



Asesor/a técnico/a en Infraestructura de Redes, Sistemas y Servicios para la Seguridad Informática

I. REQUISITOS

Escolaridad:

Estudiante avanzado/a, egresado/a o con licenciatura en Informática o Ingeniería en Sistemas, o carreras afines con experiencia comprobable en administración de sistemas o ingeniería/o de infraestructura.

Experiencia indispensable:

- Experiencia en protección de sistemas integrados, como parte de las funciones de su experiencia y/o trabajo anteriores.
- Experiencia con el uso, instalación y configuración de sistemas basados en código abierto.

Experiencia deseable:

- Al menos dos años de experiencia en puestos similares o en proyectos académicos o de otra índole con responsabilidades similares.
- Que haya colaborado o laborado con organizaciones de derechos humanos o derechos digitales, institutos y/o escuelas académicas, empresas de tecnologías o similares
- Que haya realizado voluntariado con comunidades de software libre u organizaciones sociales (o trabajos de TCU) aplicando sus conocimientos informáticos para objetivos sociales.

Principios y enfoques:

Es importante que las personas postulantes compartan nuestros principios y marco ético los cuales están disponibles en <https://www.acceso.or.cr>

Idiomas:

- Español nativo
- Inglés intermedio (verbal y escrito)

Capacidades técnicas:***Indispensables***

- Administración e implementación de servidores LAMP
- Redes (Firewall, DHCP , TCP/IP stack cabling, etc.) y DNS
- Administración de sistemas Linux

Deseables

- Conocimiento de programación en Python
- Manejo de tecnologías Proxy/Onion/VPN
- Pentesting
- Conocimientos en nubes de código abierto
- Ciberseguridad

Motivaciones profesionales:

- Especializarse en ciberseguridad / seguridad informática
- Aumentar su conocimiento informático para iniciativas de derechos digitales y derechos humanos
- Intercambiar conocimientos con pares de otras regiones del mundo sobre seguridad informática, código abierto, incidentes informáticos, derechos digitales, entre otros

Condición migratoria:

- Tener residencia permanente en Costa Rica; o DIMEX con categoría especial libre de condición con 6 meses de vigencia y/o ser costarricense.

II. RESPONSABILIDADES DEL PUESTO**Redes – Sistemas Internos**

- Diseñar, desarrollar e implementar la topología de red segura de la Fundación Acceso en colaboración con el equipo de seguridad digital.
- Dar soporte constante a la infraestructura y los servicios instalados en la red segura.

Estas responsabilidades puede incluir, pero no limitarse a:

- a) Liderar el diseño de la topología de red e infraestructura de Acceso con la participación del equipo de seguridad digital, sistematizando el diseño y elaborando el plan de traslado y migraciones de servicios existentes a la nueva infraestructura (servidores externos).
- b) Elaborar, asesorar y supervisar un plan de compra de servidores externos y conectividad.
- c) Configurar los servidores, servicios y firewall de la red e infraestructura (servidores externos).
- d) Revisar y dar mantenimiento periódico, y/o por alertas de vulnerabilidades, de los servidores, servicios y firewall.

Servicios Internos

- Brindar a Fundación Acceso información clave y soluciones a servicios internos de seguridad informática a través de acciones como estandarización, testings, monitoreo constante y asistencia a las diversas estrategias del área de seguridad digital.
- Diseñar, integrar, implementar y mantener la infraestructura de servicios que forman parte de iniciativas de seguridad informática para organizaciones de derechos humanos y personas defensoras de derechos humanos respaldados por nuestra área de seguridad digital y / o alianzas clave.

Las responsabilidades pueden incluir, pero no se limitan a:

- a) Diseñar y desarrollar funciones de seguridad informática para arquitecturas de sistemas y definir requisitos de seguridad para sistemas informáticos como servidores, estaciones de trabajo y computadoras personales
- b) Diseñar, integrar sistemas y desplegar tecnologías de seguridad informática, así como su monitoreo constante.
- c) Dar soporte y acompañamiento al personal de Acceso y personas usuarias de ser necesario, en la instalación y manejo de las herramientas desplegadas.
- d) Crear y actualizar la documentación de los sistemas y de las soluciones.

