



Dirección de las Tecnologías y
Sistemas de Información y
de las Comunicaciones

MANUAL DE ROLES Y RESPONSABILIDADES DE LOS FUNCIONARIOS DE DTIC ISO 200001 E ISO 27001



Gestion.dtic@uptc.edu.co

[https:// www.uptc.edu.co](https://www.uptc.edu.co)

TABLA DE CONTENIDO

DIRECTOR DE TI.....	3
GESTOR DE TI.....	7
COORDINADOR DE SEDE DTIC	10
GESTOR DE LA CONFIGURACIÓN - Técnico.....	13
GESTOR DE LA MESA DE SERVICIO- Técnico.....	16
GESTOR DE LA MESA DE SERVICIO- Profesional	19
LIDER DE DESARROLLO – Profesional.....	24
LIDER DE DESARROLLO.....	27
DESARROLLADOR - Técnico	30
GESTOR DE BASE DE DATOS – Profesional Especializado.....	330
SOPORTE SISTEMAS DE INFORMACION - Profesional	36
SOPORTE A SISTEMAS DE INFORMACION - Técnico.....	39
SOPORTE SISTEMAS DE INFORMACION - Técnico.....	42
LIDER DE INFRAESTRUCTURA - Profesional Especializado	45
SOPORTE INFRAESTRUCTURA - Técnico	48
SOPORTE INFRAESTRUCTURA - Técnico	51
SOPORTE INFRAESTRUCTURA – Auxiliar	54
SOPORTE TÉCNICO - Auxiliar	57
SOPORTE TÉCNICO - Auxiliar	60
SOPORTE TÉCNICO - Auxiliar	63
SOPORTE TÉCNICO – Técnico.....	66
SOPORTE TÉCNICO – Técnico.....	69
ADMINISTRADOR AULAS DE INFORMATICA - Profesional	72
GESTOR OPERATIVO DE AULAS DE INFORMATICA - Secretaria.....	75
GESTOR OPERATIVO DE AULAS DE INFORMATICA - Auxiliar	78
GESTOR OPERATIVO DE AULAS DE INFORMATICA - Auxiliar	81
ADMINISTRADOR DE SOFTWARE - Técnico.....	84
LIDER EN EVALUACIÓN Y CONCEPTUALIZACIÓN TÉCNICA – Profesional.....	87
GESTOR GOBIERNO DIGITAL – Profesional	90
OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – Profesional.....	93
OFICIAL DE PROTECCIÓN DE DATOS PERSONALES – Profesional Especializado.....	96
ADMINISTRADOR DE CORREOS ELECTRÓNICOS – Auxiliar.....	99

DIRECTOR DE TI



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022

Nivel:	Director
Categoría:	Libre Nombramiento y Remoción
Código:	100
Grado:	17
Nombre del cargo	Director de las Tecnologías y Sistemas de Información y las Comunicaciones
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Rector

Área Funcional (Reglamentadas en el Manual de funciones Resolución: 1050 de 2018)

Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones

Área Funcional (Específica)

Constituye un área encargada de liderar la planificación, provisión, gestión y supervisión de los recursos tecnológicos de la Universidad Pedagógica y Tecnológica de Colombia. Su propósito es garantizar el soporte adecuado a los procesos misionales, académicos, administrativos y de investigación, mediante el desarrollo de soluciones digitales, la implementación de buenas prácticas en gestión de servicios TI, la seguridad de la información y la transformación digital institucional.

Como área funcional, la Dirección TIC articula políticas, proyectos y servicios tecnológicos con un enfoque basado en la mejora continua, la sostenibilidad tecnológica, el cumplimiento normativo (como ISO/IEC 27001 e ISO/IEC 20000-1), y la optimización de la infraestructura digital para apoyar una gestión universitaria eficiente, segura y orientada al usuario.

Propósito Principal (Reglamentadas en el Manual de funciones Resolución: 1050 de 2018)

Proponer, coordinar y hacer seguimiento a la implementación de las normas y políticas públicas de la Universidad; diseñar, asesorar, impulsar y poner en marcha las estrategias que contribuyen al logro de los objetivos misionales, bajo las directrices dadas por el Rector y por el Ministerio de Tecnologías de la Información y las Comunicaciones.



Propósito Especial

Liderar estratégicamente la planeación, implementación, gestión y mejora continua de los sistemas de información, infraestructura tecnológica y servicios digitales institucionales, asegurando su alineación con los objetivos misionales, académicos y administrativos de la Universidad.

Funciones Esenciales (Reglamentadas en el Manual de funciones Resolución: 1050 de 2018)

Funciones Específicas de acuerdo a la Naturaleza de la Dependencia

- (Plan de continuidad) Analizar la situación presentada y tomar la decisión de activar o no el plan de continuidad y disponibilidad.
- (Plan de continuidad) Comunicar a los funcionarios clave dentro del (Plan de Comunicaciones) la situación y las acciones a seguir, por intermedio de los responsables.
- Efectuar seguimiento al proceso de recuperación, verificando los tiempos estimados para la ejecución de las actividades.
- Planificar, dirigir y supervisar la estrategia tecnológica institucional, alineada con los objetivos misionales, académicos y administrativos de la Universidad.
- Diseñar e implementar políticas, procesos y proyectos de tecnología de la información y las comunicaciones (TIC), en concordancia con normas internacionales como ISO/IEC 27001, ISO/IEC 20000-1 y marcos de referencia como ITIL y COBIT.
- Liderar proyectos de transformación digital e innovación tecnológica, garantizando la mejora continua, eficiencia operativa y sostenibilidad de los servicios TIC.
- Asegurar la disponibilidad, integridad y confidencialidad de los activos de información institucionales mediante controles y políticas de ciberseguridad.
- Gestionar el talento humano del área TIC, promoviendo la formación continua, el trabajo en equipo y el cumplimiento de metas institucionales.
- Velar por la adecuada administración del presupuesto de TIC, incluyendo la formulación, ejecución, seguimiento y control de la inversión tecnológica.
- Articular la Dirección de TIC con otras dependencias internas y externas, generando sinergias para el desarrollo de iniciativas conjuntas en materia tecnológica.
- Coordinar auditorías internas y externas, atender requerimientos de entes de control y garantizar la trazabilidad de la gestión tecnológica.
- Monitorear tendencias tecnológicas para proponer soluciones que aporten al fortalecimiento académico, investigativo y de proyección social de la Universidad.

Responsabilidades

- Aprueba los planes definidos de la gestión del servicio



- Aprueba los Procedimientos del SGS (documentación, responsables, registros, indicadores).
- Presenta informe de gestión para la rendición de cuentas.
- Coordinar la asignación de recursos necesarios para la gestión eficiente de los servicios de TI.
- Supervisar la gestión de incidentes, problemas, cambios y niveles de servicio.
- Presenta informe de gestión para la rendición de cuentas.
- Asegurar el cumplimiento de las políticas de seguridad de la información, en concordancia con la normativa interna y los estándares internacionales.
- Rendir cuentas ante la Alta Dirección y la Universidad sobre el desempeño del SGSI, proporcionando información basada en auditorías, revisiones y análisis de riesgos.
- Validar y proponer al comité el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, y tecnología.
- Establecer estrategias de mitigación de riesgos para proteger los activos digitales y garantizar la disponibilidad, integridad y confidencialidad de la información institucional.

Conocimientos Específicos

El Director de Tecnologías debe contar con una sólida formación en áreas como ingeniería de sistemas, ingeniería electrónica, telecomunicaciones o afines, complementada con conocimientos especializados en:

- Gestión de servicios TI, con base en estándares internacionales como ISO/IEC 20000-1.
- Seguridad de la información, bajo el marco normativo de ISO/IEC 27001.
- Gobierno y gestión de TI, incluyendo buenas prácticas como ITIL, COBIT y gestión de proyectos.
- Transformación digital y automatización de procesos.
- Normatividad legal y reglamentaria del sector público aplicable a las tecnologías de la información en Colombia.
- Habilidades en liderazgo estratégico, comunicación efectiva y toma de decisiones en entornos complejos.

Formación Académica Específica

El Director de Tecnologías debe contar con título profesional en áreas relacionadas con la Ingeniería de Sistemas, Telemática y Afines; Ingeniería Eléctrica y Afines, Ingeniería Electrónica, Telecomunicaciones y Afines; Ingeniería Industrial y Afines. Es deseable contar con formación pos gradual a nivel de especialización y/o maestría en temas como:

- Gestión de Tecnologías de la Información y las Comunicaciones
- Seguridad de la Información
- Arquitectura Empresarial



- Gobierno y Gestión de TI
- Gerencia de Proyectos
- Transformación Digital
- Inteligencia Artificial
- Administración Pública o afines

Adicionalmente, se tendrá en cuenta las certificaciones en estándares internacionales y marcos de referencia como:

- ISO/IEC 27001 (Seguridad de la Información)
- ISO/IEC 20000-1 (Gestión de Servicios de TI)
- ITIL (Gestión de Servicios de TI)
- COBIT (Gobierno de TI)

Esta formación permite al Director de TIC liderar con visión estratégica, capacidad técnica y enfoque en resultados la modernización tecnológica de la Universidad.



GESTOR DE TI



**Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022**

Rol del cargo	Gestor de TI
Nivel:	Profesional
Categoría:	Carrera Administrativa
Código:	2044
Grado:	5
Nombre del cargo	Profesional Universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	2
Cargo del Manual de Funciones	Resolución: 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Planificación, coordinación y control estratégico de los servicios y sistemas de información

Propósito Principal

Liderar la implementación, mantenimiento y mejora continua del Sistema de Gestión de Servicios (SGS) conforme a la norma ISO 20000-1:2018, y del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022, asegurando la entrega eficaz, segura y alineada con los objetivos institucionales de los servicios de tecnologías de la información y comunicaciones de la UPTC.

Funciones Esenciales

- Planificar y supervisar la prestación de servicios TIC bajo los requisitos de calidad y seguridad establecidos por las normas ISO.
- Definir, revisar y actualizar políticas, procedimientos y controles asociados al SGS y SGSI.
- Coordinar auditorías internas y externas y dar seguimiento a hallazgos y acciones de mejora.



- Asegurar el cumplimiento de requisitos legales, reglamentarios, contractuales y normativos en los servicios TIC.
- Promover la gestión de riesgos y la continuidad de los servicios tecnológicos.
- Gestionar la relación con partes interesadas internas y externas vinculadas al ciclo de vida de los servicios TIC.
- Elaborar informes de desempeño del sistema de gestión para la alta dirección.
- Coordinar la formación y sensibilización del personal sobre los sistemas de gestión.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Recibir, registrar, clasificar y priorizar los incidentes y solicitudes.
- Escalar incidentes críticos al personal especializado cuando sea necesario.
- Implementar controles para proteger la información sensible de la mesa de servicio.
- Acoger las políticas y objetivos de la norma SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.
- Aplicar principios de disponibilidad, integridad y confidencialidad en el manejo de la información.
- Administrar la Mesa de Servicio como punto único de contacto entre usuarios y TI.
- Monitorear el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).
- Garantizar la satisfacción del usuario mediante tiempos de respuesta y calidad del servicio.

