

<b>Dependencia:</b>	Auditoría Interna	<b>Área:</b>	Auditoría Tecnología de Información
<b>Código del Cargo:</b>	3032. 02	<b>Código del Puesto:</b>	3032
<b>Categoría:</b>	22	<b>Nombre del Puesto:</b>	Ejecutivo Bancario Administrativo 3 Auditoría
<b>Nombre del Cargo:</b>	Auditor en Ciberseguridad	<b>Reporta a:</b>	Supervisor de Auditoría de Tecnología de Información

**Objetivo del Cargo:** Ejecutar labores profesionales relacionadas con la planeación, coordinación y ejecución de actividades de Auditoría a la Ciberseguridad, para evaluar el estado de la ciberseguridad en la Institución, con el objetivo de comprobar y valorar el diseño y efectividad de los controles claves, comprobar la aplicación de las mejores prácticas y estándares de la industria en ciberseguridad, emitir recomendaciones y brindar seguimiento a las mismas.

MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES
		1	Ejecutar en coordinación con el supervisor la planificación de los estudios y pruebas de Auditoría de Ciberseguridad o Seguridad de la Información que le sean asignadas.
		2	Coadyuvar en el planeamiento y la ejecución tanto de la estrategia como de los objetivos de la Auditoría Interna especialmente los relacionados con la Ciberseguridad.
		3	Aplicar una comprensión de las dependencias de tecnología, seguridad de la información y ciberseguridad de alto riesgo, incluida la defensa contra el malware, la gestión de identidades y accesos, la protección de datos, el cifrado, la seguridad de los firewalls, los sistemas de detección y prevención de intrusiones, la gestión de incidentes, la gestión de infraestructura de la red, la gestión de vulnerabilidades, la protección de servicios en la nube y las amenazas externas.
		4	Aplicar las técnicas de Auditoría adecuadas y de alto valor ético, a fin de obtener resultados tendientes a subsanar deficiencias relacionadas con la gestión de las tecnologías y seguridad de la información del Banco para fortalecer su postura.
		5	Aplicar las principales metodologías de hacking ético y pruebas de intrusión o penetración para recomendar mejoras de seguridad mediante la evaluación de la situación actual, tendencias y la alineación con políticas internas, regulaciones, mejores prácticas y estándares.
		6	Proporcionar recomendaciones prácticas para remediar las brechas identificadas en materia de Ciberseguridad y fortalecer la postura del Banco.
		7	Proporcionar recomendaciones para la actualización y mejoramiento de las guías y planes de trabajo de la Auditoría.
		8	Desarrollar los procedimientos de las guías de trabajo asignadas por el Auditor Supervisor.
		9	Preparar los papeles de trabajo apropiados en el desarrollo de Auditorías de Tecnología de Información haciendo uso de guías y herramientas tecnológicas publicadas por la Auditoría Interna, ISACA, NIST, PCI DSS, CIS, ISO u otras referencias en materia de Ciberseguridad o seguridad de la información aplicables.
		10	Cumplir con los procedimientos de trabajo establecidos en la Auditoría Interna y sugerir posibles mejoras o ajustes a los mismos.
		11	Aplicar la metodología de Auditoría Interna y las normas de calidad a todos los aspectos del trabajo.
		12	Redactar en forma clara y concisa informes y memorándum que deben ser revisados por el supervisor y la jefatura de Auditoría de T.I.
		13	Mantener un conocimiento actualizado de las amenazas de seguridad, las tendencias de la industria, las contramedidas, las herramientas, los procesos y las tecnologías de seguridad.
		14	Cumplir con la calidad y con los tiempos de respuesta establecidos para las funciones correspondientes al cargo.
		15	Colaborar en la ejecución de actividades o proyectos establecidos de alcance Institucional para la Auditoría Interna.
		16	Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.
		17	Ejecutar otras funciones propias del puesto o la Auditoría Interna.
<b>FUNCIONES ESPECÍFICAS RELACIONADAS CON RIESGO</b>			
		18	Contribuir a que se alcancen los objetivos institucionales, mediante la práctica de un enfoque sistémico y profesional para evaluar y mejorar la efectividad de la administración del riesgo, del control y de los procesos de dirección de la Institución; en cumplimiento de sus deberes y competencias según lo establece la Ley General de Control Interno.
		19	Verificar el cumplimiento, la validez y la suficiencia del sistema de control interno de su competencia institucional, informar de ello y proponer las medidas correctivas que sean pertinentes, de conformidad con el marco regulatorio que le aplica.
		20	Conocer el marco institucional de gestión de riesgos y considerar los riesgos relevantes de los procesos evaluados, durante el desarrollo de las actividades asignadas como parte del plan de trabajo de la Auditoría.
		21	Velar por una adecuada gestión de los riesgos que pueden impactar sobre el plan estratégico y el plan de trabajo de la Auditoría Interna.
		22	Velar por un adecuado desarrollo e implementación de las medidas adoptadas para el funcionamiento del sistema de valoración del riesgo de la Auditoría, garantizando una adecuada cultura de riesgo.
		23	Participar en el desarrollo, implementación y seguimiento de los planes de acción para minimizar el impacto de los riesgos propios de los procesos de la Auditoría.
		24	Promover que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
		25	En caso de materializarse un evento de riesgo es responsable de reportarlo de conformidad con lo establecido en el sistema de gestión de riesgos de la Auditoría.

