IDEA
Instituto para el Desarrollo de Antioquia

RESOLUCIÓN DE JUNTA DIRECTIVA No. 0012-22

"Por la cual se actualiza e incorpora el Manual Específico de Funciones y de Competencias Laborales de un Profesional Especializado en la Planta de Personal del Instituto para el Desarrollo de Antioquia- IDEA".

La Honorable Junta Directiva del Instituto para el Desarrollo de Antioquia-IDEA en uso de sus atribuciones legales y estatutarias y en especial las que le confiere el artículo 76 de la Ley 489 de 1998, la Ley 909 de 2004, el Decreto 785 de 2005 y el Decreto 1083 de 2015 y sus Decretos reglamentarios, la Ordenanza 13 de 1964, el artículo 13 de la Resolución de Junta Directiva No. 006 del 3 de junio de 2014, La Resolución de la Junta Directiva No. 0001 de 2019, la Resolución de Junta Directiva No. 0003 de 2021, la Resolución de Junta Directiva No. 0007 de 2021, y Resolución de Junta Directiva No.003 de 2022.

CONSIDERANDO

A. Que de conformidad con lo preceptuado en el Artículo 209 de la Constitución Política, la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

B. Que es función de la Junta Directiva del Instituto para el Desarrollo de Antioquia - IDEA, aprobar los manuales de funciones.

C. Que mediante Resolución de Junta Directiva No. 001 de 2019, actualizada mediante la Resolución de Junta Directiva No. 0003 de 2021, la Resolución de Junta Directiva No. 0007 de 2021, y Resolución de Junta Directiva No.003 de 2022, se estableció el Manual Especifico de Funciones y Competencias Laborales para todos los empleos que conforman la Planta de Personal del Instituto para el Desarrollo de Antioquia - IDEA.

D. Que el Artículo 32 del Decreto Ley 785 de 2005, establece que la adopción, adición, modificación o actualización del manual de funciones y competencias laborales se efectuara mediante acto administrativo de la autoridad competente.

E. Que en reunión Ordinaria de Junta Directiva, celebrada el día 22 de diciembre de 2022, fue aprobada la actualización e incorporación de las funciones del cargo acá descrito.

En mérito de lo anteriormente expuesto,

IDEA
Instituto para el Desarrollo de Antioquia

RESUELVE:

ARTÍCULO PRIMERO: Modificar la Resolución de Junta de Directiva 0001 del 29 de enero de 2019, por medio de la cual se establece el Manual específico de funciones y competencias laborales del Instituto para el Desarrollo de Antioquia -IDEA-, en el sentido de incorporar funciones en el Manual Específico de Funciones y de Competencias Laborales para un empleo del nivel Profesional, denominado **PROFESIONAL ESPECIALIZADO, CODIGO 222, GRADO 04, ADSCRITO A LA OFICINA DE GESTION DEL RIESGO**, de la Planta de Personal del Instituto para el Desarrollo de Antioquia -IDEA, el cual quedara así:

MANUAL DE FUNCIONES Y COMPETENCIAS LABORALES PROFESIONAL ESPECIALIZADO
Nivel: Profesional **Denominación:** Profesional Especializado **Código:** 222 **Grado:** 04 **Dependencia:** Oficina de Gestión del Riesgos **Jefe Inmediato:** Jefe Oficina de Gestión del Riesgo
PROPÓSITO PRINCIPAL
Aplicar los conocimientos propios de su profesión, con el apoyo de herramientas informáticas y desarrollos lógicos a la medida, que permitan garantizar la integridad, confidencialidad y disponibilidad de la información procesada, almacenada y transportada por sistemas de información interconectados entre unidades de almacenamiento, redes y software, utilizados en la gestión de la Institución.
DESCRIPCIÓN DE FUNCIONES ESENCIALES
1. Diagnosticar y controlar de manera periódica, las posibles causas de riesgos que puedan afectar la integridad, confidencialidad y disponibilidad de la información; asignando permisos, usuarios y perfiles en pro de la seguridad de datos. 2. Implementar barreras de seguridad a nivel físico y lógico, necesarios en el IDEA, con el fin de proteger la información y equipos informáticos, garantizando una adecuada seguridad informática. 3. Aplicar procesos y medidas de seguridad a nivel lógico (Sistema Operativo), con el fin de proteger los activos de información institucional, abordando las amenazas a la información procesada, almacenada y transportada que transitan por las redes de información institucional. 4. Rastrear, identificar, defender y eliminar Software Maliciosos, gusanos, troyanos, spyware, adware, ransomware, rogue, entre otros, que puedan afectar la eficacia