Registrar, clasificar, priorizar y hacer seguimiento a incidentes y solicitudes de servicio.



Conocimientos Básicos

- Estándares internacionales ISO 20000-1:2018 e ISO/IEC 27001:2022
- Gestión de servicios de TI (ITSM) y seguridad de la información
- Herramientas y metodologías de gestión de calidad y mejora continua
- Normativa legal y reglamentaria en TIC del sector público colombiano
- Auditoría de sistemas de gestión
- Herramientas de documentación y análisis de procesos
- Habilidades en liderazgo, comunicación efectiva y gestión de equipos

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, administración, finanzas o afines. Deseable formación en áreas relacionadas con gestión de proyectos, gestión de servicios TIC, seguridad de la información, auditoría o administración pública. Certificaciones en normas ISO (como auditor interno/implementador) son altamente valoradas.



COORDINADOR DE SEDE DTIC



**Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1 E ISO 27001**

Rol del cargo	Coordinadora Sede Seccional de TI
Nivel:	Profesional
Categoría:	Carrera Administrativa
Código:	2044
Grado:	5
Nombre del cargo	Profesional Universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	3
Cargo del Manual de Funciones	Resolución: 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Planificación, coordinación y control estratégico de los servicios de TI y sistemas de información

Propósito Principal

Liderar y coordinar los temas de soporte técnico, coordinación de aulas de informática, mantenimiento de equipos, soporte a los sistemas de información y la implementación, mantenimiento y mejora continua del Sistema de Gestión de Servicios (SGS) conforme a la norma ISO 20000-1:2018, y del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022, asegurando la entrega eficaz, segura y alineada con los objetivos institucionales de los servicios de tecnologías de la información y comunicaciones de la UPTC.

Funciones Esenciales

- Planificar y supervisar la prestación de servicios TIC bajo los requisitos de calidad y seguridad establecidos por las normas ISO.
- Asegurar el cumplimiento de requisitos legales, reglamentarios, contractuales y normativos en los servicios TIC.



- Promover la gestión de riesgos y la continuidad de los servicios tecnológicos.
- Elaborar informes de desempeño del sistema de gestión para la alta dirección.
- Asegurar la disponibilidad, integridad y confidencialidad de los activos de información institucionales mediante controles y políticas de ciberseguridad.
- Gestionar el talento humano del área TIC, promoviendo la formación continua, el trabajo en equipo y el cumplimiento de metas institucionales.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Recibir, registrar, clasificar y priorizar los incidentes y solicitudes.
- Escalar incidentes críticos al personal especializado cuando sea necesario.
- Implementar controles para proteger la información sensible de la mesa de servicio.
- Acoger las políticas y objetivos de la norma SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.
- Aplicar principios de disponibilidad, integridad y confidencialidad en el manejo de la información.
- Administrar la Mesa de Servicio como punto único de contacto entre usuarios y TI.
- Monitorear el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).
- Garantizar la satisfacción del usuario mediante tiempos de respuesta y calidad del servicio.



- Registrar, clasificar, priorizar y hacer seguimiento a incidentes y solicitudes de servicio.

Conocimientos Básicos

- Estándares internacionales ISO 20000-1:2018 e ISO/IEC 27001:2022
- Gestión de servicios de TI (ITSM) y seguridad de la información
- Normativa legal y reglamentaria en TIC del sector público colombiano
- Habilidades en liderazgo, comunicación efectiva y gestión de equipos
- Administración de bases de datos y sistemas de información.

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, administración, finanzas o afines. Deseable formación en áreas relacionadas con gestión de proyectos, gestión de servicios TIC, seguridad de la información, auditoría o administración pública. Certificaciones en normas ISO (como auditor interno/implementador) son altamente valoradas.



GESTOR DE LA CONFIGURACIÓN – Técnico



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor de la configuración
Nivel:	Técnico
Categoría:	Carrera Administrativa
Código:	3132
Grado	13
Nombre del cargo	Técnico operativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo de jefe inmediato	Director de TIC

Área Funcional

- Gestión del ciclo de vida de los activos de configuración (CI).
- Mantenimiento y control de la Base de Datos de Configuración (CMDB).
- Aseguramiento de la trazabilidad y coherencia de la información de configuración.
- Apoyo a la gestión del cambio y la entrega de servicios en el marco del SGS (ISO/IEC 20000-1) y SGSI (ISO/IEC 27001).

Propósito Principal

Garantizar la exactitud, actualización, integridad y consistencia de la información registrada en la CMDB, mediante la administración de los elementos de configuración y sus relaciones, asegurando su alineación con los procesos de gestión del cambio, incidentes, problemas y entregas, conforme con los requisitos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales



- Registrar, actualizar y verificar la información de los elementos de configuración (CI) y sus relaciones en la CMDB.
- Validar que los cambios implementados estén reflejados en la configuración documentada.
- Realizar auditorías de configuración para asegurar la consistencia entre el entorno real y la CMDB.
- Apoyar los procesos de cambio y entrega mediante el suministro de información confiable de configuración.
- Elaborar reportes e indicadores de control sobre la CMDB y los CI.
- Participar en auditorías internas y externas de ISO 20000-1 e ISO 27001 relacionadas con la gestión de configuración.
- Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en la CMDB.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Recibir, registrar, clasificar y priorizar los incidentes y solicitudes.
- Escalar incidentes críticos al personal especializado cuando sea necesario.
- Implementar controles para proteger la información sensible de la mesa de servicio.
- Acoger las políticas y objetivos de la norma SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.
- Aplicar principios de disponibilidad, integridad y confidencialidad en el manejo de la información.



- Administrar la Mesa de Servicio como punto único de contacto entre usuarios y TI.
- Monitorear el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).
- Garantizar la satisfacción del usuario mediante tiempos de respuesta y calidad del servicio.

Registrar, clasificar, priorizar y hacer seguimiento a incidentes y solicitudes de servicio.

Conocimientos Básicos

- Fundamentos de ITIL y gestión de configuración.
- Administración de bases de datos y sistemas de información.
- Gestión de activos y elementos de configuración (CI).
- Comprensión de procesos ITSM (gestión de cambios, entregas, incidentes, etc.).
- Nociones de seguridad de la información según ISO 27001.
- Herramientas de documentación y software para la gestión de configuración.

Formación Académica

- Técnico o tecnólogo en sistemas, informática, redes o soporte de TI.
- **Deseable:** Certificación en ITIL Foundation o formación en ISO/IEC 20000-1 y/o ISO/IEC 27001.



GESTOR DE LA MESA DE SERVICIO- Técnico



Dirección de Tecnologías y Sistemas de la Información y de las Comunicaciones
ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor de la mesa de servicio
Nivel:	Técnico
Categoría:	Carrera Administrativa
Código:	3132
Grado	13
Nombre del cargo	Técnico operativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo de jefe inmediato	Director de TIC

Área Funcional

- Gestión y operación de la mesa de servicio en tecnologías de la información
- Atención, soporte y aseguramiento de la continuidad en los servicios tecnológicos
- Gestión operativa de servicios de TI en el marco del SGS (ISO/IEC 20000-1) y SGSI (ISO/IEC 27001)

Propósito Principal

Gestionar y coordinar la atención, registro, seguimiento y solución de los requerimientos, incidentes y problemas reportados por los usuarios a través de la mesa de servicio, garantizando la calidad, trazabilidad y cumplimiento de los niveles de servicio definidos en el Catálogo de Servicios de TI, conforme a los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Atender, registrar y clasificar los requerimientos, incidentes y solicitudes de servicio reportadas por los usuarios a través de los canales establecidos.
- Hacer seguimiento a la solución de casos, coordinando con los grupos de soporte especializados hasta su cierre.
- Garantizar el cumplimiento de los tiempos de atención y solución definidos en los acuerdos de niveles de servicio (ANS).



- Participar en auditorías internas y externas relacionadas con los estándares ISO 20000-1 e ISO 27001.
- Velar por la confidencialidad, integridad y disponibilidad de la información tratada en la mesa de servicio.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Recibir, registrar, clasificar y priorizar los incidentes y solicitudes.
- Escalar incidentes críticos al personal especializado cuando sea necesario.
- Implementar controles para proteger la información sensible de la mesa de servicio.
- Acoger las políticas y objetivos de la norma SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.
- Aplicar principios de disponibilidad, integridad y confidencialidad en el manejo de la información.
- Administrar la Mesa de Servicio como punto único de contacto entre usuarios y TI.
- Monitorear el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).
- Garantizar la satisfacción del usuario mediante tiempos de respuesta y calidad del servicio.
- Registrar, clasificar, priorizar y hacer seguimiento a incidentes y solicitudes de servicio.

Conocimientos Básicos



- Fundamentos en gestión de servicios TI
- Operación de mesas de ayuda / Service desk
- Gestión de incidentes, requerimientos y problemas
- Buenas prácticas de atención al usuario y comunicación efectiva
- Nociones de ISO 20000-1:2018 e ISO 27001:2022
- Herramientas ofimáticas y colaboración (correo, chat, documentación compartida)

Formación Académica

Técnico o tecnólogo en áreas de sistemas, informática, soporte de TI.

Deseable formación complementaria o certificaciones en ISO o ITIL, gestión de TI o atención al cliente.



GESTOR DE LA MESA DE SERVICIO- Profesional



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor de la mesa de servicio
Nivel:	Profesional
Categoría:	Carrera Administrativa
Código:	2044
Grado	5
Nombre del cargo	Profesional universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo de jefe inmediato	Director de TIC

Área Funcional

- Gestión y operación de la mesa de servicio en tecnologías de la información
- Atención, soporte y aseguramiento de la continuidad en los servicios tecnológicos
- Gestión operativa de servicios de TI en el marco del SGS (ISO/IEC 20000-1) y SGSI (ISO/IEC 27001)

Propósito Principal

Gestionar y coordinar la atención, registro, seguimiento y solución de los requerimientos, incidentes y problemas reportados por los usuarios a través de la mesa de servicio, garantizando la calidad, trazabilidad y cumplimiento de los niveles de servicio definidos en el Catálogo de Servicios de TI, conforme a los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Atender, registrar y clasificar los requerimientos, incidentes y solicitudes de servicio reportadas por los usuarios a través de los canales establecidos.
- Hacer seguimiento a la solución de casos, coordinando con los grupos de soporte especializados hasta su cierre.
- Garantizar el cumplimiento de los tiempos de atención y solución definidos en los acuerdos de niveles de servicio (ANS).
- Generar reportes periódicos de gestión, tendencias, tiempos de respuesta, y retroalimentación de usuarios.
- Proponer mejoras en el proceso de atención y soporte con base en los análisis de recurrencia y causas raíz.



