BASES Y LINEAMIENTOS

CONCURSO MIXTO 06-2026

Reclutamiento y selección de:
Profesional en Ciberseguridad

Contenido

SISTEMA DE EMERGENCIAS 9-1-1
CAPITAL HUMANO

Tiene el agrado de invitarlo a participar en el concurso mixto 06-2026, para seleccionar la persona que ocupará el puesto de **Profesional en Ciberseguridad**.

El presente concurso **se divulgará durante diez días hábiles**, los oferentes **deberán presentar la documentación** solicitada en el punto dos del presente documento, en los días **del 14 al 28 de mayo 2026**.

Capital Humano resalta que, este documento contiene la información relevante e indispensable que debe conocer para la postulación al puesto, razón por la cual, se le solicita leer con detenimiento, de modo que NO podrá alegar desconocimiento.

1. Características del nombramiento

Puesto	Profesional en Ciberseguridad
Jornada	48 horas
Horario	Diurno
Ubicación	Oficinas del Sistema de Emergencias 9-1-1.
Ubicación organizacional	Tecnologías de Información
Tipo de contratación	Plazo indefinido [1]
Periodo de prueba	3 meses
Modalidad	Presencial
Salario Compuesto	**Salario Base ¢846.569,26**[2] Más[3]: • Anualidades

[1] Este estará sujeto a la evaluación del periodo de prueba
[2] Sujeto a ajustes semestrales de acuerdo con los decretos emitidos por el poder ejecutivo, autorizados por la Administración
[3] Se pagarán según corresponda de conformidad con la Ley 9635 “Ley de Fortalecimiento de la Finanzas Públicas” vigente

2. Requisitos del puesto

Para participar del proceso y ser considerado como candidato, deberá cumplir con los siguientes requisitos indispensables y aportar la documentación probatoria según corresponda.

2.1. Requisitos mínimos indispensables

Los requisitos mínimos para ocupar el cargo proceden del perfil del puesto de Profesional en Ciberseguridad del Sistema de Emergencias 9-1-1; los cuales comprenden:

Requisitos Académicos	Bachiller en Ingeniería en Sistemas, Ciberseguridad, Seguridad Informática o carrera atinente con la especialidad del puesto. Inglés intermedio (B2 certificado), que permita la lectura y comprensión de documentación especializada.
Requisitos de Experiencia	Tres (3) años de experiencia ejecutando actividades relacionadas con ciberseguridad o seguridad de la información.
Certificados	Certificación en ciberseguridad orientada a respuesta a incidentes o análisis de vulnerabilidades (p.ej. CEH, CC, SECURITY + o equivalente), con una fecha de emisión no mayor a tres años de la fecha del concurso. Contar con certificado de firma digital[4]

2.2. Requisitos deseables

Conocimientos en:	• Normas técnicas para la gestión y el control de las Tecnologías de Información según COBIT2019. • Conocimiento sobre gestión y gobernabilidad de tecnología, regulaciones y estándares (ISO 27001, ISO 27031, ISO 22301, ISO 31000, COSO) COBIT 2019 • Normas de control Interno para el sector público.
Requisitos legales	Incorporado y al día con sus obligaciones en el Colegio de Profesionales en Informática y Computación de Costa Rica.

[4] En caso de resultar seleccionado y no contar con el certificado, deberá realizar las gestiones correspondientes para cumplir con el requisito

2.3. Información por considerar para la presentación de la documentación.

2.3.1. PASO 1: Formulario de inscripción

Completar el formulario de inscripción al concurso: Presione aquí para ir al formulario

⚠ Importante: El formulario de Inscripción NO sustituye el envío de los documentos obligatorios detallados en el siguiente paso.

2.3.2. PASO 2: Documentos obligatorios

La persona postulante deberá completar, firmar de forma digital y enviar los siguientes documentos obligatorios:

1) Completar y firmar el anexo 2 “Nota de postulación”
2) Completar y firmar el anexo 3 “Oferta de servicios”
3) Completar y firmar el anexo 4 “Declaración de procedimientos”

Estos documentos se encuentran disponibles en la página web: Bolsa de empleo – Sistema de Emergencias 9-1-1

La persona interesada que **no tengan firma digital deberá imprimir los documentos**, completarlos y firmarlos en físico, posteriormente deben escanearlos y enviarlos adjuntos.

