



## Desafío Tecnológico en Ciberseguridad, 2024

29/04/2024

Dentro de la **Cátedra de Ciberseguridad CiberUGR** (#CátedrasCiber\*, #NextGenerationEU\*), circunscrita al **convenio C025/24 entre el INCIBE y la UGR**, orientada a la formación y divulgación en Ciberseguridad, se contempla la actividad **Desafío Tecnológico en Ciberseguridad**, para la promoción y captación de talento joven que permita afrontar con garantías los numerosos retos presentes y futuros en el ámbito de la Ciberseguridad.



- **Retos:**

El objetivo de esta actividad es la implementación de herramientas de seguridad que muestren soluciones viables al planteamiento de un cierto reto.

Dada la gran variedad de retos existentes en el campo de la Ciberseguridad, a través del presente Desafío se hace un **planteamiento abierto** de cara a una amplia participación. En este sentido, las especificaciones a cumplir por los participantes son:

- Desarrollo de una aplicación software funcional para plataformas **Windows, Linux o Android**.
- El lenguaje de desarrollo puede ser cualquiera: **Java, Python, C,...**
- Deben requerirse los mínimos permisos/privilegios necesarios para su adecuada ejecución y operación.
- La funcionalidad a realizar debe enfocarse en alguno de los objetivos siguientes:
  1. Estimación del **nivel de seguridad de dispositivo de usuario** (smartphone, laptop, sobremesa, ...) pudiéndose tener en cuenta

aspectos tan diversos como aplicaciones instaladas, versiones software utilizadas, vulnerabilidades conocidas, actividad del usuario, comunicaciones habidas, etc.

2. Servicio para la **configuración remota e inteligente de reglas de cortafuegos**, de manera que un sistema sea fácilmente reconfigurable en cuanto a los accesos permitidos ante la posible constatación de eventos peligrosos.
3. Sistema inteligente para la **caracterización de ataques de denegación de servicio (DoS)**, de modo que resulte relativamente sencillo la aplicación posterior de filtros DoS eficaces en servicios finales como web.
4. Plataforma de **gamificación para la formación en ciberseguridad**, de manera que se permita la concienciación y formación social en ciber en especial entre los más jóvenes.
5. **Sistema anti-phishing y/o anti-spamming**, orientado a filtrar el correo electrónico para el bloqueo de mensajes maliciosos de tipo phishing y/o spamming.

- **Equipos y fechas de desarrollo:**

El desarrollo del reto elegido será **del 6 al 15 de mayo 2024**, como actividad en el marco del Día de la ETSIIT, pudiéndose realizar esta en **grupos de hasta 3 estudiantes** de la ETSIIT-UGR (de Grado o de Máster).

La **inscripción** de los equipos se realizará a través de [este enlace](#), y la **documentación** a entregar como evidencia final de lo desarrollado será la siguiente:

- Aplicación para instalar y ejecutar en el equipo correspondiente, conforme a las instrucciones precisas que se proporcionen.
- Memoria breve pero clara donde se describa el diseño, funcionalidad y uso de la herramienta desarrollada.
- Vídeo de hasta 2m de duración en el que se expongan las bondades y limitaciones de la aplicación.

Las **entregas** se realizarán por email, hasta las 24:00 horas de la fecha tope antes señalada (15 mayo), a la dirección [@email](#). Para ello, se especificará como Asunto del mismo: “Desafío Tecnológico CiberUGR, 2024: Entrega” y como Cuerpo un enlace a un repositorio (Drive, Consigna UGR, ...) donde se pueda acceder a toda la

<http://catedras.ugr.es/ciberugr-incibe/>

documentación requerida.

Del mismo modo, cualquier **duda** durante el desarrollo de la actividad se puede dirigir de dos modos:

- Por email a la dirección [@email](#), especificándose como Asunto del mismo: "Desafío Tecnológico CiberUGR, 2024: Duda".
- A través del canal de Telegram [@DTCiberUGR24](#)

- **Evaluación:**

La evaluación de las entregas se realizará por parte del equipo de desarrollo de la **Cátedra de Ciberseguridad CiberUGR, INCIBE-UGR**, junto con la **Delegación de Estudiantes de la ETSIIT**, y en ella se tendrán en consideración los siguientes **criterios**:

- Funcionalidad y completitud conseguidas.
- Aporte frente a otras herramientas similares existentes.
- Calidad y sencillez de la implementación.
- Usabilidad por parte del usuario final.
- Calidad de la documentación aportada.

Todas las propuestas presentadas que sean funcionales tendrán un **diploma de participación** en el Desafío, reconociéndose como **vencedora**, con la entrega de un **trofeo**, aquella solución que sea considerada la mejor de las evaluadas.

La resolución de la evaluación será inapelable, pudiéndose quedar desierto el puesto de vencedor si se estima que ninguna de las soluciones cumple con un mínimo de funcionalidad y calidad.

----

>>>> **Equipo ganador resultante del Desafío:** 'KakiTeam': Cristóbal Merino y Manuel V. Bolaños, por su propuesta en relación al reto 3 sobre DoS <<<<<

---

\* Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiadas por la Unión Europea (Next Generation), el proyecto del Gobierno de España que traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo, para la reconstrucción económica sólida, inclusiva y resiliente tras la crisis de la COVID19, y para responder a los retos de la próxima década.

