

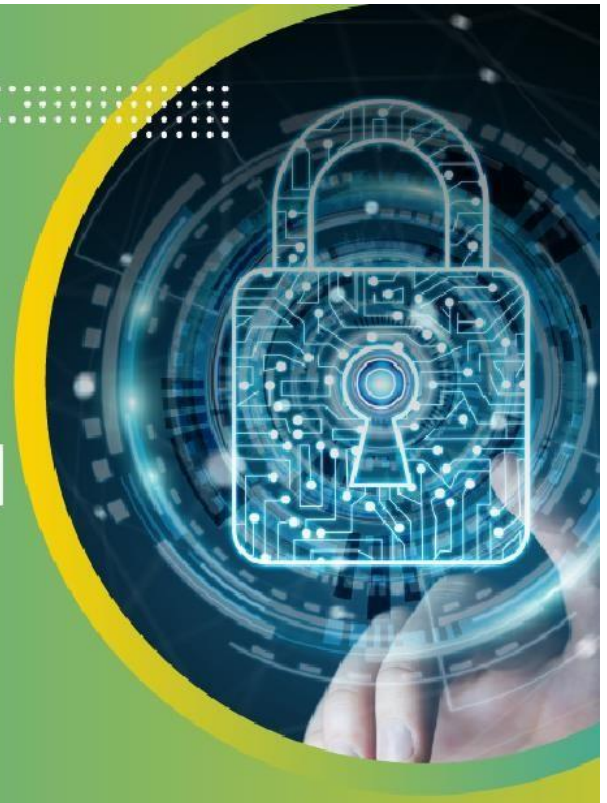


TALENTO HUMANO

FORTALEZCA SUS  
CONOCIMIENTOS A TRAVÉS  
DEL BOOTCAMP PARA

**ESPECIALISTAS EN  
CIBERSEGURIDAD**

**Y OBTENGA LA CERTIFICACIÓN  
COMPTIA SECURITY+**



**NORMAS Y CONDICIONES  
PROGRAMA DE TALENTO HUMANO**

## CONTENIDO

<b>1. INTRODUCCIÓN...</b>	<b>3</b>
<b>2. OBJETIVO.....</b>	<b>3</b>
<b>3. BENEFICIARIOS .....</b>	<b>4</b>
<b>4. REQUISITOS DE ADMISIBILIDAD.....</b>	<b>4</b>
<b>5. CRITERIOS DE EVALUACIÓN DE LOS CANDIDATOS.....</b>	<b>5</b>
<b>6. SELECCIÓN DE LOS CANDIDATOS .....</b>	<b>6</b>
<b>7. PROGRAMA DE FORMACIÓN DESGLOSADO.....</b>	<b>6</b>
<b>8. PERFIL DE SALIDA DE LAS PERSONAS BENEFICIARIAS LUEGO DE REALIZAR EL CURSO DE FORMACIÓN .....</b>	<b>7</b>
<b>9. CRONOGRAMA PARA LA EJECUCIÓN DEL PROGRAMA.....</b>	<b>9</b>
<b>10. COMPROMISO DE LA PERSONA PARTICIPANTE .....</b>	<b>9</b>

## 1. INTRODUCCIÓN

La **Estrategia de Talento Humano de PROCOTER** busca desarrollar el talento humano que requieren las empresas exportadoras y de inversión en el país con el fin de responder a la demanda existente a través de procesos de colaboración entre centros de formación, instituciones públicas y privadas y personas.

El presente documento contiene las Normas y Condiciones para que las personas interesadas puedan registrarse en el Bootcamp de formación para Especialista en Ciberseguridad, con certificación de CompTIA Security+, que se desarrolla en conjunto con el grupo corporativo YNVI- Elev8, a través de fondos del Programa Nacional de Empleo (PRONAE), en la modalidad Empléate del Ministerio de Trabajo y Seguridad Social de Costa Rica, los cuales permiten capacitar a las personas en condición de desempleo.