- Asegurar la disponibilidad y actualización del conocimiento técnico necesario para brindar soluciones eficientes.
- Participar en auditorías internas y externas relacionadas con los estándares ISO 20000-1 e ISO 27001.
- Velar por la confidencialidad, integridad y disponibilidad de la información tratada en la mesa de servicio.
- Documentar y mantener actualizados los procedimientos, formatos y manuales relacionados con la gestión de la mesa de servicio.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Recibir, registrar, clasificar y priorizar los incidentes y solicitudes.
- Escalar incidentes críticos al personal especializado cuando sea necesario.
- Implementar controles para proteger la información sensible de la mesa de servicio.
- Acoger las políticas y objetivos de la norma SGSI y del Manual de Políticas de Seguridad de la Información para su respectivo cumplimiento.
- Aplicar principios de disponibilidad, integridad y confidencialidad en el manejo de la información.
- Administrar la Mesa de Servicio como punto único de contacto entre usuarios y TI.
- Monitorear el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).



- Garantizar la satisfacción del usuario mediante tiempos de respuesta y calidad del servicio.
- Registrar, clasificar, priorizar y hacer seguimiento a incidentes y solicitudes de servicio.

Conocimientos Básicos

- Fundamentos en gestión de servicios TI
- Operación de mesas de ayuda / Service desk
- Conocimientos básicos de redes, hardware, software y sistemas operativos
- Gestión de incidentes, requerimientos y problemas
- Buenas prácticas de atención al usuario y comunicación efectiva
- Nociones de ISO 20000-1:2018 e ISO 27001:2022
- Herramientas ofimáticas y colaboración (correo, chat, documentación compartida)

Formación Académica

Profesional en áreas de sistemas, informática, soporte de TI, redes o afines.

Deseable formación complementaria o certificaciones en ISO o ITIL, gestión de servicios TI o atención al cliente.



GESTOR DE LA MESA DE SERVICIO- Auxiliar



**Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022**

Rol del cargo	Gestor de la mesa de servicio
Nivel:	Auxiliar
Categoría:	Carrera Administrativa
Código:	4044
Grado	09
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	Uno
Cargo de jefe inmediato	Director de TIC

Área Funcional

- Gestión y operación de la mesa de servicio en tecnologías de la información
- Atención, soporte y aseguramiento de la continuidad en los servicios tecnológicos
- Gestión operativa de servicios de TI en el marco del SGS (ISO/IEC 20000-1) y SGSI (ISO/IEC 27001)

Propósito Principal

Gestionar y coordinar la atención, registro, seguimiento y solución de los requerimientos, incidentes y problemas reportados por los usuarios a través de la mesa de servicio, garantizando la calidad, trazabilidad y cumplimiento de los niveles de servicio definidos en el Catálogo de Servicios de TI, conforme a los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Atender, registrar y clasificar los requerimientos, incidentes y solicitudes de servicio reportadas por los usuarios a través de los canales establecidos.
- Hacer seguimiento a la solución de casos, coordinando con los grupos de soporte especializados hasta su cierre.
- Apoyar el cumplimiento de los tiempos de atención y solución definidos en los acuerdos de niveles de servicio (ANS)



- Participar en auditorías internas y externas relacionadas con los estándares ISO 20000-1 e ISO 27001.
- Velar por la confidencialidad, integridad y disponibilidad de la información tratada en la mesa de servicio.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Conocimientos Básicos

- Fundamentos en gestión de TI
- Operación de mesas de ayuda / Service desk
- Gestión de incidentes, requerimientos y problemas
- Buenas prácticas de atención al usuario y comunicación efectiva
- Nociones de ISO 20000-1:2018 e ISO 27001:2022
- Herramientas ofimáticas y colaboración (correo, chat, documentación compartida)

Formación Académica

Bachiller con conocimiento en áreas de sistemas, informática, soporte de TI.



LIDER DE DESARROLLO – Profesional



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Líder de desarrollo
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	7
Nombre del cargo	Profesional Universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución: 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Diseño, desarrollo, integración, mantenimiento y mejora de soluciones tecnológicas institucionales.

Propósito Principal

Diseñar, construir y mantener soluciones de software y sistemas de información que respondan a las necesidades estratégicas, operativas y normativas de la Universidad, garantizando calidad, seguridad, interoperabilidad y cumplimiento con las buenas prácticas de gestión de servicios (ISO 20000-1:2018) y seguridad de la información (ISO 27001:2022).

Funciones Esenciales

- Analizar, diseñar, desarrollar y probar sistemas y aplicaciones informáticas para las distintas áreas de la UPTC.
- Garantizar que los desarrollos cumplan con los requisitos funcionales, de calidad, seguridad y accesibilidad.
- Participar en la gestión del ciclo de vida del software, desde la planificación hasta el mantenimiento.
- Aplicar metodologías ágiles, DevOps o tradicionales según las características del proyecto.



- Integrar los sistemas de información institucionales entre sí y con servicios de terceros, asegurando consistencia y eficiencia.
- Documentar adecuadamente los desarrollos y generar manuales técnicos y de usuario.
- Atender incidentes o requerimientos relacionados con los sistemas desarrollados.
- Velar por la protección de los datos personales, la seguridad del código y la continuidad de los sistemas.
- Realizar auditorías a los sistemas de información
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Evaluar y responder a las solicitudes de creación o modificación de los sistemas de información, determinando la viabilidad de su desarrollo.
- Realizar diseño, desarrollo, pruebas de funcionalidad y entrega de despliegue de la solicitud.
- Documentar los cambio o problemas presentados en los sistemas de información.
- Realizar verificaciones y auditorías a los sistemas de información periódicamente o cuando sea necesario para garantizar su integridad y seguridad.
- Documentar el código y los procesos de desarrollo.
- Implementar cambios de manera controlada según la gestión de cambios.



- Corregir defectos y mejorar funcionalidades según lo requerido.

Conocimientos Básicos

- Lenguajes de programación (como Java, Python, PHP, JavaScript, etc.)
- Bases de datos relacionales y no relacionales
- Arquitectura de software, APIs y servicios web
- Normas ISO 20000-1:2018 e ISO 27001:2022 aplicadas al desarrollo seguro y a la gestión del ciclo de vida del software
- Metodologías de desarrollo ágil y gestión de versiones (Git)
- Ciberseguridad básica y desarrollo seguro (OWASP, cifrado, autenticación)
- Conocimiento de procesos institucionales en el sector educativo (deseable)

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería de Software, Ingeniería Electrónica o afines. Estudios en desarrollo de software, ingeniería de software, seguridad informática o gestión de proyectos TIC. Certificaciones en metodologías ágiles, desarrollo seguro o estándares ISO son un valor agregado.

LIDER DE DESARROLLO



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Líder de desarrollo
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	5
Nombre del cargo	Profesional Universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución: 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Diseño, desarrollo, integración, mantenimiento y mejora de soluciones tecnológicas institucionales.

Propósito Principal

Diseñar, construir y mantener soluciones de software y sistemas de información que respondan a las necesidades estratégicas, operativas y normativas de la Universidad, garantizando calidad, seguridad, interoperabilidad y cumplimiento con las buenas prácticas de gestión de servicios (ISO 20000-1:2018) y seguridad de la información (ISO 27001:2022).

Funciones Esenciales

- Analizar, diseñar, desarrollar y probar sistemas y aplicaciones informáticas para las distintas áreas de la UPTC.
- Garantizar que los desarrollos cumplan con los requisitos funcionales, de calidad, seguridad y accesibilidad.
- Participar en la gestión del ciclo de vida del software, desde la planificación hasta el mantenimiento.
- Integrar los sistemas de información institucionales entre sí y con servicios de terceros, asegurando consistencia y eficiencia.



- Documentar adecuadamente los desarrollos y generar manuales técnicos y de usuario.
- Atender incidentes o requerimientos relacionados con los sistemas desarrollados.
- Velar por la protección de los datos personales, la seguridad del código y la continuidad de los sistemas.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
- Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Evaluar y responder a las solicitudes de creación o modificación de los sistemas de información, determinando la viabilidad de su desarrollo.
- Realizar diseño, desarrollo, pruebas de funcionalidad y entrega de despliegue de la solicitud.
- Documentar los cambio o problemas presentados en los sistemas de información.
- Realizar verificaciones y auditorías a los sistemas de información periódicamente o cuando sea necesario para garantizar su integridad y seguridad.
- Documentar el código y los procesos de desarrollo.
- Implementar cambios de manera controlada según la gestión de cambios.
- Corregir defectos y mejorar funcionalidades según lo requerido.

Conocimientos Básicos

- Lenguajes de programación (como Java, Python, PHP, JavaScript, etc.)
- Bases de datos relacionales y no relacionales



- Arquitectura de software, APIs y servicios web
- Normas ISO 20000-1:2018 e ISO 27001:2022 aplicadas al desarrollo seguro y a la gestión del ciclo de vida del software
- Metodologías de desarrollo ágil y gestión de versiones (Git)
- Desarrollo seguro (OWASP, cifrado, autenticación)

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería de Software, Ingeniería Electrónica o afines. Estudios en desarrollo de software, ingeniería de software, seguridad informática o gestión de proyectos TIC. Certificaciones en metodologías ágiles, desarrollo seguro o estándares ISO son un valor agregado.



DESARROLLADOR- Técnico

Coding



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Desarrollador
Nivel	Técnico
Categoría	Carrera administrativa
Código	2044
Grado	12
Nombre del cargo	Técnico administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución: 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Diseño, desarrollo, integración, mantenimiento y mejora de soluciones tecnológicas institucionales.

Propósito Principal

Diseñar, construir y mantener soluciones de software y sistemas de información que respondan a las necesidades estratégicas, operativas y normativas de la Universidad, garantizando calidad, seguridad, interoperabilidad y cumplimiento con las buenas prácticas de gestión de servicios (ISO 20000-1:2018) y seguridad de la información (ISO 27001:2022).

Funciones Esenciales

- Analizar, diseñar, desarrollar y probar sistemas y aplicaciones informáticas para las distintas áreas de la UPTC.
- Garantizar que los desarrollos cumplan con los requisitos funcionales, de calidad, seguridad y accesibilidad.
- Participar en la gestión del ciclo de vida del software, desde la planificación hasta el mantenimiento.
- Aplicar metodologías ágiles, DevOps o tradicionales según las características del proyecto.



- Integrar los sistemas de información institucionales entre sí y con servicios de terceros, asegurando consistencia y eficiencia.
- Documentar adecuadamente los desarrollos y generar manuales técnicos y de usuario.
- Atender incidentes o requerimientos relacionados con los sistemas desarrollados.
- Velar por la protección de los datos personales, la seguridad del código y la continuidad de los sistemas.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Evaluar y responder a las solicitudes de creación o modificación de los sistemas de información, determinando la viabilidad de su desarrollo.
- Realizar diseño, desarrollo, pruebas de funcionalidad y entrega de despliegue de la solicitud.
- Documentar los cambio o problemas presentados en los sistemas de información.
- Realizar verificaciones y auditorías a los sistemas de información periódicamente o cuando sea necesario para garantizar su integridad y seguridad.
- Documentar el código y los procesos de desarrollo.
- Implementar cambios de manera controlada según la gestión de cambios.

