Estos son: el resguardo de la confidencialidad de la información, la automatización del proceso de reportes para evitar su realización manual, la adición de un modelo de redes neuronales para las recomendaciones de CWEs, y la implementación del trabajo colaborativo.

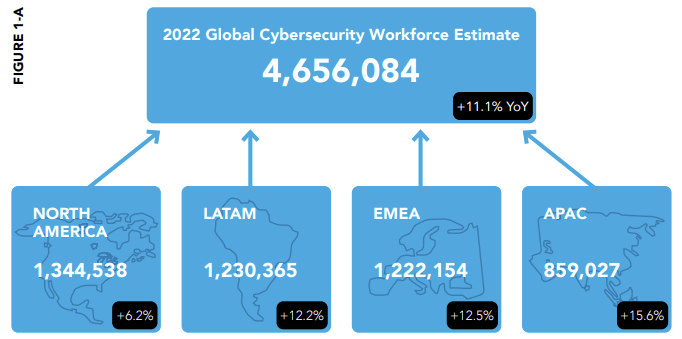
El problema aborda el ODS 9: **Industria, Innovación e Infraestructura**. Específicamente enfocado en la innovación y desarrollo de herramientas automatizadas para la industria. Esto agilizaría el proceso y reduciría el tiempo dedicado al proceso de generación de informes manual, brindando mayor eficiencia y productividad para servicios más rentables y efectivos. Por otro lado, aporta infraestructura con la creación de una plataforma segura y colaborativa para generar informes, mejorando la eficiencia y la productividad.

**Potenciales clientes y usuarios**

El **cliente** son empresas que ofrecen como servicio auditorías de ciberseguridad. Otro potencial cliente son los auditores de ciberseguridad independientes que realizan servicios de *Bug-Bounty*. Esto consiste en que empresas pagan por el hallazgo de vulnerabilidades en sus servicios a auditores independientes o *freelancers*.

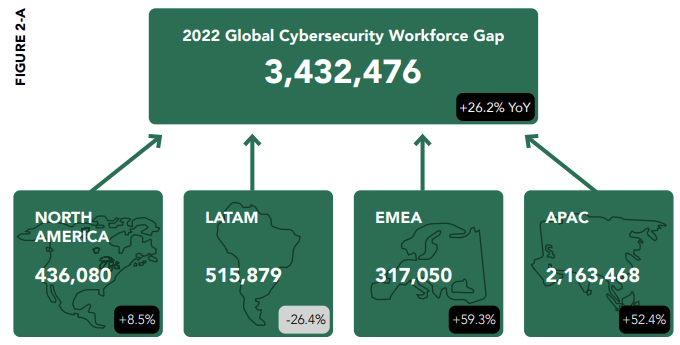
Según el estudio de la fuerza de trabajo en el ámbito de la ciberseguridad[[2]](#footnote-1) hecho en el año 2022 por la organización sin fines de lucro (ISC)² (*International Information Systems Security Certification Consortium*) se estiman aproximadamente 4.66 millones de profesionales dedicados al ámbito de la ciberseguridad en el mundo, donde específicamente 1.23 millones de estos profesionales pertenecen a Latinoamérica. Así mismo, el estudio estima que son necesarios otros 3.43 millones de profesionales a nivel mundial, o específicamente otros 515 mil profesionales a nivel latinoamericano.

Como información adicional, a pesar de añadir 464 mil profesionales en el año 2021, la brecha entre los trabajadores actuales y los necesarios para el año 2022, aumentó más del doble en comparación a los 465 mil profesionales antes mencionados.

En conclusión, si bien los profesionales de ciberseguridad aumentan considerablemente año a año, la demanda de estos aumenta más rápido.