4) Currículum vitae actualizado.
5) Cédula de identidad vigente, por ambos lados.
6) Hoja de delincuencia, con una antigüedad no mayor a treinta (30) días naturales.
7) Copia del título (Bachiller Universitario), conforme al requisito del puesto.
8) Copia de certificación en ciberseguridad orientada a respuesta a incidentes o análisis de vulnerabilidades (p.ej. CEH, CC, SECURITY + o equivalente), con una fecha de emisión no mayor a tres años (otorgadas a partir de mayo 2023).
9) Certificación, constancia o prueba TOEIC o equivalente que demuestre el nivel de dominio del idioma inglés.
10) Certificación (es) de experiencia laboral en funciones atinentes al puesto en concurso sean en el sector público o privado. Dicha experiencia debe ser documentada mediante certificación extendida por la autoridad competente de la organización de que se trate (ej. Jefatura de recursos humanos) y contener como mínimo los siguientes datos:
    - Nombre de la organización pública o privada.
    - Nombre completo y cargo de la autoridad que certifica la experiencia

- Departamento o área de trabajo, nombre de la clase del puesto y funciones desempeñadas.
- Tiempo de experiencia total (incluir fecha de inicio y de fin, formato día/mes/año, jornada y si fuera el caso motivo de la salida).

Importante: Las certificaciones deberán contener la información necesaria, de lo contrario no serán consideradas para efectos de evaluación.

2.3.3. PASO 3: Documentos complementarios

De corresponder deberá adjuntar también:

1) Copia de la licencia de conducir tipo B-1 vigente.
2) Copia de certificación en administración de proyectos.
3) Certificación ITIL.
4) Copia de títulos o certificados de capacitación específica y atinente al puesto, correspondientes a cursos de aprovechamiento o participación realizados a partir de mayo 2023.

2.3.4. PASO 4: Forma y medio de envío

Las personas interesadas en participar deberán enviar la documentación solicitada en este apartado **en formato digital PDF**, en un archivo comprimido (.zip) y **en un solo correo electrónico** a la dirección: empleo@911.go.cr

En el Asunto del correo indicar: "Postulación CM 06-2026 seguido de su nombre y apellidos (ejemplo: **Postulación CM 06-2026, Juan Pérez Pérez**).

2.3.5. Plazo improrrogable

La fecha límite e improrrogable para la recepción de postulaciones acompañadas de los documentos necesarios (requisitos solicitados en el punto 2.3.2), será el próximo 28 de mayo 2026 a las 23:59 horas.

Solo se admitirán postulaciones que incluyan todos los documentos indicados en el apartado 2.3.2 del presente documento, y de previo al cierre del periodo de postulación. **Solo se considerarán las postulaciones completas y que cumplan estrictamente con los requisitos.** Las postulaciones **que no incluyan** la totalidad de los documentos requeridos como requisitos indispensables no serán admitidas al concurso.

No obstante, cuando se trate exclusivamente de errores materiales o formales evidentes, que no impliquen la omisión de documentos, no afecten el cumplimiento de los requisitos mínimos indispensables, ni alteren el contenido sustantivo de la postulación, la Administración podrá, de manera excepcional, motivada y bajo criterios de igualdad, otorgar un plazo razonable para su corrección.

En ningún caso procederá la subsanación respecto a la falta de documentos obligatorios, requisitos académicos, experiencia, certificaciones, firmas, plazos o condiciones esenciales establecidas en estas bases.

Se reafirma la total responsabilidad que corresponde a la persona interesada, en cuanto a la información que remitirá por la vía electrónica, en el plazo y las condiciones aquí detalladas ampliamente.

2.4. Medio para notificaciones

Todas **las comunicaciones y convocatorias** del concurso **serán realizadas mediante correo electrónico** por Capital Humano.

