

		MANUAL DE CARGOS		
Dependencia:	Dirección Tecnología de la Información		Área:	Área Seguridad Operativa Informática
Código del Cargo:	3011.21		Código del Puesto:	3011
Categoría:	21		Nombre del Puesto:	Profesional Procesamiento Electrónico de Datos 2
Nombre del Cargo:	Profesional Plataforma, Infraestructura e Identidades		Reporta a:	Jefe Área Seguridad Operativa Informática
Objetivo del Cargo:	Ejecutar labores profesionales relacionadas con el 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	Analizar las alertas de los eventos críticos de la operativa de las plataformas de seguridad informática, incluidos en el registro de resultados del personal de Monitoreo.
			2	Implementar y mantener medidas preventivas y correctivas de detección, que permitan proteger los sistemas de información y tecnología de software malicioso (virus, gusanos, software espía y correo basura, entre otros).
			3	Ejecutar las medidas de seguridad lógica de la plataforma tecnológica del Banco, manteniendo los niveles razonables de seguridad de la red.
			4	Mantener un adecuado nivel de seguridad en la infraestructura tecnológica del Banco, estableciendo controles de seguridad alineados con la clasificación de los datos.
			5	Aplicar controles de seguridad de la información para el resguardo de activos sensitivos y de la tecnología de seguridad, así como, procedimientos de gestión que permitan la transmisión de datos en la red de forma segura.
			6	Ejecutar las medidas, controles de seguridad y procedimientos de gestión relacionados, para proteger la información en todos los modos de conexión.
			7	Actualizar los controles de seguridad y procedimientos de gestión, que permitan el aseguramiento de los dispositivos de usuario final.
			8	Ejecutar los mecanismos para asegurar los derechos de acceso de los usuarios, de acuerdo con los requerimientos de las funciones y procesos de negocio.
			9	Administrar sistemas criptográficos de TI, de acuerdo con las políticas y procedimientos establecidos, que ayuden a asegurar el ciclo de vida de los certificados digitales (generación, cambio, revocación, destrucción, distribución, almacenaje, uso, modificación y acceso desautorizado).
			10	Elaborar con los proveedores los planes de trabajo para la ejecución del mantenimiento y soporte de las plataformas de seguridad cuando sea requerido.
			11	Ejecutar respaldos periódicos de las bases de datos y configuraciones de la infraestructura tecnológica de seguridad.
			12	Administrar la operación de las plataformas de seguridad y realizar la configuración, mantenimiento y actualización de las herramientas de seguridad.
			13	Establecer controles técnicos que permitan la seguridad de la información en cuanto a la integridad y disponibilidad de las plataformas tecnológicas del Banco.
			14	Documentar el Plan de Pruebas de Seguridad de TI.
			15	Cumplir con la calidad y con los tiempos de respuesta establecidos para las funciones correspondientes al cargo.
			16	Colaborar en la ejecución de actividades o proyectos establecidos de alcance Institucional para la dependencia.
			17	Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.
			18	Ejecutar otras funciones propias de la depencia.
			FUNCIONES RELACIONADAS CON RIESGO	
			19	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.
			20	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.
			21	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.
			22	Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			23	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.
			24	Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			25	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.
			26	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	
			27	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 Ingeniería en Sistemas, Ingeniería Informática o Ingeniería Tecnología de la Información u otra especialidad relacionada con Sistemas de Información.		
	Legales:	No aplica.		
	Experiencia:	Tres años de experiencia en en labores relacionadas con la administración y mantenimiento de infraestructura tecnológica.		
*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 (ISACA - CSX; Certified Ethical Hacker (CEH); GIAC Security Essentials (GSEC);o equivalente).			
	3. Conocimiento en fundamentos de Ciberseguridad.			
	4. Conocimiento en herramientas de seguridad informática (Palo Alto, CheckPoint, ISE CISCO, FirePower CISCO, ForcePoint, Symantec, Seguridad Office365, Seguridad Azure, Certificados Digitales, Microfocus).			
	5. Conocimiento en la gestión de incidentes de seguridad de la información.			
	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 selección.				

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 7786.				
	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:	<p>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</p> <p>La Gerencia General Corporativa aprueba ajustes a este perfil mediante el oficio GGC-1173-2022, con fecha 21 de setiembre de 2022, aprobado el 30 de setiembre de 2022. Referencia DIRGC-462-2022/DIRCH-1272-2022</p> <p>Este perfil sustituye el cargo 3010 Ingeniero Gestión Operativa Seguridad Informática - Junior creado mediante la aprobación de la Gerencia General Corporativa en el oficio GGC-1028-2018 (Acta DGCA-Act.08-2018 (División Gestión de Calidad).</p> <p>Este perfil sustituye 3010.19 Profesional Plataforma, Infraestructura e Identidades, aprobado en una primera instancia por la Junta Directiva Nacional.</p> <p>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.</p>				