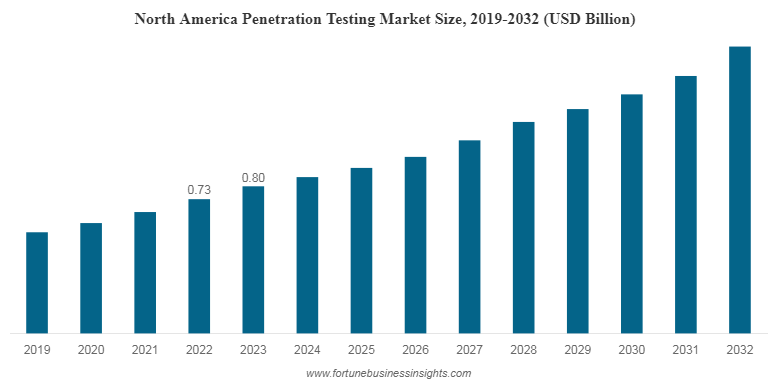
*Estimado global y desagregado de la fuerza*

*de trabajo para el año 2022*



*Brecha global y desagregada entre profesionales actuales y necesitados para el año 2022*

Por otra parte, es posible asegurar que es un mercado que se encuentra al alza según distintos estudios, donde se espera un crecimiento del 12,6% anual hasta 2032.[[3]](#footnote-2)



*Tamaño de mercado norteamericano en Penetration Testing desde 2019 hasta 2032*

El **usuario** es el auditor de seguridad, el cual realiza los servicios destinados a las empresas que contratan las auditorías. Este auditor puede ser uno que trabaje en una empresa de ciberseguridad, o uno que realice servicios de *Bug-Bounty/Freelancing*. Cabe destacar que los usuarios son de nivel profesional en términos tecnológicos, dado que realizan tareas de alta complejidad, siendo especializados en distintas áreas del *hacking* ético