- Corregir defectos y mejorar funcionalidades según lo requerido.

Conocimientos Básicos

- Lenguajes de programación (como Java, Python, PHP, JavaScript, etc.)
- Bases de datos relacionales y no relacionales
- Arquitectura de software, APIs y servicios web
- Normas ISO 20000-1:2018 e ISO 27001:2022 aplicadas al desarrollo seguro y a la gestión del ciclo de vida del software
- Metodologías de desarrollo ágil y gestión de versiones (Git)
- Ciberseguridad básica y desarrollo seguro (OWASP, cifrado, autenticación)
- Conocimiento de procesos institucionales en el sector educativo (deseable)

Formación Académica

Técnico en Sistemas, conocimiento en Software, Electrónica o afines. Estudios en desarrollo de software, seguridad informática o gestión de proyectos TIC. Conocimiento en metodologías ágiles, desarrollo seguro o estándares ISO son un valor agregado.



GESTOR DE BASE DE DATOS – Especializado



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor de bases de datos
Nivel	Profesional
Categoría	Carrera administrativa
Código	2028
Grado	14
Nombre del cargo	Profesional Especializado
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Administración, monitoreo, respaldo, integridad y seguridad de las bases de datos institucionales.

Propósito Principal

Administrar de forma eficiente y segura las bases de datos institucionales, garantizando su disponibilidad, integridad, confidencialidad y rendimiento, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los estándares ISO/IEC 20000-1:2018 e ISO/IEC 27001:2022.

Funciones Esenciales

- Administrar, monitorear y mantener operativas las bases de datos utilizadas en los sistemas de información institucionales.
- Garantizar la integridad y disponibilidad de los datos mediante planes de respaldo, recuperación y alta disponibilidad.
- Implementar controles de acceso y medidas de seguridad que aseguren la confidencialidad de la información almacenada.



- Realizar ajustes de rendimiento (tuning), optimización de consultas y mantenimiento preventivo.
- Apoyar al equipo de desarrollo en el diseño e implementación de estructuras de bases de datos eficientes y seguras.
- Documentar esquemas, políticas de acceso, planes de respaldo y procedimientos técnicos asociados a las bases de datos.
- Atender incidentes o requerimientos técnicos relacionados con las plataformas de datos.
- Participar en auditorías técnicas y de seguridad de la información, garantizando el cumplimiento normativo.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Realizar con regularidad la verificación de permisos asignados sobre la base de datos y hacer la depuración e inactivación correspondiente.
- Realizar verificaciones y auditorías a las bases de datos periódicamente o cuando sea necesario para garantizar su integridad y seguridad.
- Garantizar la disponibilidad y rendimiento de las bases de datos.
- Implementar medidas de seguridad y copias de respaldo periódicas.



- Controlar el acceso a la información según políticas establecidas.

Conocimientos Básicos

- Administración de sistemas gestores de bases de datos (Oracle, PostgreSQL, SQL Server, MySQL, etc.)
- Lenguaje SQL y optimización de consultas
- Modelado de datos, normalización y relaciones entre entidades
- Planes de respaldo, recuperación ante desastres y continuidad operativa
- Seguridad en bases de datos: cifrado, control de accesos, auditorías
- Fundamentos de ISO 20000-1:2018 e ISO/IEC 27001:2022
- Conocimientos básicos en sistemas operativos (Linux, Windows Server)
- Herramientas de monitoreo de desempeño (p. ej. Oracle Enterprise Manager, pgAdmin, etc.)

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Software o afines. con Especialización en bases de datos, seguridad informática o ingeniería de software. Con certificaciones en administración de bases de datos (Oracle, PostgreSQL, Microsoft SQL Server), seguridad de la información o gestión de servicios.



SOPORTE SISTEMAS DE INFORMACION - Profesional



**Dirección de las Tecnologías y Sistemas de la
Información y de las Comunicaciones**

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Soporte a Sistemas de Información
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	05
Nombre del cargo	Profesional Universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	5
Cargo del manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Soporte técnico y funcional a los sistemas de información institucionales.

Propósito Principal

Brindar soporte técnico, funcional y operativo a los usuarios de los sistemas de información institucionales, asegurando su disponibilidad, correcto funcionamiento, trazabilidad de incidentes y continuidad del servicio, de acuerdo con los lineamientos definidos en el Sistema de Gestión de Servicios (SGS) y en el Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Atender, analizar y resolver incidentes, requerimientos y consultas relacionados con los sistemas de información institucionales.
- Registrar, clasificar y hacer seguimiento a los casos mediante el sistema de gestión de tickets definido por la DTIC.
- Verificar el correcto funcionamiento de los módulos del sistema, reportar errores técnicos y validar soluciones con el equipo de desarrollo.



- Capacitar y acompañar a los usuarios finales en el uso adecuado de los sistemas, tanto de forma presencial como remota.
- Participar en las pruebas funcionales y técnicas de nuevos desarrollos o actualizaciones del sistema.
- Colaborar en el aseguramiento de la disponibilidad y confidencialidad de los datos, en cumplimiento de la norma ISO/IEC 27001:2022.
- Apoyar procesos de auditoría interna y externa relacionados con la operación y uso de los sistemas.
- Proponer mejoras en la experiencia de usuario y funcionalidad de los sistemas de información.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Registrar, clasificar y hacer seguimiento a los casos mediante el sistema de gestión de tickets definido por la DTIC.
- Verificar el correcto funcionamiento de los módulos del sistema, reportar errores técnicos y validar soluciones con el equipo de desarrollo.
- Capacitar y acompañar a los usuarios finales en el uso adecuado de los sistemas, tanto de forma presencial como remota.
- Documentar procedimientos, soluciones y recomendaciones técnicas en la base de conocimiento de la Mesa de Servicio.
- Participar en las pruebas funcionales y técnicas de nuevos desarrollos o actualizaciones del sistema.



- Colaborar en el aseguramiento de la disponibilidad y confidencialidad de los datos, en cumplimiento de la norma ISO/IEC 27001:2022.
- Apoyar procesos de auditoría interna y externa relacionados con la operación y uso de los sistemas.
- Proponer mejoras en la experiencia de usuario y funcionalidad de los sistemas de información.

Conocimientos Básicos

- Operación y uso funcional de sistemas de información académicos, administrativos y financieros.
- Gestión de incidentes y requerimientos bajo modelos de ITIL o ISO 20000-1.
- Conocimientos básicos en bases de datos, sistemas operativos y navegadores.
- Manejo de herramientas ofimáticas y colaboración en línea.
- Principios de seguridad de la información (ISO 27001): protección de datos, acceso autorizado, respaldo.
- Competencias en atención al usuario, comunicación efectiva y solución de problemas.

Formación Académica

Profesional en Ingeniería de sistemas, informática, soporte TI o afines. Con estudios en atención al usuario, sistemas de información institucionales y gestión de servicios TI.



SOPORTE A SISTEMAS DE INFORMACION



**Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022**

Rol del cargo	Soporte a Sistemas de Información
Nivel	Profesional
Categoría	Carrera administrativa
Código	2028
Grado	11
Nombre del cargo	Profesional Especializado
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Soporte técnico y funcional a los sistemas de información institucionales.

Propósito Principal

Brindar soporte técnico, funcional y operativo a los usuarios de los sistemas de información institucionales, asegurando su disponibilidad, correcto funcionamiento, trazabilidad de incidentes y continuidad del servicio, de acuerdo con los lineamientos definidos en el Sistema de Gestión de Servicios (SGS) y en el Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Atender, analizar y resolver incidentes, requerimientos y consultas relacionados con los sistemas de información institucionales.
- Registrar, clasificar y hacer seguimiento a los casos mediante el sistema de gestión de tickets definido por la DTIC.
- Verificar el correcto funcionamiento de los módulos del sistema, reportar errores técnicos y validar soluciones con el equipo de desarrollo.



- Capacitar y acompañar a los usuarios finales en el uso adecuado de los sistemas, tanto de forma presencial como remota.
- Documentar procedimientos, soluciones y recomendaciones técnicas en la base de conocimiento de la Mesa de Servicio.
- Participar en las pruebas funcionales y técnicas de nuevos desarrollos o actualizaciones del sistema.
- Colaborar en el aseguramiento de la disponibilidad y confidencialidad de los datos, en cumplimiento de la norma ISO/IEC 27001:2022.
- Apoyar procesos de auditoría interna y externa relacionados con la operación y uso de los sistemas.
- Proponer mejoras en la experiencia de usuario y funcionalidad de los sistemas de información.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Hacer entrega de los datos solicitados teniendo en cuenta los protocolos de seguridad en la transferencia de información.
- Monitorear la operación y el rendimiento de los sistemas de información.



- Gestionar cuentas de usuarios y asignar recursos a las mismas.
- Realizar investigación y seguimiento a las peticiones e incidencias con el fin de establecer la causa raíz y las posibles soluciones efectivas y recomendaciones de mejora para los sistemas de información involucrados
- Realizar actividades en conjunto con otros procesos de la entidad cuando sea requerido (Cierres académicos, financieros, matriculas, pagos salariales entre otros)
- Cuando el requerimiento sea un cambio, documentar lo pertinente, teniendo en cuenta el procedimiento Gestión de Cambios.

Conocimientos Básicos

- Operación y uso funcional de sistemas de información académicos, administrativos y financieros.
- Gestión de incidentes y requerimientos bajo modelos de ITIL o ISO 20000-1.
- Conocimientos básicos en bases de datos, sistemas operativos y navegadores.
- Manejo de herramientas ofimáticas y colaboración en línea.
- Principios de seguridad de la información (ISO 27001): protección de datos, acceso autorizado, respaldo.
- Competencias en atención al usuario, comunicación efectiva y solución de problemas.

Formación Académica

Profesional en Ingeniería de sistemas, informática, soporte TI o afines. Con estudios profesionales en Ingeniería de Sistemas o Ingeniería Informática. Con formación complementaria en atención al usuario, sistemas de información institucionales y gestión de servicios TI.

SOPORTE SISTEMAS DE INFORMACION - Técnico



shutterstock.com - 2299020145

Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Soporte a Sistemas de Información
Nivel	Técnico
Categoría	Carrera administrativa
Código	4044
Grado	09
Nombre del cargo	Técnico administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	2
Cargo del manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Soporte técnico y funcional a los sistemas de información institucionales.

Propósito Principal

Brindar soporte técnico, funcional y operativo a los usuarios de los sistemas de información institucionales, asegurando su disponibilidad, correcto funcionamiento, trazabilidad de incidentes y continuidad del servicio, de acuerdo con los lineamientos definidos en el Sistema de Gestión de Servicios (SGS) y en el Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Atender, analizar y resolver incidentes, requerimientos y consultas relacionados con los sistemas de información institucionales.
- Registrar, clasificar y hacer seguimiento a los casos mediante el sistema de gestión de tickets definido por la DTIC.
- Verificar el correcto funcionamiento de los módulos del sistema, reportar errores técnicos y validar soluciones con el equipo de desarrollo.