de los sistemas de la institución; dañar, acceder, secuestrar, suplantar y/o entorpecer el actuar diario, dentro de los sistemas de información corporativo.

5. Sugerir, implementar y mantener actualizado, software de defensa, que protejan los datos y software de gestión institucional.
6. Identificar posibles fallos en la vulnerabilidad de los software utilizados por la institución, evitando fallos, defectos de seguridad y puntos débiles; reportarlos a sus creadores para aportar en pro de sus correcciones (parches de seguridad) y tomar acciones preventivas, ante los posibles efectos que estos puedan ocasionar.
7. Validar, complementar y generar protocolos, identificación de amenazas, rastreo y seguimiento a los posibles fallos en la implementación de las políticas de seguridad de la información, seguridad informática y Ciberseguridad.
8. Capacitar a los diferentes usuarios institucionales acerca de las posibles vulnerabilidades naturales que puedan explotarse dentro del sistema institucional. Consecuencias y responsabilidades de las mismas.
9. Implementar medidas de cifrado y copias de datos inalterables y aislados. Para poder ser restaurados rápidamente durante un proceso de recuperación, con el fin de minimizar el impacto de ciberataque.
10. Reportar ante la Superintendencia Financiera y demás organismos de control y disciplinarios, a que dé lugar, la incursión y fallos en la implementación de las políticas, que puedan afectar la integridad, confidencialidad y disponibilidad de los activos de datos de la institución.
11. Promover la divulgación e integración de la Ciberseguridad, dentro de la Política de Seguridad de la Información y Ciberseguridad, así como la verificación del cumplimiento a través de mecanismos de monitoreo.
12. Liderar y Complementar al plan de gestión de riesgos institucional, las diferentes medidas de identificación, valoración, mitigación y control de los riesgos detectados en materia de Ciberseguridad.
13. Realizar respaldos a los activos de datos de la información, protocolos y actualizaciones permanentes, que permitan garantizar la integridad y disponibilidad de la información.
14. Generar y administrar permisos y perfiles de acceso a los activos de información, acorde con la jerarquía, gestión y control de los mismos.
15. Actuar de manera eficiente ante las incursiones ilegales, indebidas e invasivas al sistema lógico utilizado en la gestión institucional, identificadas por los diferentes sistemas de detección y alertas de fallos de y incidentes de ciberseguridad, recibidos a través de las diferentes alertas y monitoreo, y participar junto con los profesionales de seguridad informática en las etapas de análisis, contención, erradicación y recuperación de los activos de información.

16. FUNCIONES COMUNES (Transversales)

17. Definir y coordinar las pruebas de seguridad (vulnerabilidad, Ethical Hacking e ingeniería social) que se requieran realizar a la plataforma lógica, usuarios y perfiles, anticipándose a posibles fallos o incursiones del sistema.