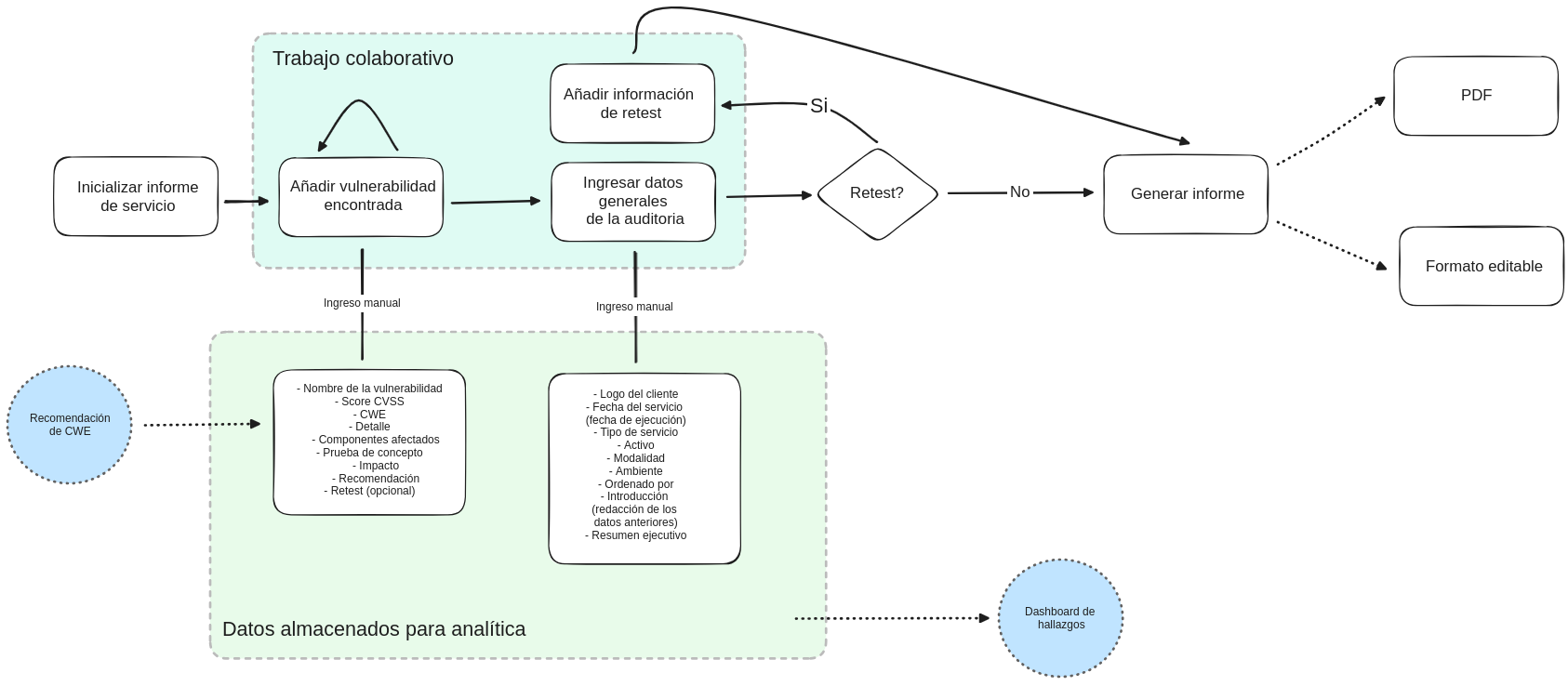
**Visualización de la solución**

Nuestra solución busca cumplir con todos los requisitos y funcionalidades necesarias para realizar la documentación de auditorías de ciberseguridad.

Las funcionalidades distintivas de nuestro producto son las siguientes:

* Ser un software open source para una mayor transparencia de sus contenidos. Además, esto permitiría que cada cliente pueda montar su propio servidor para su uso.
* Cumplir con la no divulgación de información con terceros (como son los servicios en la nube), ya que los datos se almacenan y usan de manera local.
* Poseer un dashboard personalizado sobre los clientes a los que se realizaron servicios de auditoría. Este dashboard contiene un resumen sobre las vulnerabilidades encontradas, malas prácticas, entre otros, lo que le proporciona información relevante sobre los servicios tanto a los usuarios de nuestra solución, como a los clientes que ellos auditen.
* Permitir el trabajo colaborativo entre más de un auditor de manera simultánea, agilizando el trabajo en conjunto y las correcciones de informes.
* Generar informes de vulnerabilidades de manera automatizada, evitando trabajar directamente con editores de documentos y, por lo tanto, mejorando la experiencia del usuario auditor.
* Durante la construcción del informe, incorporar recomendaciones de CWE asociados a las descripciones de vulnerabilidades mediante el uso de inteligencia artificial.

A continuación se incluye un diagrama paso a paso de la solución propuesta.



**Valor agregado**

Nuestro software permitirá mejorar los tiempos de generación de informes sin la necesidad de utilizar servicios de internet (manteniendo confidencialidad de los datos), sin la preocupación de utilizar herramientas de terceros imposibles de auditar (al ser open source) y aumentando la facilidad de uso, con herramientas desarrolladas para agilizar aún más la velocidad de generación de reportes.

A continuación se presenta una tabla comparativa entre nuestro software y software de la competencia:

|  | Dradis | Cyver Core | PwnDoc | Nuestra solución |
| --- | --- | --- | --- | --- |
| Open source | X | X | ✔ | ✔ |
| Facilidad de uso | X | X | X | ✔ |
| Offline | X | X | ✔ | ✔ |

La mayor velocidad en tiempos de entregas de informe es muy valiosa tanto para los usuarios, ya que permite ahorrar tiempo en la parte más repetitiva de su trabajo, así como para las empresas auditadas, ya que al obtener resultados de servicios de manera más rápida permite prevenir posibles ataques, generar los cambios necesarios para cubrir las vulnerabilidades y en general aumentar la seguridad de sus propios servicios.

Por otro lado, la solución permitiría almacenar información acerca de las vulnerabilidades encontradas en una visión “macro” tras realizar múltiples servicios de auditoría a una misma empresa, lo que daría la posibilidad tanto a los usuarios de nuestra solución como a las organizaciones auditadas identificar los puntos débiles de las aplicaciones u otros elementos auditados. Este conocimiento beneficia tanto a los usuarios de nuestra solución como a auditados, ya que los primeros sabrán “dónde atacar primero” en un futuro servicio, y los auditados podrán saber qué medidas tomar para reducir la cantidad de hallazgos futuros de vulnerabilidades.