- Capacitar y acompañar a los usuarios finales en el uso adecuado de los sistemas, tanto de forma presencial como remota.
- Documentar procedimientos, soluciones y recomendaciones técnicas en la base de conocimiento de la Mesa de Servicio.
- Participar en las pruebas funcionales y técnicas de nuevos desarrollos o actualizaciones del sistema.
- Colaborar en el aseguramiento de la disponibilidad y confidencialidad de los datos, en cumplimiento de la norma ISO/IEC 27001:2022.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Hacer entrega de los datos solicitados teniendo en cuenta los protocolos de seguridad en la transferencia de información.
- Monitorear la operación y el rendimiento de los sistemas de información.
- Gestionar cuentas de usuarios y asignar recursos a las mismas.
- Realizar investigación y seguimiento a las peticiones e incidencias con el fin de establecer la causa raíz y las posibles soluciones efectivas y recomendaciones de mejora para los sistemas de información involucrados

- Realizar actividades en conjunto con otros procesos de la entidad cuando sea requerido (Cierres académicos, financieros, matrículas, pagos salariales entre otros)
- Cuando el requerimiento sea un cambio, documentar lo pertinente, teniendo en cuenta el procedimiento Gestión de Cambios.

Conocimientos Básicos

- Operación y uso funcional de sistemas de información académicos, administrativos y financieros.
- Gestión de incidentes y requerimientos bajo modelos de ITIL o ISO 20000-1.
- Conocimientos básicos en bases de datos, sistemas operativos y navegadores.
- Manejo de herramientas ofimáticas y colaboración en línea.
- Principios de seguridad de la información (ISO 27001): protección de datos, acceso autorizado, respaldo.
- Competencias en atención al usuario, comunicación efectiva y solución de problemas.

Formación Académica

Técnico o tecnólogo en sistemas, informática, soporte TI o afines. Con estudios en Sistemas o Informática. Formación complementaria en atención al usuario, sistemas de información institucionales y gestión de servicios TI.



LIDER DE INFRAESTRUCTURA - Profesional Especializado



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Líder de Infraestructura
Nivel	Profesional
Categoría	Carrera administrativa
Código	2028
Grado	14
Nombre del cargo	Profesional especializado
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión, mantenimiento, monitoreo y soporte de la infraestructura tecnológica institucional (redes, servidores, comunicaciones, energía y centros de datos).

Propósito Principal

Diseñar, administrar y mantener la infraestructura tecnológica de la Universidad, incluyendo redes, conectividad, servidores, sistemas de respaldo, energía y comunicaciones, garantizando la continuidad, disponibilidad, seguridad y rendimiento de los servicios tecnológicos institucionales, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (ISO 20000-1:2018) y el Sistema de Gestión de Seguridad de la Información (ISO 27001:2022).

Funciones Esenciales

- Instalar, configurar, mantener y monitorear servidores físicos y virtuales, equipos de red, switches, routers, firewalls y otros activos tecnológicos de la infraestructura.
- Asegurar la disponibilidad y estabilidad de los servicios de red e internet, gestionando activamente el rendimiento de la infraestructura.



- Implementar y controlar políticas de respaldo, recuperación ante desastres y continuidad operativa.
- Garantizar la seguridad de la infraestructura mediante controles físicos y lógicos, aplicando estándares de seguridad informática y ciberseguridad.
- Documentar topologías, configuraciones, inventarios y procedimientos técnicos relacionados con la infraestructura tecnológica.
- Gestionar la conectividad entre sedes, incluyendo enlaces, troncales, puntos de acceso inalámbrico y cableado estructurado.
- Apoyar en auditorías internas y externas, y participar en análisis de riesgo e implementación de controles preventivos.
- Realizar mantenimiento preventivo y correctivo a los componentes de la infraestructura tecnológica.
- Asesorar técnicamente a otras áreas en aspectos relacionados con conectividad, infraestructura, almacenamiento y servidores.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Gestionar redes cableadas e inalámbricas para garantizar la conectividad estable y segura.
- Asegurar la disponibilidad de los servicios tecnológicos mediante la gestión de servidores, almacenamiento y redes.
- Implementar mecanismos de seguridad para proteger la red de accesos no autorizados o ataques



cibernéticos.

- Asegurar la disponibilidad de recursos tecnológicos.
- Documentar procedimientos y configuraciones para asegurar la continuidad del negocio.
- Realizar monitoreo de seguridad con el uso de herramientas asignadas para tal fin y gestionar las mejoras necesarias.
- Realizar monitoreo de rendimiento y funcionalidad de la red de la universidad, generar reportes y gestionar las mejoras necesarias.
- Administración y supervisión de la configuración de los elementos de comunicación y tecnologías convergentes.
- Establecer estrategias que permitan determinar la infraestructura tecnológica adecuada y los proveedores que cumplan los requisitos determinados por la universidad para el aprovisionamiento de estos elementos en un momento determinado.

Conocimientos Básicos

- Redes de datos: TCP/IP, VLAN, VPN, routing, switching, direccionamiento, IPv4/IPv6.
- Administración de servidores (Windows Server, Linux), virtualización (VMware, Hyper-V, Proxmox).
- Gestión de infraestructura física: cableado estructurado, energía regulada, UPS, climatización, racks.
- Sistemas de respaldo, recuperación de desastres y alta disponibilidad.
- Herramientas de monitoreo de red y servicios (Zabbix, PRTG, Nagios, etc.).
- Fundamentos de ciberseguridad, control de accesos, segmentación de red.
- Estándares ISO/IEC 20000-1 e ISO/IEC 27001 aplicados a infraestructura.
- Capacidad de análisis, respuesta ante incidentes y documentación técnica.

Formación Académica

Técnico, tecnólogo o profesional en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Deseable formación complementaria o certificaciones en redes (Cisco, MikroTik), virtualización, administración de servidores y seguridad informática. Se valoran conocimientos y formación en gestión de servicios TI (ITIL) y normas ISO.



SOPORTE INFRAESTRUCTURA – Técnico



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Soporte infraestructura
Nivel	Técnico
Categoría	Carrera administrativa
Código	3132
Grado	13
Nombre del cargo	Técnico operativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	2
Cargo del Manual de Funciones	Resolución 1050de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión, mantenimiento, monitoreo y soporte de la infraestructura tecnológica institucional (redes, servidores, comunicaciones, energía y centros de datos).

Propósito Principal

Diseñar, administrar y mantener la infraestructura tecnológica de la Universidad, incluyendo redes, conectividad, servidores, sistemas de respaldo, energía y comunicaciones, garantizando la continuidad, disponibilidad, seguridad y rendimiento de los servicios tecnológicos institucionales, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (ISO 20000-1:2018) y el Sistema de Gestión de Seguridad de la Información (ISO 27001:2022).

Funciones Esenciales

- Instalar, configurar, mantener y monitorear servidores físicos y virtuales, equipos de red, switches, routers, firewalls y otros activos tecnológicos de la infraestructura.
- Asegurar la disponibilidad y estabilidad de los servicios de red e internet, gestionando activamente el rendimiento de la infraestructura.



- Implementar y controlar políticas de respaldo, recuperación ante desastres y continuidad operativa.
- Garantizar la seguridad de la infraestructura mediante controles físicos y lógicos, aplicando estándares de seguridad informática y ciberseguridad.
- Documentar topologías, configuraciones, inventarios y procedimientos técnicos relacionados con la infraestructura tecnológica.
- Gestionar la conectividad entre sedes, incluyendo enlaces, troncales, puntos de acceso inalámbrico y cableado estructurado.
- Apoyar en auditorías internas y externas, y participar en análisis de riesgo e implementación de controles preventivos.
- Realizar mantenimiento preventivo y correctivo a los componentes de la infraestructura tecnológica.
- Asesorar técnicamente a otras áreas en aspectos relacionados con conectividad, infraestructura, almacenamiento y servidores.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Gestionar redes cableadas e inalámbricas para garantizar la conectividad estable y segura.
- Asegurar la disponibilidad de los servicios tecnológicos mediante la gestión de servidores, almacenamiento y redes.



- Implementar mecanismos de seguridad para proteger la red de accesos no autorizados o ataques cibernéticos.
- Asegurar la disponibilidad de recursos tecnológicos.
- Documentar procedimientos y configuraciones para asegurar la continuidad del negocio.
- Realizar monitoreo de seguridad con el uso de herramientas asignadas para tal fin y gestionar las mejoras necesarias.
- Realizar monitoreo de rendimiento y funcionalidad de la red de la universidad, generar reportes y gestionar las mejoras necesarias.
- Administración y supervisión de la configuración de los elementos de comunicación y tecnologías convergentes.
- Establecer estrategias que permitan determinar la infraestructura tecnológica adecuada y los proveedores que cumplan los requisitos determinados por la universidad para el aprovisionamiento de estos elementos en un momento determinado.

Conocimientos Básicos

- Redes de datos: TCP/IP, VLAN, VPN, routing, switching, direccionamiento, IPv4/IPv6.
- Administración de servidores (Windows Server, Linux), virtualización (VMware, Hyper-V, Proxmox).
- Gestión de infraestructura física: cableado estructurado, energía regulada, UPS, climatización, racks.
- Sistemas de respaldo, recuperación de desastres y alta disponibilidad.
- Herramientas de monitoreo de red y servicios (Zabbix, PRTG, Nagios, etc.).
- Fundamentos de ciberseguridad, control de accesos, segmentación de red.
- Estándares ISO/IEC 20000-1 e ISO/IEC 27001 aplicados a infraestructura.
- Capacidad de análisis, respuesta ante incidentes y documentación técnica.

Formación Académica

Técnico, tecnólogo o profesional en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Deseable formación complementaria o certificaciones en redes (Cisco, MikroTik), virtualización, administración de servidores y seguridad informática. Se valoran conocimientos y formación en gestión de servicios TI (ITIL) y normas ISO.



SOPORTE INFRAESTRUCTURA – Técnico



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Soporte infraestructura
Nivel	Técnico
Categoría	Carrera administrativa
Código	3124
Grado	12
Nombre del cargo	Técnico administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	2
Cargo del Manual de Funciones	Resolución 1050de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión, mantenimiento, monitoreo y soporte de la infraestructura tecnológica institucional (redes, servidores, comunicaciones, energía y centros de datos).

Propósito Principal

Diseñar, administrar y mantener la infraestructura tecnológica de la Universidad, incluyendo redes, conectividad, servidores, sistemas de respaldo, energía y comunicaciones, garantizando la continuidad, disponibilidad, seguridad y rendimiento de los servicios tecnológicos institucionales, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (ISO 20000-1:2018) y el Sistema de Gestión de Seguridad de la Información (ISO 27001:2022).