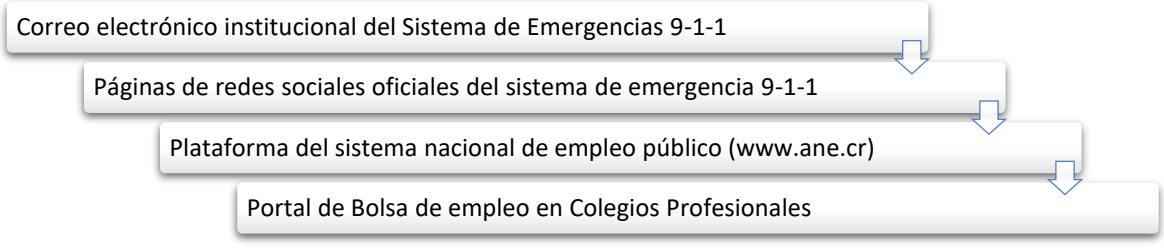
La persona postulante deberá **indicar el correo electrónico** donde desea **recibir notificaciones**, para ello debe completar el Anexo 2 “Nota de postulación”. Es responsabilidad del oferente la revisión periódica de éste.

3. Fases del procedimiento para aplicar

El proceso para reclutar y seleccionar a la persona que ocupará el puesto en concurso consta de las siguientes fases:
1. Reclutamiento,
2. Preselección,
3. Evaluación,
4. Selección y nombramiento.

3.1. Fase de reclutamiento

Esta fase tiene como propósito atraer y convocar a los candidatos que cumplan con los requisitos indispensables establecidos para ocupar el puesto objeto del concurso. Con el fin de asegurar una amplia participación y el conocimiento público del proceso, el concurso **será divulgado mínimo a través de los siguientes medios oficiales**:



3.2. Fase de preselección

Posterior a la recepción de la documentación solicitada, se realizará un proceso de preselección basado en la validación de la información proporcionada, conforme a los requisitos mínimos de admisibilidad. Aquellas personas que cumplan con los requisitos podrán avanzar a la siguiente fase del proceso y subsiguientes.

Capital Humano podrá aplicar instrumentos de evaluación técnica y práctica orientados a valorar los conocimientos técnicos específicos requeridos para el puesto, los cuales serán definidos previamente, comunicados oportunamente a las personas postulantes y aplicados bajo criterios objetivos, uniformes y verificables, garantizando el principio de igualdad y el mérito.

La fase de preselección iniciará con los siguientes criterios de admisibilidad:

I. Requisitos indispensables.
II. No le afecten las prohibiciones, impedimentos e incompatibilidades para ejercer la función pública.

3.3. Fase de evaluación

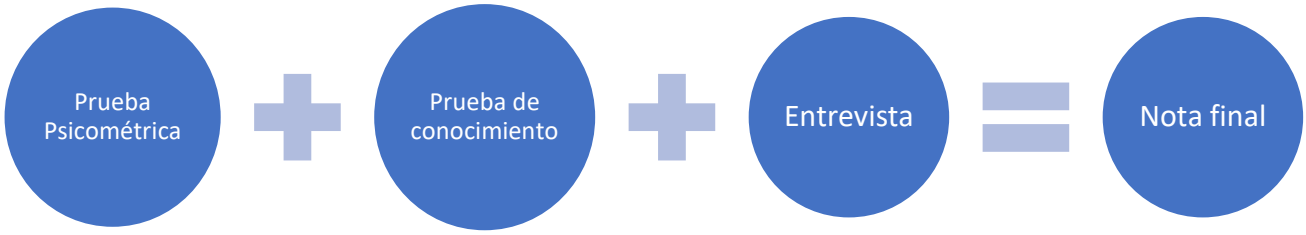
En esta fase Capital Humano realizará la evaluación de los requerimientos y conocimientos específicos solicitados, para ello, dispondrá de un plazo de 15 días hábiles a partir de la fecha de finalización de la fase de preselección, pudiendo por razones del número de postulaciones extender el plazo por uno o igual al original. Esta fase se aplicará a todos los participantes sin excepción.