## 2. OBJETIVO

El Bootcamp de Especialista en Ciberseguridad es diseñado para brindar a los participantes una base de conocimientos sólida, no solo en temas fundamentales de la industria, como intrusión, detección, amenazas a la seguridad, ataques, pruebas de penetración y escaneo de vulnerabilidades, sino también en fundamentos de arquitectura como el diseño de sistemas y de infraestructura seguros, seguridad en redes cableadas e inalámbricas, criptografía y el diseño e implementación de soluciones de gestión de identidad.

La parte técnica del currículo es, predominantemente, práctica e incluye desde la ideación y la elaboración de informes, hasta la aplicación de procesos en situaciones reales. Además de las habilidades técnicas, el Bootcamp de Especialista en Ciberseguridad forma en “*power skills*” para preparar a los participantes para el éxito en un entorno profesional de trabajo. A través de las sesiones de entrenamiento, aprenderán a pensar de manera crítica, construir proyectos de varios niveles, dominar la dinámica de equipo, planificar proyectos, comunicarse de manera profesional y colaborar en equipos. Nuestro objetivo es colaborar con las vacantes que se requieren en las empresas exportadoras y aquellas interesadas en generar inversiones en nuestro país, dándole oportunidad a las personas en busca de empleo de contar con procesos de formación que les permitan cumplir con la demanda de talento existente. Además, el poder formar personas con un perfil tan buscado en diversos sectores de la industria, nos va a permitir impactar el mercado nacional y en la movilidad social de las personas.

### 3. BENEFICIARIOS

El programa está dirigido a personas en condición de desempleo, entre los 18 y 24 años, en el caso de los hombres y entre los 18 y 35 años, en el caso de las mujeres. Es importante que cuenten con Bachillerato en Educación Media concluido y que cumplan con los requisitos de admisibilidad de la sección 4.

Se recomienda que sean capaces de adaptarse a nuevas situaciones y ser flexibles ante los cambios en un entorno laboral en constante evolución. Además, que tengan capacidad de establecer metas y trabajar de manera eficiente para alcanzar resultados.

### 4. REQUISITOS DE ADMISIBILIDAD

- I. Ser mayor de edad.
- II. Disponer de una cédula nacional o de residente válida. Se solicita a la persona participante adjuntar copia del documento de identidad.
- III. Tener entre 18 y 35 años para mujeres, y entre 18 y 24 años para hombres.
- IV. Contar con un título de Bachillerato en Educación Media. Se solicita a la persona participante adjuntar copia del título de bachillerato.
- V. No estar actualmente empleado(a) ni estudiando. Se solicitará a la persona una declaración jurada que confirme la veracidad de la información.
- VI. Tener acceso a una computadora.
- VII. Demostrar un nivel mínimo de inglés B1 (Marco Común Europeo) o equivalente. Se le solicitará a la persona participante que realice una prueba diagnóstica del nivel de inglés.
- VIII. Tener disponibilidad completa para cumplir con un horario de lunes a viernes, de 8:00 a.m. a 5:00 p.m., durante un período de 4 meses en la modalidad virtual en vivo.
- IX. Completar el formulario de registro en la plataforma Charly de PROCOMER.
- X. Registrar un perfil en la plataforma ANE a través de <https://www.ane.cr>.
- XI. Estar disponible para una entrevista personal.
- XII. Estar en la disponibilidad de realizar una prueba técnica de validación de competencias necesarias para participar en el programa.

## 5. CRITERIOS DE EVALUACIÓN DE LOS CANDIDATOS

Las personas que cumplan con los requisitos de admisibilidad pasarán a la etapa de evaluación donde se considerará:

