

Dependencia:	Dirección Corporativa de Riesgo	Área:	División Seguridad Corporativa
Código del Cargo:	3011.18	Código del Puesto:	3011
Categoría:	21	Nombre del Puesto:	Profesional Procesamiento Electrónico de Datos 2
Nombre del Cargo:	Profesional Seguridad Corporativa	Reporta a:	Jefe División Seguridad Corporativa
Objetivo del Cargo:	Realizar labores profesionales a nivel corporativo para ejecutar, coordinar, dar seguimiento y control a las actividades relacionadas al cumplimiento de leyes, regulaciones, buenas prácticas, hallazgos de auditoría (internas/externas), acuerdos (comités y JDN), requerimientos de entes supervisores, programa de cultura, programa plan de gestión seguridad de la información y ciberseguridad, lo anterior en materia de Seguridad de la Información y ciberseguridad, con el objetivo de definir, implementar y actualizar las políticas, procedimientos y controles de seguridad, para preservar la confidencialidad, integridad y disponibilidad de la información para el alineamiento con la estrategia del CFBPDC.		
MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES
			1 Ejecutar las actividades requeridas para el mantenimiento, seguimiento, monitoreo y actualización de los Sistemas y/o Programas de Gestión de Seguridad de la Información del Conglomerado Financiero Banco Popular y Desarrollo Comunal y Plan Táctico de Seguridad de la Información y Ciberseguridad para identificar el estado actual, riesgos y definición de la estrategia de seguridad de la información para su comunicación y seguimiento por las partes interesadas.
			2 Acompañar en el establecimiento de Sistemas y/o Programas de Gestión de Seguridad de la Información del Conglomerado Financiero Banco Popular y Desarrollo Comunal que se encuentren alineados con los objetivos estratégicos del Conglomerado y normativa aplicable.
			3 Realizar el seguimiento de las actividades operativas, planes de acción, iniciativas y/o proyectos correspondientes a los Programas de Gestión de Seguridad de la Información del Conglomerado Financiero Banco Popular y Desarrollo Comunal.
			4 Realizar la coordinación de los foros y Comités de Gobierno de Seguridad, además ejecutar el seguimiento del cumplimiento de acuerdos respectivos.
			5 Participar en foros y Comités de Gobiernos Corporativo que sean requeridos.
			6 Ejecutar las actividades requeridas para las elevaciones Gerenciales en materia de Seguridad de la información.
			7 Ejecutar la coordinación para la recepción, revisión, consolidación y presentación de los indicadores de desempeño de la postura de Seguridad para el Conglomerado Financiero Banco Popular.
			8 Ejecutar las actividades requeridas para el mantenimiento, monitoreo y actualización periódica de la normativa que conforma los Sistemas de Gestión de Seguridad de la Información del CFBPDC y Sistema Gestión de Calidad (políticas, directrices, procedimientos, estándares, entre otros) que asistan a las operaciones de seguridad y continuidad garantizando su debido mantenimiento, así como, dar seguimiento a su cumplimiento y métricas.
			9 Verificar el cumplimiento de aplicación de las líneas base de seguridad para las diferentes plataformas de sistemas de tecnologías de la información en el Conglomerado.
			10 Elaborar e implementar los modelos, metodologías, controles y documentos que brinden soporte y operación al proceso gestión de Seguridad.
			11 Atender o coordinar la atención de los requerimientos de entes de supervisión, reguladores, hallazgos de auditorías (internas y externas), acuerdos de comités y Junta directiva Nacional de seguridad de la información.
			12 Coordinar y ejecutar las actividades requeridas para establecimiento, implementación, revisión y mejora del Sistema de Gestión de Seguridad (SGSI).
			13 Ejecutar las actividades requeridas para el mantenimiento, monitoreo y actualización periódica del Programa de Cultura de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio para el Conglomerado Financiero que permita definir la estrategia de generación de cultura.
			14 Ejecutar las acciones para promover, evaluar y medir a nivel Corporativo el estado de la cultura en materia de seguridad de la información y continuidad del negocio, de manera que el personal y terceros comprendan su importancia y sus responsabilidades sobre ésta.
			15 Apoyar a la jefatura en el seguimiento y cumplimiento de las actividades de los planes de trabajo y tareas asignadas.
			16 Participar en reuniones con la jefatura para la asignación de prioridades de los proyectos, tareas o similar, así mismo, elaborar y autorizar documentos mediante oficios en relación con entregables correspondientes a la dependencia.