FACTOR	PORCENTAJE MAXIMO ASIGNADO A FACTOR	OBSERVACIONES
EVALUACIÓN		
Pruebas psicométricas	20%	Se aplicarán pruebas psicométricas para evaluar competencias y habilidades especificas atinentes a las funciones a desempeñar. Se aplicarán a todos los participantes sin excepción.
Pruebas de Conocimiento	35%	Aplicación de prueba para la medición de conocimientos técnicos, conocimientos especializados y destrezas directamente vinculadas al cargo.
Entrevista Conductual	45%	La entrevista conductual tendrá como objetivo evaluar competencias **conductuales y técnicas** de las personas participantes vinculadas al perfil del puesto, conforme a criterios previamente definidos y aplicados de manera uniforme a todas las personas participantes.

En caso de que alguna de las personas participantes **no realice las pruebas, entrevista o se ausentara sin razón justificada** en cualquiera de las fases de este concurso, **quedará** automáticamente **excluido/a**. Es importante destacar que, en ninguna circunstancia, será posible reprogramar las pruebas o entrevista.

3.4. Cálculo de la nota

La nota final está compuesta por la sumatoria de los porcentajes obtenidos en los siguientes criterios:



4. Fase de selección y nombramiento

4.1. Elegibilidad

Se consideran elegibles aquellos oferentes que hayan alcanzado una **calificación igual o superior a setenta (70)**.

4.2. Candidatos elegibles

Una vez culminada la fase de evaluación, se trasladará los resultados finales con las calificaciones en orden descendente al Proceso solicitante para la recomendación de selección, la cual se trasladará a la Dirección para la decisión final.

En caso de empate, se tomará como criterio los conocimientos adicionales según lo siguiente:

FACTOR	PESO	PORCENTAJE MAXIMO ASIGNADO A FACTOR	OBSERVACIONES
EXPERIENCIA			
De 3 años 1 día a 5 años	5%	10%	Se considera como experiencia únicamente el tiempo laborado relacionado con la clase de puesto.
De 5 años y un día a mas	10%		

5. Recursos Oponibles

Todo recurso debe presentarse por escrito, ante el Proceso de Capital Humano, al correo electrónico atorres@911.go.cr, dentro de los plazos y bajo las condiciones que se establecen en este apartado, adjuntando, cuando corresponda, los documentos de respaldo pertinentes.

5.1. Objeciones a las bases del concurso

Los interesados podrán presentar objeción a las bases y lineamientos del concurso cuando consideren que estos contravienen el ordenamiento jurídico, los principios de legalidad, razonabilidad o igualdad de oportunidades.

- El plazo para presentar la objeción será de tres (3) días hábiles, contados a partir del día siguiente a la publicación oficial de las bases del concurso.
- La objeción deberá presentarse debidamente fundamentada y acompañada, en caso de ser necesario, de los documentos de respaldo correspondientes.
- La resolución de la objeción será comunicada al interesado mediante notificación formal.

5.2. Recursos contra actos y resultados del concurso

Contra los actos administrativos dictados durante las distintas fases del concurso, incluyendo la comunicación de resultados parciales o finales, los participantes podrán interponer los recursos administrativos previstos en la Ley General de la Administración Pública.

- El plazo para interponer los recursos será de tres (3) días hábiles, contados a partir del día siguiente a la notificación válida del acto o resultado impugnado.
- El recurso deberá indicar con claridad el acto que se impugna, los motivos de hecho y de derecho en que se fundamenta, así como la prueba pertinente, cuando corresponda.

5.3. Recurso de revocatoria

El recurso de revocatoria deberá interponerse ante el mismo órgano que dictó el acto administrativo, el cual procederá a su análisis y resolución.

5.4. Recurso de apelación

El recurso de apelación podrá interponerse en subsidio del recurso de revocatoria o de manera directa, cuando así lo permita la normativa aplicable, y será conocido y resuelto

por la Coordinación del Proceso de Soporte a la Gestión Operativa, en su condición de órgano jerárquicamente superior.

El Proceso de Capital Humano actuará, cuando corresponda, como órgano receptor e instructor del recurso, debiendo verificar el cumplimiento de los requisitos formales y remitirlo al órgano competente para su resolución.

