

Santos Gallegos

Ingeniero de Software y de Seguridad de Aplicaciones



¡Hola! Soy Santos Gallegos, soy de Ecuador 🇪🇨. Me apasiona el desarrollo web, algoritmos, Python, Rust, Neovim, ciberseguridad, y el software libre y de código abierto. Siempre estoy entusiasmado por aprender cosas nuevas, cuando no estoy trabajando me gusta leer, ver películas, dibujar y pintar.

Descripción general

Actualmente trabajo en [Read the Docs](#) como desarrollador backend e ingeniero de seguridad de aplicaciones, en mi tiempo libre también trabajo como desarrollador Rust freelancer, y pentester para varias empresas. He participado en varias competencias de programación, CTFs y hackathons, también contribuyo activamente a proyectos de código abierto, y reporto vulnerabilidades de seguridad por diversión y en programas de bug bounty.

Además, ayudo a organizar eventos en mi comunidad local de Python, [Python Ecuador](#), y he dado varias charlas sobre Python, código abierto y ciberseguridad.

A continuación puede encontrar una descripción más detallada de mi experiencia profesional y habilidades.

La versión más actualizada de este documento se puede encontrar en <https://stsewd.dev/cv/es/>.

Información de contacto

Prefiero ser contactado por email, pero también puedes encontrarme en LinkedIn.








- **Email:** stsewd@proton.me
- **LinkedIn:** <https://www.linkedin.com/in/stsewd/>

Idiomas

Idiomas que domino:

- **Inglés** - *fluido*
- **Español** - *nativo*

Tabla de contenidos

-  [Experiencia profesional](#)
-  [Concursos](#)
-  [Charlas y eventos](#)
-  [Conocimientos y habilidades técnicas](#)
-  [Vulnerabilidades de seguridad públicamente divulgadas](#)
-  [Proyectos y contribuciones de código abierto](#)
-  [Encuéntrame en Internet](#)

Experiencia profesional

- **Read the Docs, Inc:** Desarrollador de software y ingeniero de seguridad (2018 - presente)

Durante mi tiempo en Read the Docs he trabajado en varios proyectos y he trabajado en varios componentes del código. Principalmente como desarrollador backend usando Django, pero también un poco de frontend, algunas de las cosas en las que he trabajado son:

- Soporte para buscar todas las páginas de documentación y acceso por usuario usando Elasticsearch y Django REST Framework
 - Validación y análisis del archivo de configuración
 - Sirviendo y almacenando en caché la documentación usando nginx, S3 y Cloudflare
 - Construcción y diseño de APIs usando Django REST Framework
 - Optimizando y mejorando el rendimiento de la aplicación
 - Desarrollo y mantenimiento de extensiones de Sphinx
 - Soporte de dominios personalizados usando Cloudflare
 - Autenticación y autorización para páginas de documentación mediante tokens y contraseñas
 - Webhooks y reglas de automatización para eventos de la aplicación
 - Logs de seguridad de usuarios y organizaciones
 - Invitaciones de usuarios a organizaciones y proyectos.
 - Identificación y remediación de varios problemas de seguridad en la aplicación
 - Mejoré la funcionalidad de redirects permitiendo wildcards, orden explícito y más
 - Consolidación de varios repositorios públicos y privados en uno
- **CB Cooperativa:** Auditoría de seguridad informática (2023)

Pruebas de penetración de su aplicación web, aplicación móvil y sistema bancario central.

- **Desarrollador Rust freelancer:** (2022 - 2023)

Durante los últimos años he estado aprendiendo Rust, y en 2022 tuve la oportunidad de trabajar como freelancer en un sistema de gestión de transporte para una empresa alemana, usando servicios de AWS como DynamoDB, Lambdas y S3.

- **CB Cooperativa:** Auditoría de seguridad informática (2022)

Pruebas de penetración de su aplicación web, aplicación móvil y sistema bancario central.

- **Telconet S.A:** Programa privado de bug bounty (2022)

Después de participar en varios CTFs, fui invitado a participar en un programa privado de bug bounty por Telconet, durante el programa encontré y reporté varias vulnerabilidades de seguridad.