**Factor de Innovación**

El software se diferencia de la competencia al integrar mejoras en la experiencia tanto del auditor de ciberseguridad como de los auditados, basándose en un software que ya existe pero aumentando sus características. Por un lado existe la recomendación de CWE al auditor, que soluciona un problema frecuente al no tener que buscar activamente estos elementos de manera repetitiva. Por otro lado, tanto el usuario de nuestra solución como el auditado se ven beneficiados del almacenamiento de vulnerabilidades encontradas y posterior generación de dashboard de vulnerabilidades y malas prácticas.

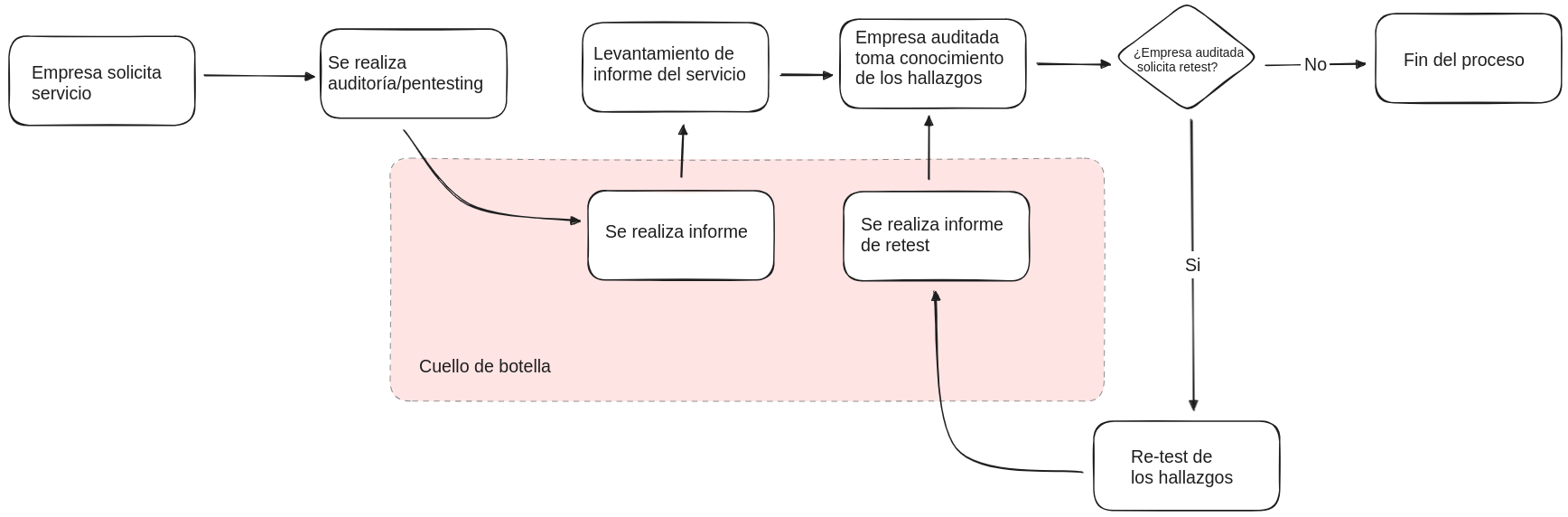
|  | Dradis | Cyver Core | PwnDoc | Nuestra solución |
| --- | --- | --- | --- | --- |
| Reportería automatizada | ✔ | ✔ | ✔ | ✔ |
| Trabajo colaborativo | ✔ | X | ✔ | ✔ |
| “Historial” de servicios (almacenamiento) | ✔ | X | ✔ | ✔ |
| Dashboard con vulnerabilidades y malas prácticas comunes del cliente | X | No, solo para los hallazgos en general. | X | ✔ |
| Recomendaciones de CWE automatizadas a través de IA | X | X | X | ✔ |

Dentro de las soluciones existentes para el problema planteado, consideramos las 17 principales aplicaciones[[4]](#footnote-3) de software según Pentest Reports. Nuestra elección en la tabla se justifica en el mayor parecido de las aplicaciones respecto a nuestra solución, donde el principal filtro fue que las empresas competidoras sean open-source.