5.5. Notificación de la resolución de los recursos

La resolución de los recursos interpuestos será comunicada al interesado mediante notificación formal, por los medios institucionales establecidos, garantizando la certeza jurídica y el adecuado cómputo de los plazos que correspondan.

5.6. Improcedencia por extemporaneidad

No se admitirán ni tramitarán los recursos que se presenten fuera de los plazos establecidos.

5.7. Normativa supletoria

En todo lo no previsto expresamente en este apartado, se aplicará de forma supletoria lo dispuesto en la Ley General de la Administración Pública (Ley n.º 6227), así como los principios generales del Derecho Administrativo.

Para obtener información acerca de este concurso favor comunicarse con la funcionaria Gidget Fajardo Vargas al teléfono 2522-2723 o al correo electrónico gfajardo@911.go.cr

¡Muchas gracias por su participación!

Firmado digitalmente
Valide las firmas digitales

Revisado por:
Auxiliadora Torres Fonseca
Coordinadora Capital Humano

6. Anexos

6.1. Perfil del Puesto

Sistema de Emergencias 9-1-1
Capital Humano
Perfil de puesto

NOMBRE DEL CARGO	Profesional de Ciberseguridad	CLASE	
UBICACIÓN ORGANIZACIONAL	Tecnologías de Información	CATEGORIA	17.1
REPORTA A	Coordinador de Tecnologías de Información	PROCESO DE TRABAJO	Ciberseguridad

OBJETIVO DEL PUESTO

Gestionar de forma integral la ciberseguridad institucional, mediante la identificación, análisis y tratamiento de los riesgos cibernéticos, la prevención, detección y respuesta a incidentes de seguridad de la información, el aseguramiento de la continuidad operativa y la resiliencia cibernética, así como el cumplimiento del marco normativo aplicable, incluyendo la protección de los datos personales, con el propósito de salvaguardar los activos de información y garantizar la continuidad de los servicios institucionales y apoyar la toma de decisiones estratégicas de la institución.

RELACIÓN DE FUNCIONES Y ACTIVIDADES DEL PUESTO

FUNCIÓN		ACTIVIDADES
Gestionar el modelo de Control de Protección de los datos, información e infraestructura tecnológica de la Institución.	1	Planificar, dirigir, coordinar y controlar las soluciones de ciberseguridad que respaldan las operaciones desde el marco de la seguridad en los entornos digitales y tecnológicos.
	2	Evaluar y gestionar los riesgos de seguridad asociados a adquisiciones de tecnología, definiendo requisitos de ciberseguridad en los procesos de contratación, evaluando arquitecturas de soluciones, revisando integraciones tecnológicas y gestionando los riesgos asociados a terceros y proveedores.
	3	Realizar la evaluación de riesgos cibernéticos a nivel organizacional, considerando servicios críticos, dependencias de terceros y proveedores, e impactos derivados de la transformación digital institucional.
	4	Diseñar, proponer e implementar las medidas y controles de seguridad de acuerdo con los riesgos detectados, incorporando el enfoque de Seguridad desde el Diseño (Security by Design) en las etapas tempranas de los proyectos institucionales.
	5	Configurar los dispositivos de la infraestructura de seguridad y solucionar los problemas que se puedan presentar.
	6	Asegurar el cumplimiento de las normativas relacionadas con la protección y almacenamiento de datos, incluyendo la recolección y gestión digital de evidencias requeridas por entes de control como la Contraloría General de la República y el MICITT.

