1er Campeonato Nacional de Ciberseguridad

Presentación:

Según el informe titulado CIBERSEGURIDAD, RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE el año 2020 promovido por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), en 22 de los países evaluados se considera que hay pocas capacidades para investigar los delitos que se cometen en el ciberespacio. En este mismo informe se señala que hasta principios de 2020, solamente 12 países habían aprobado una estrategia nacional de ciberseguridad. Uno de los factores que limita el progreso de la región en materia de ciberseguridad es la ausencia de talento humano calificado. En un ranking similar realizado por Deloitte, que analiza el compromiso con la ciberseguridad por parte de 194 estados miembros de la Unión Internacional de Telecomunicaciones (ITU), el Ecuador ocupa el puesto 14 a escala regional, y el 98 en el último índice global de Ciberseguridad.

Para todos es conocido que en la última década, los ataques cibernéticos han aumentado en frecuencia, complejidad e ingenio. El problema se agrava debido al abrupto paso de millones de personas al teletrabajo originado por la pandemia mundial provocada por el COVID-19, lo cual además ha desatado una cantidad sin precedente de ciber-delitos. Tanto las personas como las instituciones están expuestas a la incertidumbre y al impredecible ecosistema del delito cibernético.

Aunque en el Ecuador se han logrado desarrollar avances significativos en esta materia, su nivel de madurez de las capacidades de ciberseguridad es inicial y formativo y ligeramente en funcionamiento. Aún se requiere de mayor trabajo en Política y estrategia, cultura y sociedad, educación, formación, capacitación y tecnología de Ciberseguridad.

Frente a estos escenarios, la empresa, industria y la academia han unido esfuerzos para organizar el primer Campeonato Nacional de Ciberseguridad, dirigido a estudiantes universitarios y especialistas, con el firme propósito de generar conciencia social sobre la seguridad de la información como motor de desarrollo sustentable, promover el talento en seguridad de la información y motivar una alta competencia, para incrementar las habilidades y competencias técnicas que favorezcan la construcción de mejores niveles de madurez de capacidades de seguridad de la información, ciberseguridad y ciberdefensa en el ciberespacio ecuatoriano y mundial.

Objetivo General

Ser el evento referente nacional y regional para estimular el aprendizaje y la sana competencia en el ámbito de la ciberseguridad, con un enfoque a las exigencias del mercado local y global, que favorezca los niveles e madurez de las capacidades de ciberseguridad en el Ecuador.

Objetivos Específicos:

1) Crear un ecosistema colaborativo de ciberseguridad entre la academia, los proveedores de soluciones, la empresa privada y los organismos estatales.
2) Contar con un marco actualizado de habilidades en ciberseguridad requeridas en el mercado local y global.

3) Contar con un framework de evaluación de habilidades de ciberseguridad.
4) Descubrir nuevos talentos y enlazarlos con la industria para futuros trabajos, proyectos y prácticas profesionales.
5) Enlazar las iniciativas de investigación en ciberseguridad de las universidades del país con las necesidades de las empresas, potenciando la creación de proyectos Universidad-Empresa de una manera más fluida.

Descripción:

- El campeonato tendrá tres categorías: pregrado, posgrado y abierto.
- Se invitará a todas las universidades del país con carreras de pregrado y posgrados afines a la ciberseguridad y al público en general.
- Los retos serán 100% prácticos, enfocados a necesidades y situaciones actuales. Dichos retos tendrán tres niveles de dificultad: básico, medio y avanzado.
- La competencia e inscripción se realizará en modalidad de equipos con un mínimo de dos (2) y un máximo de seis (6) personas. No podrán participar los miembros del comité organizador, comité técnico y ni los representantes de los auspiciantes, ni cualquier persona que haya tenido contacto directo con los retos y bases del campeonato.
- Cada equipo se podrá registrar solo en una categoría según los criterios a continuación:
  - Pregrado: Todos los miembros deben tener una matrícula activa en una carrera de pregrado en una universidad ecuatoriana.
  - Posgrado: Todos los miembros deben tener una matrícula activa en una carrera de posgrado en temáticas afines a la ciberseguridad en una universidad ecuatoriana.
  - Abierto: Cualquier grupo de personas puede participar.
- La modalidad del campeonato será 100% virtual.
- Los equipos deben cumplir los requisitos en la inscripción y durante todo el desarrollo del campeonato. En caso de incumplimiento será descalificado por resolución del comité organizador.