- **Impodirect, CIA LTDA:** Auditoría de seguridad informática (2021 - 2022)

Pruebas de penetración de su aplicación web, y servidores.

- **CB Cooperativa:** Auditoría de seguridad informática (2020)

Pruebas de penetración de su aplicación web, servidores y sistema bancario central.

Concursos

De vez en cuando me gusta participar en competencias de programación, hackathons y CTFs. A continuación se encuentran algunos de los principales en los que he participado:

- **Devsu Code Jam:** 7mo lugar, categoría profesionales (2019)

Devsu Code Jam es una competencia de programación organizada por Devsu, donde estudiantes y profesionales compiten individualmente para resolver un conjunto de problemas de programación/algorítmicos.

La competencia tuvo dos etapas y dos categorías (estudiantes y profesionales), la primera etapa fue en línea y la segunda etapa fue presencial. De 1760 participantes de la etapa en línea, se seleccionaron 100 para participar en la etapa presencial (50 de cada categoría). En esta competencia obtuve el 7mo lugar en la categoría de profesionales.

- **IEEEXtreme Programming 11.0:** 1er lugar a nivel nacional (equipo trivialbox) (2017)

IEEEXtreme programming es una competencia mundial de programación de 24 horas, donde equipos de hasta 3 estudiantes de diferentes universidades compiten para resolver un conjunto de problemas de programación/algorítmicos. Esta fue mi tercera y última vez participando en esta competencia (ya que ya no estoy en la universidad), obtuvimos el 1er lugar de todos los equipos en Ecuador.

- **IEEEXtreme Programming 10.0:** 1er lugar a nivel nacional (equipo trivialbox) (2016)

IEEEXtreme programming es una competencia mundial de programación de 24 horas, donde equipos de hasta 3 estudiantes de diferentes universidades compiten para resolver un conjunto de problemas de programación/algorítmicos. Esta fue mi segunda vez participando en esta competencia, obtuvimos el 1er lugar de todos los equipos en Ecuador.

- **Rally Latinoamericano de Innovación:** 1er lugar a nivel local (Cuenca) y nacional (Ecuador) en la categoría de innovación (equipo Atuk Maskhay)

(2016)

Hackathon para promover la innovación abierta y el emprendimiento en los estudiantes, donde equipos de hasta 10 estudiantes y mentores compiten para presentar un proyecto innovador en 28 horas. Mi equipo obtuvo el 1er lugar en la categoría de innovación de todos los equipos en Cuenca y Ecuador. Presentamos un proyecto para construir casas sostenibles usando botellas de plástico recicladas.

- **Hackaton UPS:** 2do lugar (equipo trivialbox) (2016)

Hackathon organizado por la Universidad Politécnica Salesiana, donde equipos de hasta 4 estudiantes compiten para presentar un proyecto innovador en 24 horas. Esta fue mi primera vez participando en un hackathon, obtuvimos el 2do lugar de todos los equipos, presentamos un proyecto para ayudar a conectar a las personas que necesitan ayuda (como cruzar la calle) con personas cercanas que pueden ayudarlos.

- **IEEEXtreme Programming 9.0:** 3er lugar a nivel nacional (equipo EnigmaT) (2015)

IEEEXtreme programming es una competencia mundial de programación de 24 horas, donde equipos de hasta 3 estudiantes de diferentes universidades compiten para resolver un conjunto de problemas de programación/algorítmicos. Esta fue mi primera vez participando en esta competencia, obtuvimos el 3er lugar de todos los equipos en Ecuador.