FUNCIÓN		ACTIVIDADES
Administrar, coordinar y gestionar las Estrategias y los planes de ciberseguridad.	1	Planificar y recomendar estrategias y sistemas defensivos en contra de intrusos con base en la detección y prevención de posibles amenazas o ciberataques.
	2	Implementar protocolos capaces de contrarrestar las potenciales amenazas, integrando herramientas de seguridad para una visibilidad centralizada que facilite la toma de decisiones.
	3	Monitorear los sistemas para detectar actividades inusuales, tales como accesos no autorizados, modificaciones, duplicaciones o destrucción de información.
	4	Gestionar el ciclo completo de respuesta a incidentes de Ciberseguridad y Seguridad de la Información, comprendiendo las fases de preparación, detección, contención, erradicación, recuperación y análisis posterior, para evitar su recurrencia y fortalecer la resiliencia institucional.
	5	Ejecutar actividades de búsqueda proactiva de amenazas (Threat Hunting) dentro de la red institucional para anticipar y neutralizar riesgos antes de que se materialicen.
	6	Proponer y elaborar los procesos, políticas, procedimientos y controles sobre planes de ciberseguridad.
	7	Simular violaciones de accesos no autorizados para identificar vulnerabilidades.
	8	Participar en la definición, evaluación y prueba de Planes de Continuidad del Negocio y Planes de Recuperación ante Desastres desde la perspectiva de la ciberseguridad, coordinando acciones preventivas y de recuperación frente a ciberincidentes.
	9	Coordinar con instancias nacionales competentes en materia de ciberseguridad (CSIRT-CR, MICITT y otras autoridades regulatorias) la gestión de incidentes, el intercambio de información de amenazas y el cumplimiento de directrices nacionales.

FUNCIÓN		ACTIVIDADES
Desarrollar y mantener el SGSI (Sistema de Gestión de Seguridad de la Información).	1	Proponer y elaborar los procesos, políticas, procedimientos y controles conforme a la ISO 27001, y asegurar la revisión en intervalos planificados.
	2	Realizar y documentar la medición del desempeño de las normas aplicables al SGSI.
	3	Participar y apoyar en las auditorías internas y externas del SGSI.
	4	Mantener un inventario de todos los activos de información y coordinar con los responsables la gestión de los riesgos asociados a estos.
	5	Ejecutar y gestionar evaluaciones de riesgos sobre datos personales, apoyar técnicamente los Análisis de Impacto en Privacidad (EIPD), atender incidentes de seguridad que involucren datos personales y coordinar con la autoridad nacional competente en esta materia.
	6	Promover y fortalecer la cultura de seguridad de la información mediante el diseño e impartición de programas de capacitación y concientización institucional, fomentando un enfoque transversal de la ciberseguridad.

FUNCIÓN		ACTIVIDADES
Contribuir al logro de los objetivos institucionales mediante el desempeño eficiente, responsable y ético de sus actividades, garantizando la colaboración y el cumplimiento de las normativas vigentes	1	Cumplir con las políticas, procedimientos y normativas internas establecidos para asegurar el correcto funcionamiento y la integridad organizacional.
	2	Ejecutar oportunamente las actividades y responsabilidades encomendadas con eficiencia, calidad y respeto a los tiempos establecidos.
	3	Colaborar y mantener una comunicación abierta, clara y respetuosa para favorecer el trabajo en equipo y la consecución de objetivos comunes.
	4	Actualizar y mejorar sus conocimientos y habilidades mediante la participación en procesos de capacitación y desarrollo para contribuir al crecimiento y adaptación constante de la organización.
	5	Reportar y documentar avances, incidencias o resultados relevantes de las actividades realizadas a la jefatura, facilitando la toma de decisiones y la mejora continua.
	6	Colaborar de manera proactiva con todos los procesos de la institución dentro del ámbito de su competencia, participando en actividades y proyectos conjuntos para apoyar el cumplimiento efectivo de las metas y objetivos institucionales.
	7	Adoptar, implementar y utilizar adecuadamente las herramientas tecnológicas disponibles para optimizar la eficiencia y eficacia en la realización de las labores asignadas, contribuyendo así al mejor desempeño individual y colectivo dentro de la organización.
	8	Colaborar en la impartición de capacitaciones y procesos de inducción dentro de su área de competencia, participando activamente cuando se le asigne para favorecer la integración y actualización del personal en la organización.
	9	Participar en comisiones institucionales que le sean asignadas, aportando conocimientos y experiencia para el cumplimiento de los objetivos y compromisos de la organización.
	10	Proteger y mantener la confidencialidad, integridad y disponibilidad de la información y de los recursos tecnológicos utilizados en el desempeño de las funciones, actuando con diligencia para prevenir incidentes, reportar anomalías o vulnerabilidades y contribuir a un entorno seguro y confiable para la operación institucional.

