

<div><div></div><div>MANUAL DE CARGOS</div></div>				
Dependencia:	Dirección Tecnología de la Información		Área:	Área Seguridad Operativa Informática
Código del Cargo:	3011.20		Código del Puesto:	3011
Categoría:	21		Nombre del Puesto:	Profesional Procesamiento Electrónico de Datos 2
Nombre del Cargo:	Profesional Desarrollo y Arquitectura de la Seguridad		Reporta a:	Jefe Área Seguridad Operativa Informática
Objetivo del Cargo:	Ejecutar labores profesionales relacionadas con control, evaluación y seguimiento de los procesos, productos y proyectos tecnológicos solicitados por las diferentes áreas, asegurando la calidad y operación de los mismos y cumpliendo con los procedimientos y normativas establecidas. Así mismo, revisar y atender requerimientos varios que sean asignados por la jefatura correspondiente, brindar apoyo en lo que solicite en concordancia con la normativa y valores institucionales.			
MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES	
			1	Diseñar las arquitecturas de seguridad para las infraestructuras tecnológicas del Banco, consideradas como parte del desarrollo de proyectos e iniciativas del Conglomerado.
			2	Atender las alertas y recomendaciones sobre la gestión amenazas a los productos y servicios, coordinar los ajustes sobre los controles de seguridad o la infraestructura de TI.
			3	Apoyar en la definición e implementación de la arquitectura técnica para la protección de datos en su ciclo de vida.
			4	Gestionar la ejecución de pruebas de vulnerabilidades (DAST y SAST) en los diferentes proyectos, productos o servicios previo a su puesta en operación.
			5	Coordinar las actividades de aseguramiento durante el ciclo de vida de desarrollo de software.
			6	Coordinar y trabajar en conjunto con distintos equipos de trabajo en la implementación de los proyectos, iniciativas y/o actividades establecidas en el Plan de Gestión de Seguridad de la Información y Ciberseguridad, relacionados con la actividad del área.
			7	Coordinar la definición y actualización de controles de seguridad de la información para el resguardo de activos sensitivos y de la tecnología de seguridad informática.
			8	Dotar de los recursos necesarios para el diseño y actualización de la arquitectura de seguridad informática.
			9	Contribuir con la elaboración y ejecución de los planes de seguridad informática, considerando los requerimientos del negocio, la configuración de TI y los planes de acción del riesgo de la información.
			10	Brindar soporte en la implementación y actualización de las herramientas que conforman la arquitectura tecnológica de seguridad informática tanto de hardware como software.
			11	Apoyar la atención de alertas y emitir las recomendaciones sobre la gestión de amenazas a los productos.
			12	Realizar pruebas de identificación de vulnerabilidades y elaborar el informe técnico con su análisis y recomendaciones para las empresas del Conglomerado.
			13	Diseñar y estructurar el uso de las herramientas de seguridad que permitan una utilización eficiente por capas, integrando las tecnologías adoptadas por la Organización que permitan trazabilidad de los eventos no deseados en materia de seguridad.
			14	Asesorar a otras áreas todo lo concerniente a seguridad operativa informática, para la adquisición de nuevas herramientas de software y hardware.
			15	Realizar análisis, estudios, investigaciones, informes y recomendaciones relacionados con la Seguridad Informática.
			16	Cumplir con la calidad y con los tiempos de respuesta establecidos para las funciones correspondientes al cargo.
			17	Colaborar en la ejecución de actividades o proyectos establecidos de alcance Institucional para el Área.
			18	Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.