Laboratorio de Seguridad Informática

- Diseñar, integrar, implementar y mantener un servicio de laboratorio de seguridad informática. Este laboratorio está dirigido a personas defensoras digitales en América Latina y pretende brindar recursos e infraestructura para fortalecer su trabajo y conocimiento.
- Monitorear y dar soporte al servicio de laboratorio de seguridad informática.

Estas responsabilidades pueden incluir, pero no limitarse a:

- a) Implementar e integrar la arquitectura del laboratorio (a modo de ejemplo: implementar un sistema de simulación de redes y entornos de pruebas de seguridad informática).
- b) Dar soporte a personas usuarias del servicio de laboratorio de seguridad informática.
- c) Elaborar y mantener la documentación del laboratorio de seguridad informática actualizada para las personas usuarias y para Acceso.
- d) Administrar los permisos a personas defensoras digitales para el uso del laboratorio de seguridad informática.

III. OTROS CONOCIMIENTOS, COMPROMISOS Y CALIDADES

- Conocimiento sobre ataques digitales comunes a redes y sistemas informáticos
- Compromiso con los derechos humanos y derechos digitales
- Capacidad de relacionarse con múltiples y variados actores y actoras
- Habilidad para generar consensos y manejo de conflictos
- Buena redacción y ortografía
- Solidaria/o y respetuoso/a de la diversidad social, cultural, étnica, ideológica, política, económica, sexual, de género, geográfica, entre otros
- Ambientalmente consciente
- Honesta/o y franca/o
- Buena comunicación y trato con las personas
- Responsable y ordenado/a
- Capacidad de trabajar en equipo y de forma independiente
- Discreta/o y prudente
- Disponibilidad para viajar

IV. CONDICIONES LABORALES

- Tipo de puesto: Asesoría Técnica 1
- Tipo de contrato: Puesto por tiempo indefinido
- Jornada de trabajo: Tiempo completo (40 horas semanales)
- Salario bruto mensual: USD 1.645,90 (mil seiscientos cuarenta y cinco dólares con noventa centavos)
- Modalidad de trabajo: Virtual
- Jefatura directa: Coordinador Área Seguridad Digital

Nota: Se requiere presencialidad en algunos casos programados con el equipo de Acceso.

V. VIAJES E INTERCAMBIOS

La persona seleccionada para el puesto tendrá la oportunidad de viajar a Centroamérica u otras regiones (con gastos cubiertos) para:

- Participar en encuentros de Tech Exchange, Ford-Mozilla Fellows y/o Ford Technology Fellows
- Participar en encuentros, conferencias o seminarios relacionados con derechos digitales y derechos humanos a las que sea invitada Fundación Acceso

VI. CO-RESPONSABILIDADES

- Estar de acuerdo y firmar el marco ético y de principios de Acceso.
- Participar activamente en procesos presenciales y/o virtuales de evaluación y planificación de Acceso.
- Participar activamente en las reuniones virtuales del equipo de Acceso (mensuales) y del Área de Seguridad Digital (semanales).
- Colaborar y participar en procesos internos de fortalecimiento organizativo.
- Trabajar con planes operativos anuales y por resultados (hitos).

VII. DERECHOS Y BENEFICIOS

- Salud, pensión, invalidez, vejez y muerte, maternidad con la CCSS y el INS
- Aguinaldo
- Beneficio de cesantía anual
- Fondo de Salud Holística
- Fondo de Salud Ocupacional
- Feriados y vacaciones de ley
- Vacaciones adicionales: 9 días anuales
- Otros beneficios adquiridos por antigüedad y jornada laboral
- Trabajar de cerca con un equipo humano comprometido con los derechos humanos y derechos digitales presentes en Centroamérica.

VIII. ACCIONES POSITIVAS

- Acceso cuenta con políticas y protocolos relacionados con la no-discriminación de la diversidad sexual, inclusión de personas con alguna discapacidad y atención y prevención de la violencia basada en género.
- Acceso cuenta con una política de equidad de género y un reglamento contra el hostigamiento sexual.