Product Vision Board

| **Nombre del Producto:**  AuditForge | | El producto AuditForge está orientado a auditores y empresas de seguridad informática, que enfrentan el problema del gran consumo de tiempo que implica la creación de informes, lo que limita el tiempo del auditor para poder realizar pruebas y explotar vulnerabilidades de manera efectiva. Dicho problema se intensifica aún más cuando se debe trabajar colaborativamente, junto con la restricción de políticas anti nube (las cuales no permiten compartir datos de clientes con terceros). Esta problemática se resuelve mediante el uso de nuestro software, el cual brinda a los usuarios la posibilidad generar informes de forma automatizada sin la necesidad de utilizar servicios de internet y sin la preocupación de utilizar herramientas de terceros, resguardando así la confidencialidad de los datos manejados. Lo anterior permite la aceleración del proceso de generación de informes, reduciendo el tiempo total dedicado al proyecto, optimizando así el proceso y servicio de auditoría. Nuestra solución se diferencia de Dradis, Cyver Core y PwnDoc por proveer las funcionalidades de un Dashboard con información segregada por clientes, como también las recomendaciones de CWE automatizadas a través de IA, por otra parte posee un valor agregado relevante dentro del negocio, como lo es ser un software de código abierto. | | |
| --- | --- | --- | --- | --- |
| Ojo  **Segmento Objetivo** | | Advertencia  **Necesidades** | Engranajes  **Funcionalidades** | Diana  **Beneficios** |
| **Usuarios:**  Auditores de ciberseguridad  Bug Hunters  Freelancers | | * Reducción de tiempos en la generación de informes. * Almacenamiento de datos para posterior analítica. * Posibilidad de trabajo colaborativo. | * Automatización en la generación de informes. * Poseer dashboard con información de los clientes auditados. * Trabajo colaborativo en la generación de informes. | * Facilidad de uso, realizando la generación de informe de forma intuitiva y eficaz. |
| **Cliente:**  Bug Hunters  Empresas de auditoría | | * Aumento de la productividad. * Aumento de la satisfacción de clientes auditados. * Cumplimiento de políticas anti nube. | * Dashboard de clientes que han sido auditados. | * Open Source para garantizar la seguridad de los datos del cliente. |
|  | **Identificar el problema** | La generación de reportes (en el contexto de auditorías de ciberseguridad) es algo tedioso y toma tiempo de manera excesiva, que puede tener requerimientos de confidencialidad total (políticas anti nube), carece de colaboratividad en su desarrollo y al hacerse de forma manual dificulta el almacenamiento de datos acerca de los mismos. | | |
|  | **Fundamentar la Innovación** | El servicio permitirá mejorar los tiempos de desarrollo de informes, sin la necesidad de utilizar servicios de internet (manteniendo confidencialidad de los datos), sin la preocupación de utilizar herramientas de terceros imposibles de auditar (al ser open source) y aumentando la facilidad de uso, con herramientas desarrolladas para agilizar aún más la velocidad de generación de reportes y la posterior analítica de datos. | | |