Funciones Esenciales

- Instalar, configurar, mantener y monitorear servidores físicos y virtuales, equipos de red, switches, routers, firewalls y otros activos tecnológicos de la infraestructura.
- Asegurar la disponibilidad y estabilidad de los servicios de red e internet, gestionando activamente el rendimiento de la infraestructura.
- Implementar y controlar políticas de respaldo, recuperación ante desastres y continuidad operativa.
- Garantizar la seguridad de la infraestructura mediante controles físicos y lógicos, aplicando estándares de seguridad informática y ciberseguridad.
- Documentar topologías, configuraciones, inventarios y procedimientos técnicos relacionados con la infraestructura tecnológica.



- Gestionar la conectividad entre sedes, incluyendo enlaces, troncales, puntos de acceso inalámbrico y cableado estructurado.
- Apoyar en auditorías internas y externas, y participar en análisis de riesgo e implementación de controles preventivos.
- Realizar mantenimiento preventivo y correctivo a los componentes de la infraestructura tecnológica.
- Asesorar técnicamente a otras áreas en aspectos relacionados con conectividad, infraestructura, almacenamiento y servidores.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Gestionar redes cableadas e inalámbricas para garantizar la conectividad estable y segura.
- Asegurar la disponibilidad de los servicios tecnológicos mediante la gestión de servidores, almacenamiento y redes.
- Implementar mecanismos de seguridad para proteger la red de accesos no autorizados o ataques cibernéticos.
- Asegurar la disponibilidad de recursos tecnológicos.



- Documentar procedimientos y configuraciones para asegurar la continuidad del negocio.
- Realizar monitoreo de seguridad con el uso de herramientas asignadas para tal fin y gestionar las mejoras necesarias.
- Realizar monitoreo de rendimiento y funcionalidad de la red de la universidad, generar reportes y gestionar las mejoras necesarias.
- Administración y supervisión de la configuración de los elementos de comunicación y tecnologías convergentes.
- Establecer estrategias que permitan determinar la infraestructura tecnológica adecuada y los proveedores que cumplan los requisitos determinados por la universidad para el aprovisionamiento de estos elementos en un momento determinado.

Conocimientos Básicos

- Redes de datos: TCP/IP, VLAN, VPN, routing, switching, direccionamiento, IPv4/IPv6.
- Administración de servidores (Windows Server, Linux), virtualización (VMware, Hyper-V, Proxmox).
- Gestión de infraestructura física: cableado estructurado, energía regulada, UPS, climatización, racks.
- Sistemas de respaldo, recuperación de desastres y alta disponibilidad.
- Herramientas de monitoreo de red y servicios (Zabbix, PRTG, Nagios, etc.).
- Fundamentos de ciberseguridad, control de accesos, segmentación de red.
- Estándares ISO/IEC 20000-1 e ISO/IEC 27001 aplicados a infraestructura.
- Capacidad de análisis, respuesta ante incidentes y documentación técnica.

Formación Académica

Técnico, tecnólogo o profesional en ingeniería de sistemas, telecomunicaciones, electrónica o afines. Deseable formación complementaria o certificaciones en redes (Cisco, MikroTik), virtualización, administración de servidores y seguridad informática. Se valoran conocimientos y formación en gestión de servicios TI (ITIL) y normas ISO.



SOPORTE INFRAESTRUCTURA – Auxiliar



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Soporte infraestructura
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
Grado	13
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión, mantenimiento, monitoreo y soporte de la infraestructura tecnológica institucional (redes, servidores, comunicaciones, energía y centros de datos).

Propósito Principal

Diseñar, administrar y mantener la infraestructura tecnológica de la Universidad, incluyendo redes, conectividad, servidores, sistemas de respaldo, energía y comunicaciones, garantizando la continuidad, disponibilidad, seguridad y rendimiento de los servicios tecnológicos institucionales, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (ISO 20000-1:2018) y el Sistema de Gestión de Seguridad de la Información (ISO 27001:2022).

Funciones Esenciales

- Instalar, configurar, mantener y monitorear servidores físicos y virtuales, equipos de red, switches, routers, firewalls y otros activos tecnológicos de la infraestructura.
- Asegurar la disponibilidad y estabilidad de los servicios de red e internet, gestionando activamente el rendimiento de la infraestructura.



- Implementar y controlar políticas de respaldo, recuperación ante desastres y continuidad operativa.
- Garantizar la seguridad de la infraestructura mediante controles físicos y lógicos, aplicando estándares de seguridad informática y ciberseguridad.
- Documentar topologías, configuraciones, inventarios y procedimientos técnicos relacionados con la infraestructura tecnológica.
- Gestionar la conectividad entre sedes, incluyendo enlaces, troncales, puntos de acceso inalámbrico y cableado estructurado.
- Apoyar en auditorías internas y externas, y participar en análisis de riesgo e implementación de controles preventivos.
- Realizar mantenimiento preventivo y correctivo a los componentes de la infraestructura tecnológica.
- Asesorar técnicamente a otras áreas en aspectos relacionados con conectividad, infraestructura, almacenamiento y servidores.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Gestionar redes cableadas e inalámbricas para garantizar la conectividad estable y segura.
- Asegurar la disponibilidad de los servicios tecnológicos mediante la gestión de servidores, almacenamiento y redes.
- Implementar mecanismos de seguridad para proteger la red de accesos no autorizados o ataques cibernéticos.
- Asegurar la disponibilidad de recursos tecnológicos.



- Documentar procedimientos y configuraciones para asegurar la continuidad del negocio.
- Realizar monitoreo de seguridad con el uso de herramientas asignadas para tal fin y gestionar las mejoras necesarias.
- Realizar monitoreo de rendimiento y funcionalidad de la red de la universidad, generar reportes y gestionar las mejoras necesarias.
- Administración y supervisión de la configuración de los elementos de comunicación y tecnologías convergentes.

Establecer estrategias que permitan determinar la infraestructura tecnológica adecuada y los proveedores que cumplan los requisitos determinados por la universidad para el aprovisionamiento de estos elementos en un momento determinado.

Conocimientos Básicos

- Redes de datos: TCP/IP, VLAN, VPN, routing, switching, direccionamiento, IPv4/IPv6.
- Administración de servidores (Windows Server, Linux), virtualización (VMware, Hyper-V, Proxmox).
- Gestión de infraestructura física: cableado estructurado, energía regulada, UPS, climatización, racks.
- Sistemas de respaldo, recuperación de desastres y alta disponibilidad.
- Herramientas de monitoreo de red y servicios (Zabbix, PRTG, Nagios, etc.).
- Fundamentos de ciberseguridad, control de accesos, segmentación de red.
- Estándares ISO/IEC 20000-1 e ISO/IEC 27001 aplicados a infraestructura.
- Capacidad de análisis, respuesta ante incidentes y documentación técnica.

Formación Académica

Técnico, tecnólogo en ingeniería de sistemas, telecomunicaciones, electrónica, redes y seguridad informática, mantenimiento de equipos o afines. O en curso en telecomunicaciones, redes (Cisco, MikroTik), virtualización, administración de servidores y seguridad informática. Se valoran conocimientos y formación en gestión de servicios TI (ITIL) y normas ISO.



SOPORTE TÉCNICO – Auxiliar



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Nombre del cargo	Soporte Técnico
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
Grado	13
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de funciones	Resolucion1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Atención, diagnóstico, solución y seguimiento de incidentes relacionados con hardware, software, conectividad y equipos tecnológicos.

Propósito Principal

Brindar soporte técnico de primer y segundo nivel a los usuarios de la comunidad universitaria, asegurando la operatividad de los equipos, el software institucional y los recursos tecnológicos, con criterios de oportunidad, calidad y seguridad, contribuyendo a la continuidad y confiabilidad de los servicios de TI, en el marco del Sistema de Gestión de Servicios (ISO/IEC 20000-1:2018) y del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001:2022).

Funciones Esenciales

- Atender y resolver incidentes técnicos relacionados con hardware, software, impresoras, periféricos, redes locales y conectividad.
- Realizar diagnósticos y mantenimientos preventivos y correctivos a equipos de cómputo y dispositivos tecnológicos.
- Instalar, configurar y actualizar sistemas operativos, software institucional y antivirus.



- Gestionar y registrar solicitudes en el sistema de Mesa de Ayuda, asegurando su trazabilidad.
- Escalar casos de mayor complejidad al área correspondiente, realizando seguimiento hasta su cierre.
- Brindar soporte presencial o remoto, garantizando una atención oportuna y eficiente al usuario.
- Documentar procedimientos de soporte y generar reportes de atención e indicadores de servicio.
- Apoyar jornadas de despliegue tecnológico, renovación de equipos y configuración de nuevos ambientes.
- Cumplir con las políticas de seguridad de la información, protección de datos y uso adecuado de activos institucionales.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Brindar soporte técnico a usuarios en software y hardware.
- Realizar revisiones periódicas a equipos tecnológicos para prevenir fallas.
- Administrar y restringir accesos, garantizando que solo los usuarios autorizados puedan acceder.
- Realizar actualizaciones de seguridad en sistemas operativos.
- Promover buenas prácticas de seguridad como el uso de contraseñas seguras y la protección de datos sensibles.
- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Atender los mantenimientos llevado a cabo por proveedores externos, realizar las pruebas correspondientes de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Realizar diagnóstico y emitir conceptos técnicos relacionados con la infraestructura tecnológica.



- Realizar los mantenimientos preventivos y correctivos, hacer las pruebas de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Asegurar el cumplimiento de los estándares y procedimientos aplicables.
- Mantener el servicio en óptimas condiciones

Conocimientos Básicos

- Diagnóstico y reparación de hardware (equipos de cómputo, impresoras, proyectores, periféricos).
- Instalación y configuración de sistemas operativos (Windows, Linux).
- Software institucional, antivirus, herramientas ofimáticas y colaboración en la nube.
- Conectividad básica: redes LAN, Wi-Fi, configuración de puntos de red.
- Herramientas de soporte remoto (AnyDesk, TeamViewer, etc.).
- Uso de plataformas de mesa de ayuda (GLPI, OTRS, etc.).
- Fundamentos de seguridad de la información y protección de datos.
- Normas básicas ISO 20000-1 e ISO 27001 en entornos de soporte.
- Habilidades de atención al usuario, comunicación efectiva y resolución de problemas.

Formación Académica

Técnico o tecnólogo en soporte de sistemas, informática, redes, mantenimiento de computadores o afines. Se valora formación complementaria en atención al cliente, certificaciones básicas en soporte técnico, y conocimientos en estándares de gestión de servicios TI (ITIL) o seguridad informática.

SOPORTE TÉCNICO – Auxiliar



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Nombre del cargo	Soporte Técnico
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
Grado	16
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Atención, diagnóstico, solución y seguimiento de incidentes relacionados con hardware, software, conectividad y equipos tecnológicos.

Propósito Principal

Brindar soporte técnico de primer y segundo nivel a los usuarios de la comunidad universitaria, asegurando la operatividad de los equipos, el software institucional y los recursos tecnológicos, con criterios de oportunidad, calidad y seguridad, contribuyendo a la continuidad y confiabilidad de los servicios de TI, en el marco del Sistema de Gestión de Servicios (ISO/IEC 20000-1:2018) y del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001:2022).

