

# I CONCURSO PÚBLICO 728 - 2022

## 728 N° 002 – 2022 ESPECIALISTA 3 EN CYBER HUNTER

### INTENDENCIA NACIONAL DE SISTEMA DE INFORMACIÓN

#### I. ASPECTOS GENERALES:

El proceso de selección de personal se rige de acuerdo con las [Bases de la convocatoria para la contratación bajo el régimen laboral del Decreto Legislativo N° 728 del I Concurso Público 728-2022.](#)

##### 1.1 Lugar de ejecución del proceso:

Todas las etapas del proceso de selección se ejecutarán de manera virtual de acuerdo con las fechas establecidas en el cronograma.

#### II. ASPECTOS ESPECIFICOS:

##### 2.1 Objeto de la convocatoria:

Contratar los servicios de UN (1) ESPECIALISTA 3 EN CYBER HUNTER para investigar, analizar, evaluar e identificar actividades o anomalías producidas en el entorno de red para interrumpir o eliminar las causas raíz con la finalidad de mantener la seguridad en la información.

##### 2.2 Unidad orgánica solicitante:

1U0100 - OFICINA DE SEGURIDAD INFORMÁTICA

##### 2.3 Dependencia encargada de realizar el proceso de selección:

8A1400 - División de Incorporación y Administración de Personal – INRH (DIAP).

#### III. FUNCIONES A DESARROLLAR:

1. Realizar investigaciones y análisis en las fuentes de datos disponibles, así como indicadores de ataque en busca de potenciales amenazas avanzadas que existen en la red para mantener la seguridad de la información.
2. Desarrollar y utilizar la inteligencia de amenazas para detectar, responder y vencer las amenazas persistentes avanzadas (APT) proponiendo soluciones técnicas.
3. Analizar incidentes y brindar las iniciativas de respuesta para atender el incidente de seguridad de la información identificado.
4. Elaborar, proponer y ejecutar estrategias y proyectos para construir y madurar el programa de búsqueda de amenazas desde un nivel de respuesta ad-hoc hasta un equipo de operaciones proactivo que permitan mantener la seguridad de la información.
5. Desarrollar y mejorar el marco de procesos, procedimientos y métricas de búsqueda de amenazas para que el equipo trabaje las ejecute de manera coherente y repetible.
6. Elaborar y proponer la estrategia de acción para los perfiles típicos de los actores de amenazas y sus indicadores, para desarrollar técnicas que detecten su actividad.
7. Realizar la identificación priorizada de los activos vulnerables, en coordinación con los propietarios de los activos, así como definir y elevar técnicas para detectar posibles actividades de ataque para que sean utilizadas por la unidad de organización competente.
8. Realizar coordinaciones y acciones conjuntas con otras entidades del estado y privadas a fin de consolidar esfuerzos con respecto a posibles incidentes de seguridad.
9. Apoyar en la capacitación, difusión y entrenamiento de los colaboradores de las unidades de organización competentes para la implementación de las acciones que se definan para la identificación, prevención y tratamiento de las amenazas.
10. Otras funciones que se le asignen.

#### IV. COORDINACIONES PRINCIPALES:

**4.1 Coordinaciones Internas :**  
Todas las unidades orgánicas de la SUNAT.

**4.2 Coordinaciones Externas :**  
Proveedores.

#### V. REQUISITOS DEL PERFIL DE PUESTO:

DETALLE	REQUISITOS	REGISTRAR EN "REGISTRO DE HOJA DE VIDA"
<b>Formación Académica</b>	<ul style="list-style-type: none"> <li>- Titulado Universitario en Ingeniería de Sistemas o menciones afines, o</li> <li>- Titulado Universitario en Ingeniería en Ciberseguridad o menciones afines, o</li> <li>- Titulado Universitario en Ingeniería Informática o menciones afines, o</li> <li>- Titulado Universitario en Ingeniería de Software o menciones afines, o</li> <li>- Titulado Universitario en Ciencias de la Computación o menciones afines.</li> </ul>	<i>Sección 3 "Formación Académica"</i>
<b>Conocimientos Técnicos</b>	<ul style="list-style-type: none"> <li>- Manejo de Incidentes (Detección, Análisis, Triage),</li> <li>- Caza (detección de patrones anómalos y administración de contenido) y Análisis de Malware.</li> <li>- Sistemas operativos (Windows, OS X, Linux), comprensión conceptual de Windows Active Directory con conocimiento de la red.</li> <li>- Protocolos de enrutamiento y comunicaciones (TCP, UDP, ICMP, BGP, MPLS) y aplicaciones y estándares (SMTP, DNS, DHCP, SQL, HTTP, HTTPS). Entorno Cloud.</li> <li>- Lenguajes de scripting.</li> <li>- Manejo de herramientas de Cyber Hunter, SOC.</li> <li>- Ley de datos personales.</li> </ul>	<i>Declaración Jurada de Postulación</i>
<b>Cursos o Programas de Especialización</b>	<ul style="list-style-type: none"> <li>- Curso Cazador de amenazas cibernéticas con una duración mínima de 12 horas (no acumulables) o menciones afines.</li> <li>- Curso de Etical Hacking o Hackeo Ético con una duración mínima de 12 horas (no acumulables) o menciones afines.</li> </ul>	<i>Sección 4 "Cursos o Programas de Especialización"</i>
<b>Conocimientos de Ofimática e Idiomas/ Dialectos</b>	<ul style="list-style-type: none"> <li>- Microsoft Power Point Nivel Intermedio.</li> <li>- Microsoft Excel Nivel Intermedio.</li> <li>- Microsoft Word Nivel Intermedio.</li> <li>- Inglés Nivel Intermedio.</li> </ul>	<i>Sección 6 "Conocimientos de Ofimática e Idiomas/Dialectos"</i>
<b>Experiencia (1)</b>	<p><b>General:</b></p> <ul style="list-style-type: none"> <li>- Cuatro (04) años</li> </ul> <p><b>Específica (Incluido en la experiencia general):</b></p> <ul style="list-style-type: none"> <li>- Un (01) año de experiencia específica en la identificación e implementación de contramedidas o controles de mitigación para el despliegue e implementación en el entorno de red empresarial.</li> </ul> <p><b>Nivel mínimo a ser considerado como experiencia específica:</b></p> <ul style="list-style-type: none"> <li>- ANALISTA</li> </ul>	<i>Sección 7 "Experiencia"</i>
<b>Requisitos Adicionales</b>	Disponibilidad para participar de la etapa del "Curso de Tecnología de Información INSI.	<i>Declaración Jurada de Postulación</i>
<b>Habilidades o competencias</b>	Trabajo en Equipo, Vocación de Servicio, y Orientación a Resultados.	<i>Se evaluará en la etapa de Entrevista</i>

