

<div><div></div><div>MANUAL DE CARGOS</div></div>				
Dependencia:	Auditoría Interna		Área:	Dirección Auditoría Tecnología de Información
Código del Cargo:	3032.01		Código del Puesto:	3032
Categoría:	22		Nombre del Puesto:	Ejecutivo Bancario Administrativo 3 (Auditoría)
Nombre del Cargo:	Auditor Senior 2- TI		Reporta a:	Director de Auditoría de Tecnología de la Información-ATI
Objetivo del Cargo:	Ejecutar labores profesionales relacionadas con la coordinación, evaluación, supervisión y ejecución de actividades de Auditoría relativas a los Sistemas de Información e Infraestructura Tecnológica del Banco, con el objetivo de comprobar la aplicación del sistema de control interno, emitir recomendaciones y dar seguimiento a las mismas.			
MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES	
			1. Desarrollar la planificación detallada del estudio de Auditoría partiendo de los riesgos y objetivos planteados en la asignación del trabajo.	
			2. Definir la estrategia a seguir para realizar el trabajo de Auditoría, en función de los objetivos planteados.	
			3. Tomar decisiones sobre las áreas de mayor riesgo por auditar y sobre las cuales se llevarán a cabo procesos de verificación o cumplimiento y pruebas sustantivas.	
			4. Aplicar, modificar y en caso de que no existan, confeccionar las guías de trabajo para su aplicación respectiva.	
			5. Hacer planteamientos escritos sobre los resultados de sus análisis, con miras a generar recomendaciones tendientes a subsanar deficiencias relacionadas con la gestión de las tecnologías de información en el Banco.	
			6. Brindar asistencia práctica a su equipo de trabajo ayudando a comprender los objetivos e implicaciones de éstos.	
			7. Aplicar los procedimientos de las guías de trabajo.	
			8. Preparar los papeles de trabajo apropiados en el desarrollo de auditorías en diversas áreas del Banco, haciendo uso de herramientas tecnológicas de la mayor actualidad posible.	
			9. Revisar los trabajos realizados por el resto del equipo de trabajo para verificar el cumplimiento de los programas de trabajo y de los procedimientos de la Auditoría Interna.	
			10. Aplicar las técnicas de Auditoría de TI adecuadas con miras a obtener resultados y conclusiones sobre problemas particulares y generales.	
			11. Aplicar los procedimientos de trabajo estandarizados utilizados en la Auditoría Interna y sugerir posibles mejoras o ajustes a los mismos.	
			12. Preparar los borradores de los informes producto de las evaluaciones realizadas y participar en la conferencia final de los mismos.	
			13. Desarrollar los programas de trabajo y elaborar los informes dentro del tiempo asignado por el Supervisor o la Jefatura.	
			14. Colaborar en la formulación de la planificación estratégica y en el plan anual de trabajo de la Auditoría de TI.	
			15. Realizar asesoría profesional a las áreas de negocio, TI u otras áreas de Auditoría Interna, en áreas como gobierno, riesgo, seguridad y cumplimiento en las tecnologías de información.	
			16. Participar en sesiones de Comités de Junta Directiva o Comisiones del Banco.	
			17. Cumplir con la calidad y con los tiempos de respuesta establecidos para las funciones correspondientes al cargo.	
			18. Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.	
			19. Ejecutar otras funciones propias de la Dirección.	
			FUNCIONES RELACIONADAS CON RIESGO	
			20. 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.	
			21. 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.	
			22. 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.	
			23. Velar por una adecuada gestión de los riesgos que pueden impactar sobre el plan estratégico y el plan de trabajo de la Auditoría Interna.	
			24. 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.	
			25. 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.	
			26. Promover que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.	
			27. 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			
	Formación Académica:	Licenciatura en Ingeniería de Sistemas e Informática o Contaduría Pública (u otra especialidad que la Auditoría requiera).		
	Legales:	Incorporado al Colegio Profesional respectivo y estar al día con sus obligaciones.		
	Experiencia:	Tres años de experiencia en labores relacionadas con la Auditoría de Tecnología de Información.		
CODIGO	* REQUISITOS TÉCNICOS EXIGIBLES			
	1. Certificación CISA (Auditor certificado en Sistemas de Información).			
	2. Auditor certificado en Fundamentos de COBIT 5 o versión superior.			
	3. 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.			
	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 (Reglamentos Internos, SUGEF, BCCR, Contraloría General de la República).			
	7. Conocimiento sobre las directrices, estándares, herramientas y técnicas de aseguramiento y auditoría de TI emitidas por la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association/ ISACA).			
	8. Conocimiento de técnicas de redacción y comunicación de informes de auditoría.			
	9. Conocimiento de la arquitectura de TI en relación con los datos, las aplicaciones, lenguajes de programación y la tecnología (Mainframe, aplicaciones distribuidas, aplicaciones basadas en la web, servicios web, aplicaciones de n-capas, middleware, core bancario, aplicaciones móviles).			
	10. Conocimiento en la gestión del ciclo de vida del desarrollo de sistemas e infraestructura tecnológica.			
	11. Conocimiento en gestión de controles de seguridad de la información y ciberseguridad.			
	12. Conocimientos sobre prácticas de gestión de la capacidad, disponibilidad y uso de herramientas y técnicas de monitoreo relacionadas.			
	13. Conocimiento sobre las prácticas de gestión de incidentes y problemas de TI, incluyendo el monitoreo y respuesta a incidentes de seguridad de la información.			
* 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 en marcos de gestión y control de las tecnologías de información (ITIL v3, ISO / IEC 27001, TOGAF).				
	2. Conocimiento y domino de Microsoft Project.				
	3. Conocimiento y dominio de software de diseño de diagramas de flujo de procesos.				
	4. Conocimiento de herramientas de análisis de datos mediante técnicas de auditoría asistida por computadora (CAATs), por ejemplo, ACL o IDEA.				
	5. Conocimiento intermedio del idioma inglés.				
CODIGO	SISTEMAS UTILIZADOS				
	Word, Excel, Power Point, Outlook. Sharepoint, Teams				
	SIPRE				
	SIAR				
	Service Manager				
	Sistema de Control de Tiempos				
	ACL				
	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL: AUDITORES JR Y SR			
CÓDIGO	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				
CÓDIGO	Gerenciales:	D	C	B	A
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CÓDIGO	Del 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				
CÓDIGO	Del Soporte:	D	C	B	A
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CÓDIGO	DISC - Personalidad	D	C	B	A
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	<p>Este perfil se aprueba mediante Acuerdo, Sesión JDN-5548, Acd-260, Art-9, Inciso: 2a, del 10 de abril de 2018.</p> <p>Se agregan las funciones Relacionadas con Riesgo, según autorización brindada por la Gerencia General Corporativa mediante HT-493-GGC-2019, de fecha 14 de octubre de 2019.</p> <p>La Gerencia General Corporativa aprueba el ajuste de este perfil, mediante el oficio GGC-313-2021, con fecha 01 de marzo 2021. Referencia DIRCH-0299-2021</p>				