Criterio	Mecanismo de comprobación	Puntaje
La persona cuenta con un título superior al de Bachiller en Educación Media.	Se adjunta fotografía del título superior al de Bachiller en Educación Media.	<b>25 puntos</b>
La persona cuenta con un nivel superior al B1 en inglés según el Marco Común Europeo.	Prueba técnica que el centro le aplica al candidato y el resultado es superior a B1	<b>15 puntos</b>
Se evalúan 9 tecnologías (Sistemas Operativos, Desarrollo web, Backup and Recovery, Redes, Cloud computing, App Services, Virtualización, Administración de servicios, Monitoreo). Cada una de estas evaluaciones tendrá una nota y se obtiene, de todas, un ponderado que debe ser de 7, como mínimo.	Ponderado de nota 7, como mínimo, en la evaluación en 9 tecnologías.	<b>25 puntos</b>
La persona no ha recibido otra beca 100% de algún programa del gobierno.	Revisión de base de datos de PRONAE y declaración jurada del participante	<b>15 puntos</b>
La persona ha tenido experiencia en áreas STEM	Confirmación mediante la entrevista personal con el equipo Elev8	<p><b>20 puntos</b></p> <p>La persona ha trabajado en empleos relacionados en áreas STEM: <b>20 puntos</b></p> <p>La persona ha realizado prácticas, pasantías en áreas relacionadas a STEM: <b>15 puntos</b></p> <p>No cuenta con experiencia: <b>10 puntos</b></p>

Estos criterios permitirían evaluar de manera integral a los candidatos y determinar su idoneidad para participar en el programa Especialista en Ciberseguridad con certificación de CompTIA Security+ en modalidad Bootcamp.

## 6. SELECCIÓN DE LOS CANDIDATOS PARA LA FORMACIÓN

Para elegir a los candidatos beneficiarios del programa Especialista en Ciberseguridad con certificación de CompTIA Security+ en modalidad Bootcamp, PROCOMER y Elev8 realizarán la elección final para lo que se designará un equipo técnico evaluador que estará conformado por especialistas en reclutamiento del sector IT, expertos en tecnología y asesores de aprendizaje, además de un supervisor del proceso.

El comité que elige a las personas que serán beneficiarias después de la evaluación realizada, se encontrará conformado por funcionarios tanto de PROCOMER como del centro formador Elev8 según se detalla a continuación:

- a) La coordinación de la Estrategia de Talento Humano de PROCOMER o a quien este designe en su lugar.
- b) El Gerente País de Elev8 o a quien esta designe en su lugar.

Del total de candidatos que se postulen, se evaluarán únicamente los que cumplan con los requisitos de admisibilidad indicados en este documento de Normas y Condiciones.

## 7. PROGRAMA DE FORMACIÓN DESGLOSADO

El programa se dividirá en 11 módulos desarrollados en 4 meses con un total de 576 horas de formación, de las cuales 475 son de aprendizaje en competencias duras o técnicas, 64 horas de desarrollo en Power Skills y 57 horas de preparación para el examen de certificación de CompTIA Security+.

El contenido de la formación técnica contemplada en 11 módulos se detalla a continuación:

Módulo	Contenido
<b>Módulo I</b>	Sistemas Operativos e Introducción a Linux.
<b>Módulo II</b>	Linux y scripting.
<b>Módulo III</b>	Conceptos básicos e introducción a la Ciberseguridad.
<b>Módulo IV</b>	Redes y ciberseguridad
<b>Módulo V</b>	Seguridad de aplicaciones y ciberseguridad
<b>Módulo VI</b>	Recuperación ante desastres
<b>Módulo VII</b>	Ataques cibernéticos, vulnerabilidades y Mitigación
<b>Módulo VIII</b>	Gestión de vulnerabilidades y dispositivos móviles
<b>Módulo IX</b>	Gestión de incidentes y forensia.
<b>Módulo X</b>	Vulnerabilidades complejas y computación en la nube
<b>Módulo XI</b>	Pruebas de penetración, informes y resultados.
<b>Examen de certificación</b>	

## 8. PERFIL DE SALIDA DE LAS PERSONAS BENEFICIARIAS LUEGO DE REALIZAR EL CURSO DE FORMACIÓN

Después de completar el Bootcamp los participantes podrán buscar roles de soporte y administración de redes con un enfoque en la seguridad empresarial. Desarrollarán competencias en scripting de PowerShell, Linux, acceso y gestión de identidad, técnicas de ciberataques y criptografía. Esto les permitirá desarrollar funciones de seguridad en profundidad dentro de una organización, tales como:

-

- Analizar indicadores de compromiso, detectar malware e identificar diferentes tipos de ataques cibernéticos.
- Implementar controles de gestión de identidad y acceso en redes.
- Solucionar problemas comunes de seguridad o implementar dispositivos móviles de forma segura.
- Asegurarse de que la importancia de las políticas, planes y procedimientos relacionados con la seguridad organizacional se mantengan en primer plano dentro del negocio.
- Resumir conceptos seguros de desarrollo de aplicaciones, implementación, nube y virtualización para sus equipos directivos.
- Comparar y contrastar conceptos criptográficos básicos o implementar infraestructura pública crítica.
- Capacidad para identificar estrategias de ataque en redes y sistemas desarrolladas por adversarios cibernéticos y desplegar contramedidas efectivas.
- Comprender los principios de la seguridad organizacional y los elementos de las políticas de seguridad efectivas.
- Desarrollar un conocimiento en profundidad sobre los usos y la tecnología detrás de los estándares y productos criptográficos.
- Instalar y configurar tecnologías de seguridad basadas en redes y sistemas.
- Describir cómo se implementa la seguridad inalámbrica y de acceso remoto a la alta dirección y a toda la organización.
- Describir los estándares y productos utilizados para hacer cumplir la seguridad en tecnologías web y de comunicación ante la alta dirección, partes interesadas relevantes y partes de la organización según corresponda.
- Identificar e implementar estrategias para garantizar la continuidad del negocio, la tolerancia a fallos y la recuperación ante desastres.
- Identificar vulnerabilidades en aplicaciones y código, y desarrollar métodos para mitigarlos.



**Este programa permite a los participantes destacar en roles como:**

- Analista de Seguridad Operativa.
- Analista de Ciberseguridad.
- Analista de Seguridad de Aplicaciones.
- Analista de Cumplimiento.
- Analista de Puntos Finales.
- Agente de Soporte en Ciberseguridad

## 9. CRONOGRAMA DE EJECUCIÓN DEL PROGRAMA

El siguiente cuadro resume los plazos máximos para la ejecución del programa.

**Cuadro 1. Etapas del programa**

Anuncio del programa en diversos medios	14/07/2023
Cierre del formulario de inscripción	31/07/2023
Comunicación de los candidatos elegidos como beneficiarios del programa	23/08/2023
Inicio del curso de formación Especialista en Ciberseguridad-Certificación CompTIA+	4/09/2023
Finalización del curso de formación Especialista en Ciberseguridad-Certificación CompTIA+	12/01/2024

## 10. COMPROMISO DE LA PERSONA PARTICIPANTE

La persona participante se compromete, de manera voluntaria y consciente, a participar en el programa **Especialista en Ciberseguridad** que se llevará a cabo a partir de septiembre de 2023, aceptando los términos y condiciones establecidos y confirmando que cuenta con:

- Disponibilidad de tiempo de, al menos, 4 horas diarias de lunes a jueves, desde las 8:00 a.m. hasta las 12:00 p.m., para la atención y desarrollo del programa, reconociendo que el mismo se llevará a

cabo en la modalidad virtual en vivo, por lo que debe estar presente y participar activamente durante las sesiones programadas.

- Conexión a Internet estable y de calidad para poder acceder adecuadamente a las lecciones y actividades del programa, de, al menos, 30 Mbps en su lugar de residencia o en el sitio donde recibirá las lecciones. Comprende que una conexión lenta o inestable, puede afectar el éxito de su participación en el programa.
- La disponibilidad de dedicar 256 horas (4 meses) a partir de septiembre de 2023. para cumplir con el programa intensivo. La persona debe asumir la responsabilidad de administrar su tiempo de manera eficiente para poder cumplir con los objetivos y requisitos del programa dentro del plazo establecido.
- La responsabilidad de participar activamente en todas las actividades, tareas y discusiones propuestas en el programa. La participación es fundamental para obtener el máximo provecho de esta experiencia de aprendizaje y contribuir al desarrollo de un entorno de aprendizaje colaborativo y enriquecedor