18. Definir roles de acción ante los planes de mitigación, derivados de los análisis de riesgos, pruebas de seguridad, auditorías internas y externas, incidentes materializados, evaluación de indicadores, nuevos lineamientos, entre otros, así como garantizar la adecuada implementación de estos, para el plan de mejoramiento necesario en materia de ciberseguridad.
19. Liderar el Comité de Seguridad de la Información y Ciberseguridad.
20. Coordinar el cumplimiento normativo vigente, asociado a la seguridad de la información y ciberseguridad.
21. Capacitarse de manera continua en materia de ciberseguridad; al igual que participar de manera proactiva, en diplomados, foros, grupos afines, entre otros medios y métodos de actualización lógica.
22. Participar en los diferentes eventos de inducción y reinducción, con los aportes en materia de responsabilidad en la aplicación y protocolos ante los activos de la información y de ciberseguridad institucional y personal.
23. Documentar cartillas de protocolo en ciberseguridad, que propenda a garantizar la integridad, confidencialidad y disponibilidad de los activos de datos del instituto, con el fin de mitigar fallos mediante causas lógicas, mecánicas y externas. Con el fin de fortalecer los diferentes focos de vulnerabilidad.
24. Ejecutar las funciones propias de la dependencia de acuerdo a la vigilancia especial del Instituto, ejercida por la Superintendencia Financiera de Colombia y establecidas internamente en los Manuales que para el efecto se hayan implementado.
25. Ejercer la supervisión, el control y seguimiento a contratos y actividades que se requieran y se reciban por delegación, en materia de ciberseguridad a implementar por el instituto.
26. Desarrollar los procesos, actividades y acciones necesarias para la planeación, ejecución, evaluación y mejoramiento continuo del sistema de gestión Institucional.
27. Conocer la política del Sistema de Seguridad y Salud en el Trabajo (SGSST).
28. Conocer los riesgos referentes a su labor.
29. Hacer sugerencias para mejorar la seguridad y salud en el trabajo (SST).
30. Estar familiarizado con los planes de respuesta a emergencias.
31. Cumplir las normas, reglamentos e instrucciones del Sistema de Seguridad y Salud en el Trabajo (SGSST).
32. Informar oportunamente al empleador acerca de los peligros y riesgos latentes en su sitio de trabajo.
33. Las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, naturaleza y el área de desempeño del cargo.

CRITERIOS DE DESEMPEÑO

- Integridad, confidencialidad y disponibilidad de activos de datos.
- Implementación de controles, protocolos, adopción de perfiles y permisos, ante la red institucional y activos de datos.

- Implementación de herramientas y procedimientos vanguardistas en materia de ciberseguridad.

CONOCIMIENTOS BÁSICOS O ESENCIALES

- Conocimientos básicos de programación lógica.
- Conocimientos en Sistemas Operativos Windows a nivel de usuario avanzado
- Conocimientos en Seguridad informática (seguridad perimetral, redes, Protocolos de comunicación y seguridad)
- Conocimientos en Administración de contenidos en ambientes WEB.
- Conocimientos de Seguridad en redes
- Conocimiento en Modelo TCP/IP
- Conocimiento en herramientas de seguridad (antivirus, Firewall, WAF, IDS)
- Conocimiento en Criptografía y mecanismos de seguridad (firmas digitales, certificados)
- Conocimiento en riesgo de seguridad de la información y riesgo cibernético.
- Conocimientos de estándares y normas técnicas (ISO 27001)
- Sistema de Gestión de la Calidad
- Modelo estándar de Control Interno -MECI- (Metodología de administración de riesgos)
- Modelo Integrado de Planeación y Gestión

RANGO O CAMPO DE APLICACIÓN

- Clientes Internos y Externos
- Partes interesadas

EVIDENCIAS

DE PRODUCTO:

- Sistemas lógicos, redes y activos de información protegidos.