CODIGO	REQUISITOS EXIGIBLES
	<b>Formación Académica:</b> Licenciatura o Maestría en Ingeniería de Sistemas, Informática, Telemática (u otra especialidad que la Auditoría requiera).
	<b>Legales:</b> Incorporado al Colegio Profesional respectivo y estar al día con sus obligaciones.
	<b>Experiencia:</b> Tres años de experiencia en labores relacionadas con evaluaciones en ciberseguridad o seguridad informática.

CODIGO	* REQUISITOS TÉCNICOS EXIGIBLES
	1. Certificación de Hackeo Ético (CEH) o Comp TIA Pentest+.
	2. Cursos Cisco Certified Networking Associate.
	3. Conocimiento de las mejores prácticas y estándares de la industria de Ciberseguridad y Seguridad de la Información.
	4. Conocimiento de los conceptos de valoración de riesgos, herramientas y técnicas en un contexto de auditoría.
	5. Conocimiento de técnicas de planificación de la auditoría y de gestión de proyectos de auditoría.
	6. Conocimiento sobre leyes, regulaciones y estándares relevantes de la Industria que regulan la actividad de la Institución.
	7. Conocimiento del gobierno, la gestión, la seguridad y los marcos de control de T.I., así como de los estándares, las directrices y las prácticas relacionadas.
	8. Conocimiento de la Arquitectura de T.I. en relación con los datos, las aplicaciones, lenguajes de programación y la tecnología (Mainframe, aplicaciones distribuidas, virtualización de centros de datos, aplicaciones basadas en la web, servicios y arquitectura en la nube (IaaS, PaaS, SaaS), servicios web, aplicaciones de n-capas, middleware, Core Bancario, aplicaciones móviles).
	9. Conocimiento en el uso y configuración de tecnologías de seguridad informática, tales como: NAC, VPN, NG Firewalls, IPS, IDS, DLP, Cifrado de Discos, WAF, SIEM, Detección de Amenazas y Malware.
	10. Conocimiento de la Ley de Contratación Administrativa, Ley General de Control Interno, Ley General de Administración Pública, Ley contra la Corrupción y el Enriquecimiento Ilícito en la función pública y otras leyes aplicables.
	11. Conocimiento en la elaboración de informes de auditoría.

\* Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares. Los requisitos técnicos exigibles serán evaluados por medio de la prueba de conocimiento que forma parte del proceso de selección.

CODIGO	REQUISITOS TÉCNICOS DESEABLES				
	1. Certificación CISA Certified Information Systems Auditor.				
	2. Certificación CSX-P—Cybersecurity Practitioner Certification de ISACA.				
	3. Conocimiento en Cybersecurity Audit Certificate Program de ISACA.				
	4. Certificación ISO/IEC 27032 Lead Cybersecurity Manager.				
	5. Certificación CompTIA Security+.				
	6. Conocimiento certificado en administración de servidores en ambientes Windows y Linux.				
	7. Conocimiento certificado en seguridad de nube, por ejemplo: Certified Cloud Security Professional - CCSP, de la (ISC)2 o Certificación de Conocimientos de Seguridad de la Nube (CCSK				
	8. Conocimiento intermedio del idioma inglés.				
CODIGO	SISTEMAS UTILIZADOS				
	Programas de Ofimática, Microsoft Office 365 o similares.				
	SIPRE.				
	SIAR.				
	Service Manager.				
	Sistema de Control de Tiempos.				
	ACL.				
	COMPETENCIAS REQUERIDAS				
	PERFIL KOMPE DISC:	PERFIL: AUDITOR JR Y SR			
CODIGO	Competencias Cardinales	D	C	B	A
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CODIGO	Competencias Gerenciales	D	C	B	A
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CODIGO	Competencias de Negocio	D	C	B	A
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CODIGO	Competencias de Negocio	D	C	B	A
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CODIGO	DISC - Personalidad	D	C	B	A
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	La Gerencia General Corporativa aprueba la creación de este perfil en categoría 22 mediante el oficio GGC-1208-2022, aprobado el 10 de octubre del 2022. Referencia DIRGC-520-2022 y DIRCH-1397-2022. Este cargo sustituye al Auditor en Ciberseguridad, categoría 21, código 3044,01.				