Charlas y eventos

Ayudo a organizar varios eventos en mi comunidad local, incluyendo:

- [Meetups de Python Ecuador](#)

- [Hacktoberfest Cuenca](#)
- [Django Girls Cuenca](#)

También he dado varias charlas en meetups y eventos locales (principalmente en español):

- [Reportando vulnerabilidades en proyectos Open Source](#) - Día de la Seguridad Informática, Cuenca (2023)
- [Ciclo de vida de un proyecto FLOSS](#) - FLISoL Quito y Loja (2023)
- [Introducción al software libre y de código abierto](#) - Hacktoberfest Cuenca (2022 y 2018)
- [Impulsa tu carrera con Open Source](#) - Meetup de JavaScript Ecuador (2021)
- [Search the Docs - Elastic Search at Read the Docs](#) - Meetup de Elastic San Diego (2021)
- [Escribiendo Documentación con Sphinx](#) - FLISoL Ecuador Online (2020)
- [Resolución de problemas y competencias de programación](#) - Universidad de Cuenca (2019)
- [Open Source no es gratis. Porqué debería importarte](#) - FLISoL Cuenca (2019)
- [Viajando en el tiempo con Git](#) - Meetup de Python Ecuador (2018)
- [Introducción a Neovim](#) - Meetup de Python Ecuador (2018)
- [Comprensión de listas](#) - Meetup de Python Ecuador (2017)



Conocimientos y habilidades técnicas

Esta es una lista no exhaustiva de las tecnologías/herramientas/habilidades que uso activamente y tengo experiencia:

- **Lenguajes de programación**
 - Python
 - Rust
 - C
 - JavaScript
 - Lua
 - Bash
- **Herramientas generales**
 - AWS
 - S3
 - Linux
 - Git
 - GitHub
 - GitLab
 - Vim/Neovim
- **Habilidades generales**
 - Software libre y de código abierto
 - Mantenedor de proyectos de código abierto
 - Ciberseguridad
 - Pruebas de penetración
 - Algoritmos
 - Estructuras de datos
 - Resolución de problemas
 - Línea de comandos
 - Bash scripting
 - Automatización de procesos
 - Desarrollo web
- **Frameworks web**
 - Django
 - Django REST Framework

- Celery
- **Bases de datos**
 - PostgreSQL
 - SQLite
 - Redis
 - DynamoDB
 - Elasticsearch
- **CI/CD**
 - Docker
 - GitLab CI
 - GitHub Actions
 - CircleCI
 - Codecov
- **Testing**
 - pytest
 - unittest
 - coverage
- **Documentación**
 - Sphinx
 - reStructuredText
 - Markdown
- **Pruebas de penetración**
 - OWASP ZAP

Vulnerabilidades de seguridad públicamente divulgadas

He reportado varias vulnerabilidades de seguridad de forma responsable; algunas de las públicas se listan a continuación.

- **Denial of service via regular expression in Django Wiki** - [GHSA-wj85-w4f4-xh8h](#) (2024)

Esta vulnerabilidad podría haber permitido a un atacante causar una condición de denegación de servicio creando un artículo malicioso que tomaría mucho tiempo en procesarse.

- **CAS session takeover in Read the Docs for Businesses** - [GHSA-pw32-ffxw-68rh](#) (2024)

Esta vulnerabilidad podría haber permitido a un atacante secuestrar un tipo específico de sesión de usuario, dada una URL creada. Explotar esta vulnerabilidad habría requerido que el usuario tenga habilitada la funcionalidad de pull requests previews siguiera un enlace malicioso, lo que permitiría al atacante robar el ticket CAS utilizado para autenticar al usuario hacia varias APIs de solo lectura.

■

- **XSS in search integrations when including search results from malicious projects in Read the Docs** - [GHSA-qhqx-5j25-rv48](#) (2024)

Esta vulnerabilidad podría haber permitido a un usuario malicioso ejecutar código JavaScript arbitrario en la página de resultados de búsqueda de cualquier proyecto que incluyera resultados de búsqueda de un proyecto malicioso. Esta vulnerabilidad estaba presente en tres integraciones de proporcionadas por Read the Docs.

- **Creation of integrations for any project in Read the Docs** - [GHSA-45hq-g76r-46wv](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso crear integraciones que no requieren validación del payload para cualquier proyecto. Esta integración podría haber sido usada para realizar compilaciones a versiones existentes, crear versiones

externas, y actualizar el identificador de la versión predeterminada del proyecto bajo ciertas circunstancias.

- **Arbitrary command execution on Windows in Vim** - [CVE-2023-4736](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso ejecutar comandos arbitrarios en sistemas Windows engañando al usuario para que abra un archivo con Vim desde un directorio no confiable.