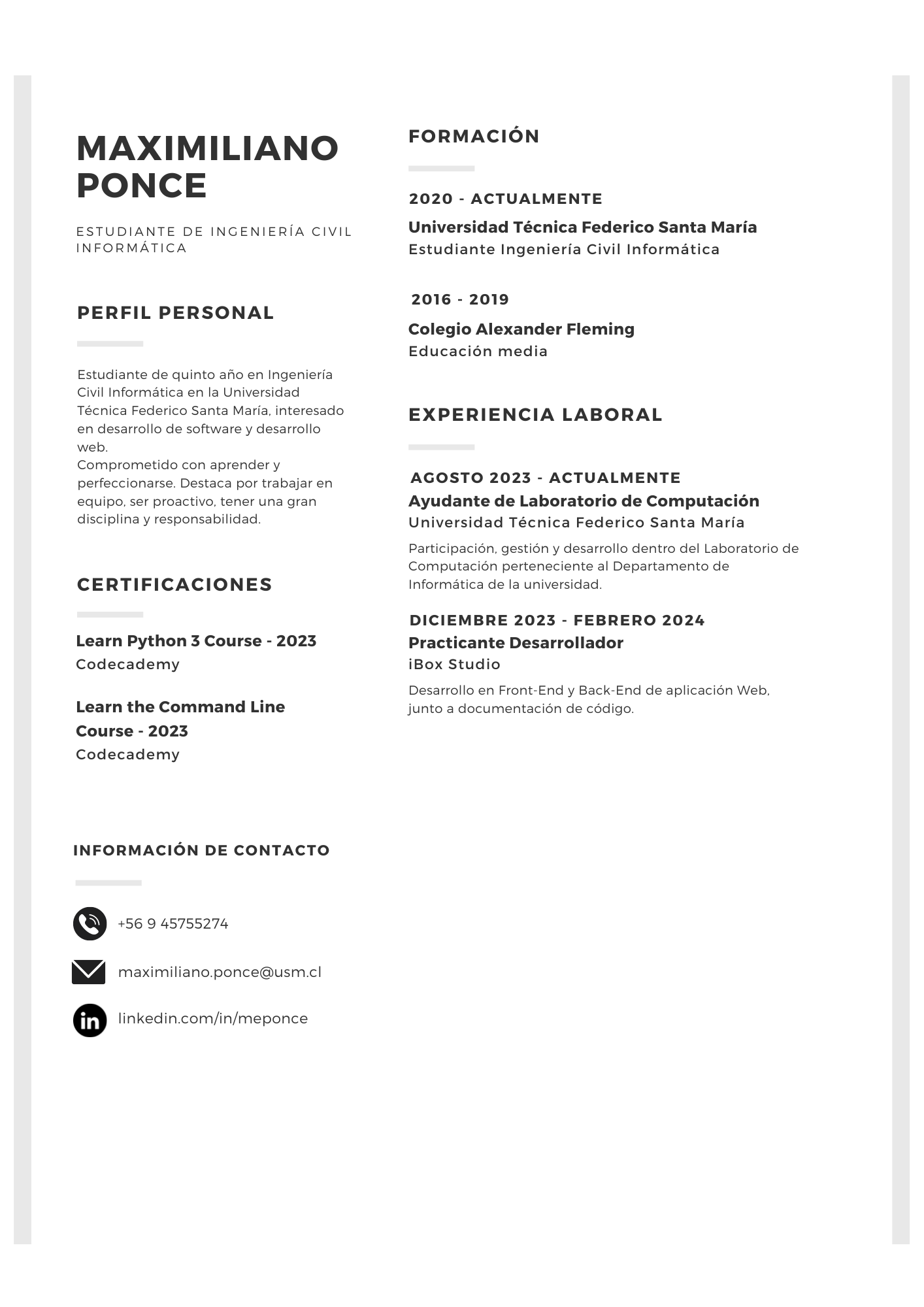
ANEXO 1















1. [Pentest Reporting Tips: Spend Less Time on Reports](https://core.cyver.io/pentest-reporting-tips-spend-less/) [↑](#footnote-ref-0)
2. [ISC2 - Cybersecurity Workforce Study (2022)](https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196) [↑](#footnote-ref-1)
3. [Penetration Testing Market Size, Share | Growth Report [2032]](https://www.fortunebusinessinsights.com/amp/penetration-testing-market-108434) [↑](#footnote-ref-2)
4. <https://pentestreports.com/software/> [↑](#footnote-ref-3)