			19	Ejecutar otras funciones propias del Área.
			FUNCIONES RELACIONADAS CON RIESGO	
			20	Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			21	Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			22	Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			23	Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			24	Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			25	Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			26	Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			27	En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
			FUNCIONES RELACIONADAS CON SUGEF	
			28	Según el Acuerdo SUGEF 14-17 “Reglamento General de Gestión de la Tecnología de Información”, el cual establece los requerimientos mínimos para la gestión de tecnología de información que deben de acatar las entidades supervisadas y reguladas del sistema financiero costarricense y en concordancia con la Ley de Control Interno, Capítulo III, Sección I “Deberes del jerarca y los titulares subordinados”, capítulo 12,13 y 14, este puesto es responsable del desarrollo de las actividades y tareas que le asignen velando por un adecuado ejercicio del mismo, debe garantizar la eficiencia y eficacia de las operaciones que le corresponde ejecutar tomando las medidas correctivas en beneficio de la institución. Por el nivel del puesto deberá promover mecanismos y procesos que mejoren el sistema de control interno en la gestión que le corresponde realizar. Debe procurar mantener las operaciones con un nivel de riesgo aceptable.
CÓDIGO	REQUISITOS EXIGIBLES			
	*Formación Académica:	Licenciatura en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Sistemas Informáticos u otra especialidad relacionada con Sistemas de Información. Preferiblemente con formación en Administración de Recursos Tecnológicos y Seguridad Informática.		
	Legales:	No aplica.		
	Experiencia:	Tres años de experiencia en labores relacionadas con la arquitectura de seguridad informática.		
*Para los puestos profesionales que no cuentan con el requisito académico de Licenciatura según el perfil, deben ostentar mínimo el grado de Bachillerato Universitario en la rama y demostrar mediante certificación la experiencia para el ejercicio del cargo.				
CÓDIGO	* REQUISITOS TÉCNICOS EXIGIBLES			
	1. Certificación COMPTIA Security +.			
	2. Certificación de Ciberseguridad (I ISACA - CSX; Certified Ethical Hacker (CEH); GIAC Security Essentials (GSEC); CISSP (Certified Information Systems Security Professional); o equivalente).			
	3. Conocimiento en desarrollo seguro.			
	4. Conocimiento en herramientas de desarrollo seguro.			
	5. Conocimiento en arquitectura de seguridad.			
	6. Conocimiento intermedio en inglés técnico para la lectura e interpretación de manuales y libros.			
* 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 seleccón.				

CÓDIGO	REQUISITOS TÉCNICOS DESEABLES				
	1. Conocimiento en la Normativa externa relacionada con la Superintendencia General de Entidades Financieras (SUGEF).				
	2. Conocimiento en la Normativa externa relacionada con el Cumplimiento de la Ley 8204.				
	3. Conocimiento en la Normativa Interna del Conglomerado Financiero.				
	4. Conocimiento en Hacker Ético Básico.				
	5. Conocimiento avanzado en las Mejores prácticas en TI (COBIT, ITIL o ISO 27000).				
	6. Conocimiento en Autorías de Sistemas Básico.				
	7. Conocimiento en la Planificación y Administración del Tiempo.				
	8. Conocimiento en procesos de Investigación.				
	9. Conocimiento en la ejecución de Informes Profesionales.				
	10. Conocimiento en Análisis Forenses.				
CÓDIGO	SISTEMAS UTILIZADOS				
	Word, Excel, Power Point, Outlook				
	Sistema de Gestión de Seguridad de la Información				
	Herramientas de seguridad informática a modo de supervisión (lectura)				
	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL: PROFESIONAL SOPORTE			
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:	La Junta Directiva Nacional aprueba la creación de este perfil mediante el acuerdo JDN-5939-Acd-707-2022-Art-23, con fecha 29 de julio de 2022. Referencia GGC-841-2022/DCD-0626-2022				
	La Gerencia General Corporativa aprueba ajustes a este perfil mediante el oficio GGC-1210-2022, con fecha 07 de octubre de 2022, aprobado el 10 de octubre de 2022. Referencia DIRGC-498-2022/DIRCH-1315-2022				
	Este perfil sustituye el cargo 3011.02 Iniciativas-Seguridad Operativa Informática creado mediante la aprobación de la Gerencia General Corporativa en el HT-041-GGC-2017 del 25 de enero 2017.				
	La Gerencia General Corporativa aprueba ajustes a este perfil, mediante oficio GGC-1516-2022, con fecha 13 de diciembre de 2022, en cuanto al requisito legal y observación de formación académica. Referencia DIRGC-620-2022 / DIRCH- 1586-2022.				