- **Untrusted search path on Windows systems leading to arbitrary code execution in GitPython** - [CVE-2023-40590](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso ejecutar código arbitrario en sistemas Windows engañando al usuario para que ejecute GitPython desde un directorio o repositorio no confiable.

- **Blind local file inclusion in GitPython** - [CVE-2023-41040](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso cargar archivos arbitrarios del sistema, esto se puede usar para verificar si un archivo existe o no, o causar una denegación de servicio leyendo un archivo grande.

- **Arbitrary write to files from builder server in Read the Docs** - [GHSA-v7x4-rhpg-3p2r](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso escribir en cualquier archivo al que la aplicación tenga acceso de escritura. El contenido que se puede escribir no está completamente controlado por el atacante, por lo que el impacto de este ataque es limitado.

- **Write access to projects via API V2 for any logged-in user in Read the Docs** - [GHSA-rqfv-8rrx-prmh](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso usar la API v2 para crear, actualizar y eliminar cualquier proyecto en la versión comunitaria de Read the Docs. En Read the Docs for Business, el usuario malicioso necesita pertenecer a la organización del proyecto objetivo para explotar esta vulnerabilidad (a cualquier equipo de la organización con al menos acceso de lectura).

- **CAS session hijacking in Read the Docs for Businesses** - [GHSA-4mgr-vrh5-hj8q](#) (2023)

Esta vulnerabilidad podría haber permitido a un atacante secuestrar un tipo específico de sesión de usuario, dada una URL creada. Explotar esta vulnerabilidad habría requerido que el usuario siguiera un enlace malicioso, lo que permitiría al atacante robar el ticket CAS utilizado para autenticar al usuario hacia varias APIs de solo lectura.

- **Serving content from pull requests previews on main docs domains in Read the Docs** - [GHSA-h4cf-8gv8-4chf](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso servir contenido arbitrario en el dominio principal de sitios de documentación.

- **Cache poisoning: serving arbitrary content on documentation sites in Read the Docs** - [GHSA-mp38-vprc-7hf5](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso servir contenido arbitrario en sitios de documentación sin tener acceso a estos.

- **Arbitrary code execution when using treesitter with injections in Neovim** - [GHSA-6f9m-hj8h-xjgj](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso ejecutar código arbitrario en el sistema de la víctima al abrir un archivo con Neovim.

- **Path traversal: access to files from any project in Read the Docs** - [GHSA-5w8m-r7jm-mhp9](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso acceder a archivos de documentación de cualquier proyecto dado su identificador, independientemente de los permisos de usuario. Esto fue posible usando una URL que puede sobrepasar las protecciones de path traversal.

- **Symlink following: arbitrary file access from builder server in Read the Docs** - [GHSA-hqwg-gjqw-h5wg](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso acceder a cualquier archivo al que la aplicación tenga acceso de lectura. Explotar esta vulnerabilidad requiere crear enlaces simbólicos que apunten a archivos fuera de la raíz del proyecto.

- **Cache poisoning in Read the Docs** - [GHSA-7fcx-wwr3-99jv](#) (2023)

Esta vulnerabilidad podría haber permitido a un usuario malicioso servir contenido arbitrario en sitios de documentación sin tener acceso a estos.

- **Arbitrary command execution in simple-git** - [CVE-2022-25860](#) (2022)

- **Symlink following: arbitrary file access from builder server in Read the Docs** - [GHSA-368m-86q9-m99w](#) (2022)

Esta vulnerabilidad podría haber permitido a un usuario malicioso acceder a cualquier archivo al que la aplicación tenga acceso de lectura. Explotar esta vulnerabilidad requiere crear enlaces simbólicos que apunten a archivos fuera de la raíz del proyecto.

- **Allow serving of arbitrary HTML files from the main domain in Read the Docs** - [GHSA-98pf-gfh3-x3mp](#) (2022)

Esta vulnerabilidad podría haber permitido a un usuario malicioso servir archivos HTML arbitrarios desde el dominio principal de la aplicación (readthedocs.org/readthedocs.com).