(1) De acuerdo con lo señalado en las Bases del proceso de selección, el postulante es responsable de la información consignada en el Formato Único de Postulación, el cual tiene carácter de declaración jurada y debe encontrarse sustentado con los documentos que adjunte, caso contrario, dicha información se considera no válida. Asimismo, se indica que el tiempo de experiencia laboral se contabiliza desde la fecha de egreso de la formación correspondiente.

## VI. CRITERIOS DE EVALUACIÓN:

Los factores de evaluación del proceso de selección tienen un puntaje mínimo aprobatorio en escala vigesimal (20 puntos), distribuyéndose de esta manera:

EVALUACIONES	PESO	PUNTAJE MÍNIMO	PUNTAJE MÁXIMO
Verificación de Información Declarada	-	APTO(Cualitativo)	
Evaluación de Integridad	-	APTO(Cualitativo)	
<b>Evaluación de Conocimientos</b>			
- Prueba piloto	-	APTO(Cualitativo)	
- Aplicación de la evaluación de conocimientos	25%	13.00	20.00
Evaluación Curricular	-	APTO(Cualitativo)	
Entrevista	35%	13.00	20.00
Curso de Tecnología de Información INSI	40%	13.00	20.00
<b>PUNTAJE FINAL</b>	<b>100%</b>	<b>13.00</b>	<b>20.00</b>

## VII. CONDICIONES ESENCIALES DEL CONTRATO

CONDICIONES	DETALLE
Lugar de prestación del servicio	Sedes o establecimientos donde opera la unidad orgánica solicitante.
Modalidad de trabajo	Trabajo remoto, presencial, mixto (De acuerdo con la necesidad del servicio y las normas sobre la materia).
Duración del contrato	<b>A plazo indeterminado.</b>
Remuneración mensual	<b>S/ 7,350.00 (Siete Mil Trescientos Cincuenta Y 00/100 soles)</b> Incluyen los montos y afiliaciones de ley, así como toda deducción aplicable al trabajador.
Jornada Laboral	40 horas semanales

## VIII. CRONOGRAMA Y ETAPAS DEL PROCESO

- Las publicaciones del proceso de selección de personal se realizan en el portal web <https://unete.sunat.gob.pe/>. La institución podrá realizar comunicaciones a través de los correos electrónicos declarados por los postulantes en su Formato Único de Postulación, siendo responsabilidad del postulante la verificación de los mismos.
- Es responsabilidad del postulante realizar el seguimiento permanente de las publicaciones y mantener habilitada la cuenta de correo electrónico consignada en su inscripción en el Formato Único de Postulación, así como, gestionar que las notificaciones electrónicas enviadas no sean consideradas como correo no deseado o SPAM.
- El postulante debe contar con una conexión a internet estable para evitar inconvenientes durante el desarrollo de cada una de las etapas del proceso de selección.
- El cronograma puede estar sujeto a variaciones que se publicarán oportunamente.
- Las instrucciones de cada etapa serán publicadas con los resultados de la etapa anterior.

ETAPAS DEL PROCESO DE SELECCIÓN	FECHAS
Publicación talentoperu.servir.gob.pe y unete.sunat.gob.pe	09/03/2022 al 22/03/2022
Inscripción virtual en unete.sunat.gob.pe	Del 18/03/2022 al 22/03/2022
Verificación de Información Declarada (VID)	23/03/2022 al 24/03/2022
Publicación de resultados de la VID	25/03/2022
Evaluación de integridad	Del 26/03/2022 al 28/03/2022
Publicación de Resultados de la Evaluación de integridad	29/03/2022
Prueba piloto	Del 07/04/2022 al 13/04/2022
Resultados de prueba piloto	19/04/2022
Evaluación de conocimientos	24/04/2022
Publicación de Resultados de la Evaluación de conocimientos	05/05/2022
Evaluación curricular	Del 09/05/2022 al 13/05/2022
Publicación de resultados de evaluación curricular	18/05/2022
Entrevista	Del 23/05/2022 al 27/05/2022
Resultados de entrevista	30/05/2022
<b>Curso de Tecnología de Información INSI</b>	Del 3/06/2022 al 30/06/2022
Publicación de resultados finales	08/07/2022
Suscripción de contrato	Del 11/07/2022 al 15/07/2022
Inicio de labores	<b>18/07/2022</b>

**División de Incorporación y Administración de Personal**  
**Gerencia de Gestión del Empleo**  
**Intendencia Nacional de Recursos Humanos**