DE DESEMPEÑO:

- Informe de avance de actividades asignadas
- Cumplimiento normativo
- Procedimientos, políticas y manuales.
- Información con atributos de confidencialidad, disponibilidad e integridad.
- Evaluación del Desempeño del funcionario

REQUISITOS DE ESTUDIO Y EXPERIENCIA

ESTUDIOS	EXPERIENCIA

IDEA
Instituto para el Desarrollo de Antioquia

Núcleo Básico del Conocimiento: Título Profesional en Ingeniería de Sistemas, Telemática y afines. Especialización en seguridad informática, ciberseguridad o seguridad de la información. Y Tarjeta profesional en los casos requeridos por la Ley.	Cuarenta y dos (42) meses de experiencia profesional relacionada.
COMPETENCIAS LABORALES	
COMUNES	**COMPORTAMENTALES POR NIVEL**
APRENDIZAJE CONTINUO: Identificar, incorporar y aplicar nuevos conocimientos sobre regulaciones vigentes, tecnologías disponibles, métodos y programas de trabajo, para mantener actualizada la efectividad de sus prácticas laborales y su visión del contexto. **ORIENTACIÓN A RESULTADOS:** Realizar las funciones y cumplir los compromisos organizacionales con eficacia, calidad y oportunidad. **ORIENTACIÓN AL USUARIO Y AL CIUDADANO:** Dirigir las decisiones y acciones a la satisfacción de las necesidades e intereses de los usuarios (internos y externos) y de los ciudadanos, de conformidad con las responsabilidades públicas asignadas a la entidad. **COMPROMISO CON LA ORGANIZACIÓN:** Alinear el propio comportamiento a las necesidades, prioridades y metas organizacionales. **TRABAJO EN EQUIPO:** Trabajar con otros de forma integrada y armónica para la consecución de metas institucionales comunes.	**APORTE TÉCNICO PROFESIONAL:** Poner a disposición de la Administración sus saberes profesionales específicos y sus experiencias previas, gestionando la actualización de sus saberes expertos. **COMUNICACIÓN EFECTIVA:** Establecer comunicación efectiva y positiva con superiores jerárquicos, pares y ciudadanos, tanto en la expresión escrita, como verbal y gestual. **GESTIÓN DE PROCEDIMIENTOS:** Desarrollar las tareas a cargo en el marco de los procedimientos vigentes y proponer e introducir acciones para acelerar la mejora continua y la productividad. **INSTRUMENTACIÓN DE DECISIONES:** Decidir sobre las cuestiones en las que es responsable con criterios de economía, eficacia, eficiencia y transparencia de la decisión.

0012-22

IDEA
Instituto para el Desarrollo de Antioquia

ADAPTACIÓN AL CAMBIO: Enfrentar con flexibilidad las situaciones nuevas asumiendo un manejo positivo y constructivo de los cambios.	

ARTÍCULO SEGUNDO: El Director, adscrito a la Dirección De Gestión Humana, quien hace las veces de Jefe de Recurso Humano deberá entregar copia del Manual de funciones y competencias laborales determinadas en el presente acto administrativo que forma parte integral del mismo, al titular del empleo relacionado o en caso de estar vacantes una vez se posesione el servidor público que ocupe el empleo.

Los jefes inmediatos responderán por la orientación del empleado en el cumplimiento de sus funciones.

ARTÍCULO TERCERO: La presente Resolución rige a partir de la fecha de su expedición y modifica la Resolución de la Junta Directiva No. 0001 de 2019, la Resolución de Junta Directiva No. 0003 de 2021, la Resolución de Junta Directiva No. 0007 de 2021 y la Resolución de Junta Directiva No.003 de 2022, en lo que respecta a las funciones del empleo en mención del presente acto administrativo.

PARÁGRAFO: En las demás disposiciones continuara vigente los Manuales de Funciones y Competencias Laborales para los diferentes empleos de la Planta de Personal Global del Instituto para el Desarrollo de Antioquia –IDEA-, establecidos en la Resolución de Junta Directiva No. 0001 de 2019, la Resolución de Junta Directiva No. 0003 de 2021, la Resolución de Junta Directiva No. 0007 de 2021, y Resolución de Junta Directiva No.003 de 2022.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Medellín, a los 28 DIC 2022

JUAN PABLO LÓPEZ CORTÉS
PRESIDENTE O DELEGADO.
JUNTA DIRECTIVA IDEA

REGINA TATIANA URAN NAVARRO
SECRETARIO (E)
JUNTA DIRECTIVA IDEA