



MANUAL DE CARGOS

Dependencia:	Dirección Corporativa de Riesgo			Área:	División de Riesgo Operativo
Código del Cargo:	3004.126			Código del Puesto:	3004
Categoría:	20			Nombre del Puesto:	Ejecutivo Bancario Administrativo 1
Nombre del Cargo:	Gestor de Riesgo Ciberseguridad			Reporta a:	Jefe División de Riesgo Operativo
Objetivo del Cargo:	Ejecutar labores profesionales relacionadas con la asesoría en la gestión y control de actividades con los riesgos de ciberseguridad, a fin de velar por una adecuada aplicación de las normas y gestión del riesgo de ciberseguridad en el Conglomerado Financiero Banco Popular. Así mismo, revisar y atender requerimientos varios que sean asignados por la jefatura correspondiente y brindar apoyo en lo que solicite, en concordancia con la normativa y valores institucionales.				
MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES		
			1	Investigar, identificar, medir, analizar y controlar el riesgo de ciberseguridad en el Conglomerado Financiero Banco Popular.	
			2	Ejecutar acciones de actualización, mantenimiento y evaluación de los planes de mitigación relacionados con la gestión de riesgos de T.I y ciberseguridad.	
			3	Asesorar a la Dirección Corporativa de Riesgos y las dependencias en materia de la gestión de riesgos de ciberseguridad.	
			4	Elaborar informes técnicos sobre la gestión de riesgo de ciberseguridad que presenta el Conglomerado Financiero Banco Popular.	
			5	Diseñar y actualizar las políticas y metodologías de administración de riesgo de seguridad de información.	
			6	Realizar el análisis de riesgos de ciberseguridad en el Conglomerado Financiero Banco Popular.	
			7	Analizar y evaluar el costo o cuantificación de los incidentes asociados a eventos de ciberseguridad.	
			8	Dar seguimiento de los eventos de pérdida correspondientes al Banco.	
			9	Analizar, emitir criterios y asesorar en estudios de factibilidad de riesgos de ciberseguridad a distintas dependencias, basado en la Metodología de Riesgos de Contratos de Proveedores del CFBP.	
			10	Bridar seguimiento y monitoreo de incidentes de ciberseguridad.	
			11	Analizar los riesgos de ciberseguridad de nuevos productos, servicios y canales.	
			12	Realizar sesiones de riesgo para la elaboración de Talleres de Riesgos Ciberseguridad.	
			13	Brindar seguimiento y monitoreo de incidentes tecnológicos.	
			14	Participar en reuniones con la jefatura para la asignación de prioridades, tareas o similar, así mismo, elaborar informes y oficios correspondientes a la dependencia.	
			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 División de Riesgo Operativo.	
			17	Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.	
			18	Ejecutar otras funciones propias de la División de Riesgo Operativo.	
			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.	
CÓDIGO	REQUISITOS EXIGIBLES				
	Formación Académica:	Licenciatura en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Sistemas Informáticos, Ingeniería Industrial, Ingeniería en Producción Industrial o Administración de Negocios.			
	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 CISM (Gerente de Seguridad de la Información), o Certificación CISSP (Profesional certificados en sistemas de seguridad de la información) o Certificación SSCP (Profesional Certificado en Seguridad de Sistemas) o Certificación CEH (Hacker Ético).				
	2. Conocimiento de la Normativa de Gestión del Riesgo (ISO 27005 o ISO31000).				
* Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares o a través 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 avanzado en las Mejores prácticas en TI (COBIT o ITIL).				
	3. Conocimiento en análisis e identificación de vulnerabilidades en sistemas de información.				
	4. Conocimiento en Gestión de Riesgos Operativo.				
	5. Conocimiento en Gestión de Riesgos de Fraude.				

CÓDIGO	SISTEMAS UTILIZADOS				
	Word, Excel, Power Point, Outlook (Office 365)				
	Centro Soporte Logístico y Service Manager Console				
	Oprisk				
	COMPETENCIAS REQUERIDAS				
	PERFIL KOMPE DISC:	PERFIL: PROFESIONAL DE SOPORTE			
CÓDIGO	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	De Soporte	D	C	B	A
SOP-01	Precisión				
SOP-02	Practicidad				
Observaciones:	La Gerencia General Corporativa aprueba este perfil mediante oficio GGC-1211-2022, con fecha 07 de octubre de 2022 Referencia DIRGC-499-2022/ DIRCH-1303-2022. Se ajustan las competencias en mayo de 2025, acorde con el "Modelo de Competencias" aprobado por la Gerencia General Corporativa, mediante oficio GGC-1293-2022.				