- **CSRF from documentation domains in Read the Docs** - [GHSA-3v5m-qmm9-3c6c](#) (2021)

Esta vulnerabilidad podría haber permitido a un usuario malicioso obtener información confidencial de un usuario autenticado en readthedocs.org/readthedocs.com creando un sitio malicioso en readthedocs.io/readthedocs-hosted.com o en cualquier dominio registrado en la plataforma.

- **Serving arbitrary files in domains of other projects in Read the Docs** - [2.3.0 release](#) (2018)

Esta vulnerabilidad podría haber permitido a un usuario malicioso servir archivos arbitrarios en los dominios de otros proyectos al agregar un proyecto como traducción del proyecto objetivo.

Proyectos y contribuciones de código abierto

Una lista de algunos de los proyectos de código abierto que he creado, ayudado a mantener o contribuido de manera sustancial.

- **Read the Docs** - core developer

Read the Docs es una plataforma de alojamiento de documentación. Soy desarrollador principal y actualmente trabajo para la compañía.

- **GitPython** - contribuidor

Librería de Python usada para interactuar con repositorios Git. He contribuido con correcciones de errores y ayudado a identificar y remediar vulnerabilidades de seguridad. [Ver todas las contribuciones.](#)

- **nvim-treesitter** - contribuidor y ex-core maintainer

Integración de la librería de análisis sintáctico tree-sitter para Neovim. Fui un contribuidor temprano y mantenedor principal, ayudé a agregar soporte para nuevos lenguajes y mejorar varias características. [Ver todas las contribuciones.](#)

- **tree-sitter-query** - contribuidor

Grammar del lenguaje Query para tree-sitter, he contribuido agregando nuevas características y corrigiendo errores. [Ver todas las contribuciones.](#)

- **tree-sitter-python** - contribuidor

Grammar del lenguaje Python para tree-sitter, he contribuido agregando nuevas características y corrigiendo errores. [Ver todas las contribuciones.](#)

- **Python Ecuador** - autor y core maintainer

Sitio web principal de la comunidad Python Ecuador. Soy mantenedor principal y ayudé a construir el sitio web.

- **rstcheck** - contribuidor

Linter para reStructuredText. He contribuido agregando nuevas características y corrigiendo errores. [Ver todas las contribuciones.](#)

- **nox** - contribuidor y ex-core maintainer

Automatizador de pruebas flexible para Python, alternativa a tox. Fui un contribuidor temprano y ayudé a agregar nuevas

características y corregir errores. [Ver todas las contribuciones.](#) .

- **fzf-checkout.vim** - autor

Extensión de Vim para administrar ramas y tags de Git con fzf. Soy el autor y mantenedor.

- **gx-extended.vim** - autor

Extensión de Vim para extender el comando `gx` para abrir URLs, archivos y más. Soy el autor y mantenedor.

- **sphinx.nvim** - autor

Integración de Sphinx para Neovim. Soy el autor y mantenedor.

- **spotify.nvim** - autor

Integración de Spotify para Neovim. Soy el autor y mantenedor.

- **tree-sitter-rst** - autor

Grammar del lenguaje reStructuredText para tree-sitter. Soy el autor y mantenedor.

- **tree-sitter-comment** - autor

Grammar de anotaciones de comentarios para tree-sitter. Soy el autor y mantenedor.

- **ieee-pandoc-template** - autor

Template de Pandoc para artículos IEEE. Soy el autor y mantenedor.



Encuéntrame en Internet

- **GitHub:** <https://github.com/stsewd>
- **GitLab:** <https://gitlab.com/stsewd>
- **Hackerone:** <https://hackerone.com/stsewd>
- **Hackerrank:** <https://www.hackerrank.com/stsewd>
- **HackerEarth:** <https://www.hackerearth.com/@stsewd>
- **Stack Overflow:** <https://stackoverflow.com/users/5689214/>
- **LinkedIn:** <https://www.linkedin.com/in/stsewd/>
- **Personal blog:** <https://stsewd.dev>
- **Email:** stsewd@proton.me *(Prefiero ser contactado por email)*