Funciones Esenciales

- Atender y resolver incidentes técnicos relacionados con hardware, software, impresoras, periféricos, redes locales y conectividad.
- Realizar diagnósticos y mantenimientos preventivos y correctivos a equipos de cómputo y dispositivos tecnológicos.
- Instalar, configurar y actualizar sistemas operativos, software institucional y antivirus.
- Gestionar y registrar solicitudes en el sistema de Mesa de Ayuda, asegurando su trazabilidad.
- Escalar casos de mayor complejidad al área correspondiente, realizando seguimiento hasta su cierre.



- Brindar soporte presencial o remoto, garantizando una atención oportuna y eficiente al usuario.
- Documentar procedimientos de soporte y generar reportes de atención e indicadores de servicio.
- Apoyar jornadas de despliegue tecnológico, renovación de equipos y configuración de nuevos ambientes.
- Cumplir con las políticas de seguridad de la información, protección de datos y uso adecuado de activos institucionales.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Brindar soporte técnico a usuarios en software y hardware.
- Realizar revisiones periódicas a equipos tecnológicos para prevenir fallas.
- Administrar y restringir accesos, garantizando que solo los usuarios autorizados puedan acceder.
- Realizar actualizaciones de seguridad en sistemas operativos.
- Promover buenas prácticas de seguridad como el uso de contraseñas seguras y la protección de datos sensibles.
- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Atender los mantenimientos llevado a cabo por proveedores externos, realizar las pruebas correspondientes de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Realizar diagnóstico y emitir conceptos técnicos relacionados con la infraestructura tecnológica.



- Realizar los mantenimientos preventivos y correctivos, hacer las pruebas de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Asegurar el cumplimiento de los estándares y procedimientos aplicables.
- Mantener el servicio en óptimas condiciones

Conocimientos Básicos

- Diagnóstico y reparación de hardware (equipos de cómputo, impresoras, proyectores, periféricos).
- Instalación y configuración de sistemas operativos (Windows, Linux).
- Software institucional, antivirus, herramientas ofimáticas y colaboración en la nube.
- Conectividad básica: redes LAN, Wi-Fi, configuración de puntos de red.
- Herramientas de soporte remoto (AnyDesk, TeamViewer, etc.).
- Uso de plataformas de mesa de ayuda (GLPI, OTRS, etc.).
- Fundamentos de seguridad de la información y protección de datos.
- Normas básicas ISO 20000-1 e ISO 27001 en entornos de soporte.
- Habilidades de atención al usuario, comunicación efectiva y resolución de problemas.

Formación Académica

Técnico o tecnólogo en soporte de sistemas, informática, redes, mantenimiento de computadores o afines. Se valora formación complementaria en atención al cliente, certificaciones básicas en soporte técnico, y conocimientos en estándares de gestión de servicios TI (ITIL) o seguridad informática.

SOPORTE TÉCNICO - Auxiliar



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Nombre del cargo	Soporte Técnico
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
Grado	8
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Atención, diagnóstico, solución y seguimiento de incidentes relacionados con hardware, software, conectividad y equipos tecnológicos.

Propósito Principal

Brindar soporte técnico de primer y segundo nivel a los usuarios de la comunidad universitaria, asegurando la operatividad de los equipos, el software institucional y los recursos tecnológicos, con criterios de oportunidad, calidad y seguridad, contribuyendo a la continuidad y confiabilidad de los servicios de TI, en el marco del Sistema de Gestión de Servicios (ISO/IEC 20000-1:2018) y del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001:2022).

Funciones Esenciales

- Atender y resolver incidentes técnicos relacionados con hardware, software, impresoras, periféricos, redes locales y conectividad.
- Realizar diagnósticos y mantenimientos preventivos y correctivos a equipos de cómputo y dispositivos tecnológicos.
- Instalar, configurar y actualizar sistemas operativos, software institucional y antivirus.
- Gestionar y registrar solicitudes en el sistema de Mesa de Ayuda, asegurando su trazabilidad.
- Escalar casos de mayor complejidad al área correspondiente, realizando seguimiento hasta su cierre.
- Brindar soporte presencial o remoto, garantizando una atención oportuna y eficiente al usuario.



- Documentar procedimientos de soporte y generar reportes de atención e indicadores de servicio.
- Apoyar jornadas de despliegue tecnológico, renovación de equipos y configuración de nuevos ambientes.
- Cumplir con las políticas de seguridad de la información, protección de datos y uso adecuado de activos institucionales.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Brindar soporte técnico a usuarios en software y hardware.
- Realizar revisiones periódicas a equipos tecnológicos para prevenir fallas.
- Administrar y restringir accesos, garantizando que solo los usuarios autorizados puedan acceder.
- Realizar actualizaciones de seguridad en sistemas operativos.
- Promover buenas prácticas de seguridad como el uso de contraseñas seguras y la protección de datos sensibles.
- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Atender los mantenimientos llevado a cabo por proveedores externos, realizar las pruebas correspondientes de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Realizar diagnóstico y emitir conceptos técnicos relacionados con la infraestructura tecnológica.
- Realizar los mantenimientos preventivos y correctivos, hacer las pruebas de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.



- Asegurar el cumplimiento de los estándares y procedimientos aplicables.
- Mantener el servicio en óptimas condiciones

Conocimientos Básicos

- Diagnóstico y reparación de hardware (equipos de cómputo, impresoras, proyectores, periféricos).
- Instalación y configuración de sistemas operativos (Windows, Linux).
- Software institucional, antivirus, herramientas ofimáticas y colaboración en la nube.
- Conectividad básica: redes LAN, Wi-Fi, configuración de puntos de red.
- Herramientas de soporte remoto (AnyDesk, TeamViewer, etc.).
- Uso de plataformas de mesa de ayuda (GLPI, OTRS, etc.).
- Fundamentos de seguridad de la información y protección de datos.
- Normas básicas ISO 20000-1 e ISO 27001 en entornos de soporte.
- Habilidades de atención al usuario, comunicación efectiva y resolución de problemas.

Formación Académica

Técnico o tecnólogo en soporte de sistemas, informática, redes, mantenimiento de computadores o afines. Se valora formación complementaria en atención al cliente, certificaciones básicas en soporte técnico, y conocimientos en estándares de gestión de servicios TI (ITIL) o seguridad informática.

SOPORTE TÉCNICO – Técnico



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Nombre del cargo	Soporte Técnico
Nivel	Técnico
Categoría	Carrera administrativa
Código	3132
Grado	13
Nombre del cargo	Técnico operativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	2
Cargo del Manual de funciones	Resolucion1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Atención, diagnóstico, solución y seguimiento de incidentes relacionados con hardware, software, conectividad y equipos tecnológicos.

Propósito Principal

Brindar soporte técnico de primer y segundo nivel a los usuarios de la comunidad universitaria, asegurando la operatividad de los equipos, el software institucional y los recursos tecnológicos, con criterios de oportunidad, calidad y seguridad, contribuyendo a la continuidad y confiabilidad de los servicios de TI, en el marco del Sistema de Gestión de Servicios (ISO/IEC 20000-1:2018) y del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001:2022).

Funciones Esenciales

- Atender y resolver incidentes técnicos relacionados con hardware, software, impresoras, periféricos, redes locales y conectividad.
- Realizar diagnósticos y mantenimientos preventivos y correctivos a equipos de cómputo y dispositivos tecnológicos.
- Instalar, configurar y actualizar sistemas operativos, software institucional y antivirus.
- Gestionar y registrar solicitudes en el sistema de Mesa de Ayuda, asegurando su trazabilidad.
- Escalar casos de mayor complejidad al área correspondiente, realizando seguimiento hasta su cierre.
- Brindar soporte presencial o remoto, garantizando una atención oportuna y eficiente al usuario.
- Documentar procedimientos de soporte y generar reportes de atención e indicadores de servicio.



- Apoyar jornadas de despliegue tecnológico, renovación de equipos y configuración de nuevos ambientes.
- Cumplir con las políticas de seguridad de la información, protección de datos y uso adecuado de activos institucionales.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Brindar soporte técnico a usuarios en software y hardware.
- Realizar revisiones periódicas a equipos tecnológicos para prevenir fallas.
- Administrar y restringir accesos, garantizando que solo los usuarios autorizados puedan acceder.
- Realizar actualizaciones de seguridad en sistemas operativos.
- Promover buenas prácticas de seguridad como el uso de contraseñas seguras y la protección de datos sensibles.
- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Atender los mantenimientos llevado a cabo por proveedores externos, realizar las pruebas correspondientes de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Realizar diagnóstico y emitir conceptos técnicos relacionados con la infraestructura tecnológica.
- Realizar los mantenimientos preventivos y correctivos, hacer las pruebas de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Asegurar el cumplimiento de los estándares y procedimientos aplicables.



- Mantener el servicio en óptimas condiciones

Conocimientos Básicos

- Diagnóstico y reparación de hardware (equipos de cómputo, impresoras, proyectores, periféricos).
- Instalación y configuración de sistemas operativos (Windows, Linux).
- Software institucional, antivirus, herramientas ofimáticas y colaboración en la nube.
- Conectividad básica: redes LAN, Wi-Fi, configuración de puntos de red.
- Herramientas de soporte remoto (AnyDesk, TeamViewer, etc.).
- Uso de plataformas de mesa de ayuda (GLPI, OTRS, etc.).
- Fundamentos de seguridad de la información y protección de datos.
- Normas básicas ISO 20000-1 e ISO 27001 en entornos de soporte.
- Habilidades de atención al usuario, comunicación efectiva y resolución de problemas.

Formación Académica

Técnico o tecnólogo en soporte de sistemas, informática, redes, mantenimiento de computadores o afines. Se valora formación complementaria en atención al cliente, certificaciones básicas en soporte técnico, y conocimientos en estándares de gestión de servicios TI (ITIL) o seguridad informática.

SOPORTE TÉCNICO – Técnico



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Nombre del cargo	Soporte Técnico
Nivel	Técnico
Categoría	Carrera administrativa
Código	3124
Grado	12
Nombre del cargo	Técnico administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Atención, diagnóstico, solución y seguimiento de incidentes relacionados con hardware, software, conectividad y equipos tecnológicos.

Propósito Principal

Brindar soporte técnico de primer y segundo nivel a los usuarios de la comunidad universitaria, asegurando la operatividad de los equipos, el software institucional y los recursos tecnológicos, con criterios de oportunidad, calidad y seguridad, contribuyendo a la continuidad y confiabilidad de los servicios de TI, en el marco del Sistema de Gestión de Servicios (ISO/IEC 20000-1:2018) y del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001:2022).

Funciones Esenciales

- Atender y resolver incidentes técnicos relacionados con hardware, software, impresoras, periféricos, redes locales y conectividad.
- Realizar diagnósticos y mantenimientos preventivos y correctivos a equipos de cómputo y dispositivos tecnológicos.
- Instalar, configurar y actualizar sistemas operativos, software institucional y antivirus.