			17 Preparar y presentar informes relacionados con las actividades al cumplimiento de leyes y regulaciones, investigaciones, trabajos realizados por el equipo a cargo, así como, colaborar en la gestión administrativa relativa al cumplimiento del PAO, Presupuesto, Plan de Acción, Planes de Mitigaciones, entre otros.
			18 Validar y presentar los informes profesionales sobre avances y comportamiento del desarrollo general del proceso asignado.
			19 Ejecutar actividades para la atención de oficios, acuerdos, análisis, solicitudes, entre otra documentación que le sea asignada, así como su elaboración, revisión y/o firma cuando sea requerido y según corresponda.
			20 Colaborar y ejecutar labores relacionadas con la prestación y solicitudes de servicios en SICOP.
			21 Cumplir con la calidad y con los tiempos de respuesta establecidos para las funciones correspondientes al cargo.
			22 Colaborar en la ejecución de actividades o proyectos establecidos de alcance Institucional para la División
			23 Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.
			24 Ejecutar otras funciones propias del puesto o de la División Seguridad Corporativa.
			<b>FUNCIONES RELACIONADAS CON RIESGO</b>
			25 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.
			26 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.

			27	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.	
			28	Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.	
			29	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.	
			30	Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.	
			31	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.	
			32	En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.	
CÓDIGO	REQUISITOS EXIGIBLES				
	Formación Académica:	Licenciatura en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Sistemas Informáticos, Ingeniería Industrial, Ingeniería en Producción Industrial.			
	Legales:	Incorporado al Colegio Profesional respectivo y estar al día con sus obligaciones.			
	Experiencia:	Tres años de experiencia en gestiones, actividades y proyectos relacionados con la seguridad de información o ciberseguridad.			
CÓDIGO	* REQUISITOS TÉCNICOS EXIGIBLES				
	1. Certificación normativa ISO/IEC 27001 (Implementador o auditor) o Certificación Gerente de Seguridad de la Información (CISM).				
	2. Certificación en alguna de las siguientes especialidades: LCSPC, CEH, CompTIA Security +, GSEC, SSCP, CISSP o semejantes.				
	3. Certificación en Fundamentos COBIT 5 o COBIT 2019.				
	4. Conocimiento de la normativa de Gestión del Riesgo (ISO 27005 o ISO31000).				
	5. Conocimiento en la administración de plataformas: Microsoft (Windows 10, Servidores, bases de datos SQL, Office 365, Azure), AS400, S390, Cisco, Citrix NetScaler, Servidores basados en Linux.				
	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. Certificación en ITIL v4 Fundamentos.				
	2. Conocimiento de estándar PCI DSS para la protección de datos de tarjetas.				
	3. Conocimiento de los principios de privacidad y protección de datos personales según regulaciones y Ley 8968.				
	4. Conocimiento en análisis e identificar vulnerabilidades en sistemas de información.				
	5. Conocimiento de la arquitectura de seguridad de la información empresarial de la organización.				
	6. Conocimiento en la administración de plataformas: Microsoft (Windows 10, Servidores, bases de datos SQL, Office 365, Azure), AS400, S390, Cisco, Citrix NetScaler, Servidores				
	7. Conocimiento intermedio en inglés técnico para la lectura e interpretación de manuales y libros.				
CÓDIGO	SISTEMAS UTILIZADOS				
	Word, Excel, Power Point, Outlook (Office 365)				
	Centro Soporte Logístico y Service Manager Console				
	SIPRE				
	SIAR y CAR				
	Herramientas de seguridad informática a modo de supervisión (lectura)				
	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL PROFESIONAL DE SOPORTE			
Código	Competencias Cardinales	D	C	B	A
CAR-01	Orientación al Cliente				
CAR-02	Innovación y Creatividad				
CAR-03	Orientación a Resultados				
CAR-04	Seguimiento de procedimientos (Integridad)				
CAR-05	Inteligencia Emocional				
Código	Competencias de Soporte	D	C	B	A
SOP-01	Precisión				
SOP-02	Practicidad				
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 Este perfil sustituye el cargo por roles 3011.10 creado mediante la aprobación de la Gerencia General Corporativa en el HT-558-GGC-2019, de fecha 18 de noviembre de 2019. La Gerencia General Corporativa aprueba ajustes a este perfil mediante el GGC-1211-2024, del 03 de setiembre del 2024. Referencia DIRCCH-1243-2024. Como parte de la implementación del Modelo Organizacional 2.0, aprobada por la Junta Directiva Nacional con el acuerdo JDN-6070-Acd-1469-2023-Art-4, sesión celebrada 20 de diciembre del 2023.				