MANUAL DE CARGOS

Dependencia:	División Control Operativo	**Área**	Área Seguridad Operativa Informática
Código del Cargo:	2009.XX	**Código del Puesto:**	2009
Categoría	17	**Nombre del Puesto:**	Técnico PED 2
Nombre del Cargo:	Técnico de Seguridad Operativa Informática	**Reporta a:**	Jefe Área Seguridad Operativa Informática
Objetivo del Cargo:	Técnico encargado del monitoreo de la infraestructura tecnológica de seguridad operativa informática, así como de los procesos y eventos relevantes de seguridad que permita identificar aquellos posibles incidentes que atenten contra la seguridad de la información.		

MACRO PROCESO	PROCESO	ACTIVIDAD		FUNCIONES PRINCIPALES
			1	Planear y organizar el trabajo en coordinación con su superior inmediato.
			2	Evacuar consultas y atender solicitudes de clientes internos, así como participar en diferentes actividades cuando sea solicitado por la Jefatura.
			3	Velar porque los trabajos encomendados se cumplan oportunamente y de acuerdo con las fechas establecidas.
			4	Permanecer actualizado en cuanto los cambios y nuevas tendencias que se presentan en la dependencia a la que pertenece.
			5	Monitoreo y análisis de tendencias del ciberespacio del panorama global de amenazas informáticas y su evolución, con el fin de analizar su impacto en la organización, así como sus remediaciones o medidas requeridas.
			6	Acatar y velar por el cumplimiento de normas, leyes, procedimientos y políticas tanto internas como externas que afecten la función.
			7	Cumplir con los estándares de calidad en la ejecución de sus labores.
			8	Ejecutar otras tareas propias del puesto.
				FUNCIONES ESPECÍFICAS
			9	Colaborar con la elaboración de reportes de los beneficios identificados de las inversiones, en temas de seguridad operativa informática.
			10	Proveer información para la actualización de códigos SICA.
			11	Colaborar con implementación y divulgación de las políticas de TI.
			12	Colaborar con la preparación y entrega de insumos para elaborar el Plan de Mantenimiento.
			13	Vigilar que el monitoreo de la seguridad de TI, se brinde de acuerdo al esquema establecido por la dependencia y en línea con protocolos de atención predefinidos.
			14	Operar las plataformas de prevención y detección de software malicioso, (IPS, Antivirus, Firewall Next Generation), así como de los controles de seguridad de la red.
			15	Cooperar con las actualizaciones de seguridad de los equipos administrados por el Área.
			16	Administrar el registro y clasificación de incidentes, con el fin de que sean analizadas para recomendar mejoras a los esquemas de monitoreo y atención de incidentes.
			17	Participar en el diagnóstico y análisis de incidentes y dar seguimiento a las recomendaciones y acciones correctivas propuestas.
			18	Cooperar con la gestión de solicitudes de servicios, relacionados con la seguridad operativa informática.
			19	Cooperar con el respaldo de las configuraciones de los equipos de la plataforma tecnológica.
			20	Dar seguimiento a los reportes de fallas o caídas de los servicios, de acuerdo al resultado del monitoreo de incidentes, eventos en la infraestructura y escalar a los niveles superiores en los casos que corresponda.
			21	Apoyar en las labores para dar protección adicional a aplicaciones claves en la Institución, tales como procesos de análisis de vulnerabilidades y procesos de hardening y seguimiento de sus atenciones.
			22	Mantener un inventario actualizado de los activos sensitivos de TI.
			23	Participar en la implementación de cambios en componentes o parámetros sobre seguridad operativa.
			24	Participar en la inclusión y aplicaciones de respaldo y restauraciones.
			25	Ejecutar tareas específicas de acuerdo al plan de pruebas de controles de seguridad.
				FUNCIONES RELACIONADAS CON RIESGO
			26	Desarrollar las actividades de gestión de los riesgos (identificar, valorar y controlar) de aquellos que impactan los procesos y planes de acción del Conglomerado.
			27	Velar por el logro de los objetivos y las metas institucionales, relacionadas directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda, alineados a la Metodología Institucional de Administración de Riesgos y las políticas internas del Conglomerado.
			28	Aplicar las herramientas y técnicas para identificación y control de los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			29	Ejecutar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			30	Adoptar a las acciones necesarias para el funcionamiento adecuado del sistema de valoración del riesgo, garantizando una cultura de riesgo integral.
			31	Conocer sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			32	Le puede corresponder participar activamente en las diferentes reuniones en las que se dé a conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes a la Dependencia donde se encuentre asignado.
			33	En caso de materializarse un evento de riesgo es responsable de reportarlo a su superior inmediato, para el trámite respectivo ante la Dirección Corporativa de Riesgo.
				FUNCIONES RELACIONADAS CON SUGEF
			34	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.

CODIGO	REQUISITOS EXIGIBLES	
	Formación Académica:	Tercer año Universitario o Diplomado Universitario en Ingeniería de Sistemas u otra carrera universitaria afín con las funciones del puesto.
	Legales:	No aplica.
	Experiencia:	Dos años de experiencia en actividades propias a las descritas.

CODIGO	* REQUISITOS TÉCNICOS EXIGIBLES
	Contar al menos con una especialización certificada y vigente en materia de seguridad de la información, tales como:
	1. Certified Ethical Hacker (CEH)
	2. Certified Information Security Manager (CISM)
	3. Certified Information Systems Security Professional (CISSP)
	4. Certified CompTIA Security+
	5. CSX Practitioner

*** 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. Conocimiento de las leyes aplicables al Conglomerado de normativa interna, reglamentos, directrices y circulares que regulan la actividad del Conglomerado.
	2. Conocimiento en Inglés Técnico (comprensión y lectura).
	3. Conocimiento en Servicios de Monitorización de los Procesos y Eventos de Seguridad de la Información.
	4. Conocimiento en Operaciones de Seguridad de la Información y Gestión de Riesgos e Incidentes.
	5. Conocimiento en la Ley de delitos informáticos y norma SUGEF 14-09.
CODIGO	**SISTEMAS UTILIZADOS**

COMPETENCIAS REQUERIDAS					
PERFIL KOMPE DISC:		PERFIL: TECNICOS SOPORTE			
CODIGO	**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				
CODIGO	**Gerenciales**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CODIGO	**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				
CODIGO	**Soporte**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CODIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	**Este perfil se aprueba con oficio GGC-1028-2018 de la Gerencia General Corporativa (Acta DGCA-Act.08-2018 (División Gestión de Calidad).** **Se incluyen Funciones de Riesgo las cuales se incorporan a los perfiles con la aprobación de la Gerencia General Corporativa, emitida en el HT-493-GGC-2019, de fecha el 14 de octubre 2019. Referencia: DIRGE-689-2019 / DIRCH-1477-2019.**				