CONDICIONES ORGANIZACIONALES

Supervisión Recibida	Sigue instrucciones generales de las jefaturas u órganos superiores respectivos , así como los métodos y procedimientos establecidos en la legislación vigente. Su labor es evaluada mediante la aplicación anual de la evaluación de desempeño conforme al cumplimiento de los objetivos y metas definidos para el puesto
Supervisión Ejercida	No le corresponde tener personal subordinado
Responsabilidad por funciones	Las actividades se deben cumplir con diligencia, imparcialidad y probidad, asumiendo plena responsabilidad por sus actos y omisiones en el ejercicio del cargo, garantizando la correcta aplicación de los recursos y el respeto a los principios del servicio público
Responsabilidad por relaciones de trabajo	En el desempeño de sus labores requiere mantener relaciones laborales respetuosas, colaborativas y éticas con superiores, pares, subordinados y otras instancias internas o externas a la institución; fomentando el trabajo en equipo, la comunicación efectiva y el cumplimiento de objetivos institucionales en un ambiente de respeto mutuo y profesionalismo

Responsabilidad por equipo y materiales	Es responsable por utilizar, custodiar y conservar de manera responsable, eficiente y adecuada los recursos, activos, equipos, materiales, sistemas informáticos y documentación asignados, velando por su uso racional y destino exclusivo para las actividades y tareas encomendadas, conforme a la normativa institucional y los principios de responsabilidad patrimonial del servidor público, con el fin de optimizar su aprovechamiento.
Condiciones de trabajo	El trabajo se ejecuta pricipalmente en un ambiente de oficina. La actividad demanda alto esfuerzo mental para el análisis de situaciones complejas, atención de incidentes, cumplimiento de plazos y adaptación constantes a escenarios de riesgos cambiantes. Es probable que por necesidad institucional requiera trasladarse fuera de la oficina.
Impacto de la gestión	Los errores cometidos pueden causar pérdidas, daños o atrasos de consideración, por lo que las actividades deben ser ejecutadas con cuidado y exactitud. Pueden perjudicar al funcionario, al proceso, problemas legales o de imagen

REQUISITOS

REQUISITOS INDISPENSABLES

Bachiller en Ingeniería en Sistemas, Ciberseguridad, Seguridad Informática o carrera atinente con la especialidad del puesto.

Certificación en ciberseguridad orientada a respuesta a incidentes o análisis de vulnerabilidades (p.ej. CEH, CC, SECURITY + o equivalente), con una fecha de emisión no mayor a tres años de la fecha del concurso.

Tres (3) años de experiencia ejecutando actividades relacionadas con ciberseguridad o seguridad de la información.

Incorporado y al día con sus obligaciones en el Colegio de Profesionales en Informática y Computación

Inglés intermedio (B2 certificado), que permita la lectura y comprensión de documentación especializada.

REQUISITOS DESEABLES

Conocimientos en:

Normas técnicas para la gestión y el control de las Tecnologías de Información según COBIT2019.

Conocimiento sobre gestión y gobernabilidad de tecnología, regulaciones y estándares (ISO 27001, ISO 27031, ISO 22301, ISO 31000, COSO) COBIT 2019

Normas de control interno para el sector público.

COMPETENCIAS

Nivel	Competencia
B	Humanismo
B	Atención efectiva
B	Orientación a resultados
B	Capacidad de análisis
B	Solución de problemas
B	Comunicación efectiva
B	Trabajo Colaborativo

CONTROL DE ACTUALIZACIONES

Elaborado por	Revisado por	Aprobado por	Rige a partir	Número de versión
Gidget Fajardo Vargas Profesional Capital Humano	Auxiliadora Torres Fonseca Coordinadora Capital Humano Carlos Leiva Mejía Coordinador Tecnologías de Información	Kathya Villar Bonilla Directora	mayo-26	01-2026

Firmado digitalmente
Valido las firmas digitales