La Organización del Evento

Antecedentes

En el año 2019 se planteó la idea colaborativa entre las líneas de investigación en ciberseguridad de las universidades EPN, ESPE, ESPOL y algunas empresas privadas. Como resultado se lograron algunos objetivos como workshops colaborativos, prácticas profesionales, descubrimiento de nuevos talentos, y la ejecución de proyectos.

Luego de esto, nace la idea de acelerar la interacción del ecosistema de ciberseguridad, mediante un campeonato que sea el catalizador de diferentes objetivos.

Organización

La **Coorganización** de este Primer Campeonato Nacional de Ciberseguridad estará a cargo de las siguientes instituciones:

- Escuela Superior Politécnica del Litoral (ESPOL)
- Escuela Politécnica Nacional (EPN)

- Escuela Superior Politécnica del Ejército (ESPE)
- Comando de Ciberdefensa de las FF.AA. del Ecuador
- Telconet S.A.
- Syscloudsec S.A.

Para el **apoyo** de gestión, captación y difusión del evento colaborarán las instituciones siguientes:

- Asociación Ecuatoriana de Ciberseguridad (AECI)
- Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA)
- IEEE Young Professionals Sección Ecuador
- Open Web Application Security Project (OWASP)

Estructura de la Organización

Existirá un **Comité Técnico** que estará conformado por profesionales referentes con amplia experiencia en ciberseguridad. Cada miembro del comité técnico colaborará, como mínimo, con un reto práctico de cualquiera de los niveles de dificultad. En primera instancia, el listado del comité estará presente en sitio web junto con la referencia de la cantidad de retos aportados. Adicional al reconocimiento reputacional y otros beneficios intangibles de su participación, cualquier otro beneficio dependerá de los auspiciantes del evento.

Dentro del comité técnico, también se contará con un grupo de profesionales destinados al **Soporte Técnico**, cuyas funciones serán la de habilitar las plataformas necesarias para el diseño, implementación, despliegue y operación de los retos entregados por el Comité Técnico.

La organización, en esta primera edición, aceptará contar con un grupo de **auspiciantes** (máximo cinco), los cuales no tendrá ningún tipo de injerencia que no sea de dar publicidad y lo que los acuerdos de auspicio determinen en el ámbito del marketing.

Los fondos y/o donaciones entregadas por los auspiciantes, serán destinadas para los premios de los equipos ganadores, menciones de honor, reconocimientos al comité técnico y adquisición de recursos para el entorno virtual de los retos.

Disciplinas Participantes

Referente a las **áreas/temas/disciplinas de evaluación**, los retos corresponderán al desarrollo de las habilidades necesarias en el ámbito local y global. También se tomará como referencia lo ofertado y recomendado por instituciones como: SANS Institute, Offensive Security, HacktheBox, OWASP, FIRST. El desarrollo de estas habilidades técnicas permitirá que los profesionales puedan formar parte de equipos Red, Blue o Purple de ciberseguridad.

Las **áreas/temas** de evaluación, corresponde a las habilidades de los equipos: blue team, purple team y read team. A continuación, se describen los responsables de coordinación y los temas a cubrir en los diferentes retos**.**

Equipo	Temas
BLUE TEAM	- Forense de Red - Forense de Host

	- Análisis de tráfico (tiempo) - Detección de intrusos - Fortalecimiento (hardening) - Desarrollo de scripts/herramientas (Programación) - Machine learning
RED TEAM	- Ingeniería reversa y exploits - Criptografía - Mobile - Internet de las cosas (IoT) - Web - Desarrollo de scripts/herramientas (Programación) - Machine learning - WiFi - Esteganografía
PURPLE TEAM	- OSINT - Hunting - Desarrollo de scripts/herramientas (Programación) - Machine Learning - Devsecops

Los temas serán actualizados, ratificados en la primera reunión del comité técnico y se escogerá a los coordinadores por cada equipo o por agrupación de temas.

Fechas importantes

1) Difusión:18 de agosto
2) Inscripciones: 14 de septiembre
3) Fechas del torneo: 15 al 18 de octubre
4) Fechas fase final: 22 al 24 octubre