- Gestionar y registrar solicitudes en el sistema de Mesa de Ayuda, asegurando su trazabilidad.
- Escalar casos de mayor complejidad al área correspondiente, realizando seguimiento hasta su cierre.
- Brindar soporte presencial o remoto, garantizando una atención oportuna y eficiente al usuario.
- Documentar procedimientos de soporte y generar reportes de atención e indicadores de servicio.
- Apoyar jornadas de despliegue tecnológico, renovación de equipos y configuración de nuevos ambientes.
- Cumplir con las políticas de seguridad de la información, protección de datos y uso adecuado de activos institucionales.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Brindar soporte técnico a usuarios en software y hardware.
- Realizar revisiones periódicas a equipos tecnológicos para prevenir fallas.
- Administrar y restringir accesos, garantizando que solo los usuarios autorizados puedan acceder.
- Realizar actualizaciones de seguridad en sistemas operativos.
- Promover buenas prácticas de seguridad como el uso de contraseñas seguras y la protección de datos sensibles.
- Verificar los requerimientos asignados y atender las solicitudes dentro de los tiempos establecidos.
- Realizar seguimiento de las peticiones o incidencias asignadas.
- Atender los mantenimientos llevado a cabo por proveedores externos, realizar las pruebas correspondientes de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.



- Realizar diagnóstico y emitir conceptos técnicos relacionados con la infraestructura tecnológica.
- Realizar los mantenimientos preventivos y correctivos, hacer las pruebas de funcionalidad y presentar los informes en los que se evidencien dichas pruebas.
- Asegurar el cumplimiento de los estándares y procedimientos aplicables.
- Mantener el servicio en óptimas condiciones

Conocimientos Básicos

- Diagnóstico y reparación de hardware (equipos de cómputo, impresoras, proyectores, periféricos).
- Instalación y configuración de sistemas operativos (Windows, Linux).
- Software institucional, antivirus, herramientas ofimáticas y colaboración en la nube.
- Conectividad básica: redes LAN, Wi-Fi, configuración de puntos de red.
- Herramientas de soporte remoto (AnyDesk, TeamViewer, etc.).
- Uso de plataformas de mesa de ayuda (GLPI, OTRS, etc.).
- Fundamentos de seguridad de la información y protección de datos.
- Normas básicas ISO 20000-1 e ISO 27001 en entornos de soporte.
- Habilidades de atención al usuario, comunicación efectiva y resolución de problemas.

Formación Académica

Técnico o tecnólogo en soporte de sistemas, informática, redes, mantenimiento de computadores o afines. Se valora formación complementaria en atención al cliente, certificaciones básicas en soporte técnico, y conocimientos en estándares de gestión de servicios TI (ITIL) o seguridad informática.

ADMINISTRADOR AULAS DE INFORMATICA - Profesional



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Administrador de aulas de informática
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	7
Nombre del cargo	Profesional universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo de Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión operativa, mantenimiento, soporte técnico y aseguramiento de la disponibilidad de las aulas de informática institucionales, garantizando su correcto funcionamiento para el apoyo a los procesos académicos y administrativos.

Propósito Principal

Administrar los recursos tecnológicos de las aulas de informática, asegurando la disponibilidad, funcionalidad y actualización de los equipos, software y periféricos, con el fin de brindar un entorno adecuado para el desarrollo de actividades académicas y de formación, conforme con los lineamientos del Sistema de Gestión de Servicios (SGS) y el Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Instalar, configurar y mantener operativos los equipos de cómputo, software y periféricos en las aulas de informática.
- Realizar mantenimiento preventivo y correctivo de hardware y software para asegurar la continuidad del servicio.
- Gestionar el acceso de usuarios a los equipos y recursos tecnológicos, aplicando controles de seguridad y uso responsable.



- Apoyar actividades académicas que requieran el uso de tecnología, incluyendo clases, evaluaciones y capacitaciones.
- Documentar procedimientos técnicos, manuales de uso, bitácoras de fallos y soluciones aplicadas.
- Coordinar con las áreas de infraestructura y soporte para resolver incidencias críticas.
- Participar en los procesos de actualización tecnológica de las aulas, incluyendo renovación de equipos y licenciamiento de software.
- Verificar el cumplimiento de las normas institucionales de uso de tecnologías y políticas de seguridad de la información.
- Realizar monitoreo y evaluación del estado de uso y funcionamiento de las aulas, proponiendo mejoras cuando sea necesario.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Verificar disponibilidad de aulas de informática según normativas establecidas y necesidades académicas.
- Asignar y habilitar el acceso a las aulas según normativas establecidas y necesidades académicas.
- Coordinar la distribución de horarios asegurando un uso eficiente de los espacios.
- Administra la disponibilidad de las aulas con el material de apoyo como equipos multimedia.
- Verificar el software instalado dentro del aula.
- Gestionar los recursos necesarios para la operación de las aulas.
- Supervisar al equipo técnico de soporte en aulas.

- Monitorear el cumplimiento de los acuerdos de nivel de servicio (ANS).

Conocimientos Básicos

- Sistemas operativos Windows y Linux.
- Mantenimiento de hardware y periféricos (impresoras, proyectores, etc.).
- Instalación y gestión de software educativo e institucional.
- Conectividad básica y redes locales.
- Control de acceso, usuarios, y políticas de uso seguro de equipos.
- Principios de seguridad informática y protección de datos personales.
- Fundamentos de ISO/IEC 20000-1 e ISO/IEC 27001 aplicados a entornos educativos.
- Habilidades de atención al usuario, trabajo en equipo y solución de problemas técnicos.

Formación Académica

Profesional en ingeniería de sistemas, administración de empresas, Ingeniería de Software, Ingeniería en Telecomunicaciones, Ingeniería Electrónica, Licenciatura en Tecnología, Licenciatura en Informática Educativa, Administración de Sistemas Informáticos o carreras afines en el área TIC con conocimientos o formación complementaria en gestión de aulas TIC, mantenimiento de equipos, o seguridad informática. Deseable formación en atención al usuario o soporte de servicios TI (ITIL, fundamentos ISO).

GESTOR OPERATIVO DE AULAS DE INFORMATICA – Secretaria



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor operativo de aulas de informática
Nivel	Secretaria
Categoría	Carrera administrativa
Código	4178
Grado	13
Nombre del cargo	Secretaria
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Administración, mantenimiento y soporte de las aulas de informática de la Universidad, garantizando su disponibilidad, funcionalidad y seguridad.

Propósito Principal

Gestionar y asegurar la operatividad de las aulas de informática de la Universidad, mediante el mantenimiento, configuración y soporte de los equipos, software y redes locales, contribuyendo al acceso eficiente y seguro de los recursos tecnológicos por parte de estudiantes y docentes, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Instalar, configurar y mantener operativos los equipos de cómputo y periféricos de las aulas de informática.
- Realizar mantenimientos preventivos y correctivos, asegurando la disponibilidad de los recursos tecnológicos.
- Gestionar el acceso de usuarios, perfiles, contraseñas y restricciones según normativas institucionales.
- Instalar y actualizar software educativo, sistemas operativos, antivirus y herramientas especializadas.



- Apoyar el desarrollo de clases, prácticas académicas y evaluaciones, garantizando el correcto funcionamiento de los equipos.
- Monitorear el estado de red, conectividad, impresión y disponibilidad de insumos en las aulas.
- Reportar incidentes al sistema de Mesa de Ayuda y hacer seguimiento hasta su resolución.
- Documentar procedimientos técnicos, manuales de uso y bitácoras de mantenimiento.
- Aplicar buenas prácticas en seguridad informática, protección de datos y uso responsable de los equipos.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
- Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Controlan el acceso a las aulas para que los docentes puedan ingresar en el momento adecuado.
- Verificar que tanto los docentes como los estudiantes hagan correcto uso de las salas de informática.
- Reportar incidentes o irregularidades en el uso de las salas.
- Realizar verificaciones de las condiciones de los equipos de multimedia.
- Reportar fallas en los equipos de cómputo.
- Conocer e implementar las políticas de seguridad en sus actividades diarias.
- Instalar, configurar y actualizar software y hardware en las aulas.
- Atender incidentes y solicitudes de soporte en el menor tiempo posible.
- Aplicar protocolos de mantenimiento preventivo y correctivo.



- Documentar fallas y soluciones implementadas.

Conocimientos Básicos

- Sistemas operativos Windows y Linux (instalación, configuración y administración).
- Equipos de cómputo, impresoras, proyectores y periféricos.
- Software académico, utilitarios y herramientas de gestión educativa.
- Conectividad básica: redes locales, puntos de red, configuraciones de acceso.
- Herramientas de soporte técnico y control remoto.
- Procedimientos de mantenimiento preventivo y correctivo.
- Fundamentos de seguridad informática y protección de datos personales.
- Conocimiento básico de las normas ISO/IEC 20000-1:2018 e ISO/IEC 27001:2022.
- Habilidades de servicio al usuario, comunicación efectiva y trabajo en equipo.

Formación Académica

Técnico o tecnólogo en sistemas, informática, soporte de TI, redes o áreas afines. Se valora experiencia en administración de aulas informáticas o laboratorios tecnológicos. Deseable formación complementaria en seguridad informática, mantenimiento de equipos, o gestión de servicios TI (ITIL).



GESTOR OPERATIVO DE AULAS DE INFORMATICA - Auxiliar



**Dirección de las Tecnologías y Sistemas de la
Información y de las Comunicaciones**

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor operativo de aulas de informática
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
Grado	13
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Administración, mantenimiento y soporte de las aulas de informática de la Universidad, garantizando su disponibilidad, funcionalidad y seguridad.

Propósito Principal

Gestionar y asegurar la operatividad de las aulas de informática de la Universidad, mediante el mantenimiento, configuración y soporte de los equipos, software y redes locales, contribuyendo al acceso eficiente y seguro de los recursos tecnológicos por parte de estudiantes y docentes, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Instalar, configurar y mantener operativos los equipos de cómputo y periféricos de las aulas de informática.
- Realizar mantenimientos preventivos y correctivos, asegurando la disponibilidad de los recursos tecnológicos.
- Gestionar el acceso de usuarios, perfiles, contraseñas y restricciones según normativas institucionales.
- Instalar y actualizar software educativo, sistemas operativos, antivirus y herramientas especializadas.
- Apoyar el desarrollo de clases, prácticas académicas y evaluaciones, garantizando el correcto funcionamiento de los equipos.



- Monitorear el estado de red, conectividad, impresión y disponibilidad de insumos en las aulas.
- Reportar incidentes al sistema de Mesa de Ayuda y hacer seguimiento hasta su resolución.
- Documentar procedimientos técnicos, manuales de uso y bitácoras de mantenimiento.
- Aplicar buenas prácticas en seguridad informática, protección de datos y uso responsable de los equipos.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
- Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Controlan el acceso a las aulas para que los docentes puedan ingresar en el momento adecuado.
- Verificar que tanto los docentes como los estudiantes hagan correcto uso de las salas de informática.
- Reportar incidentes o irregularidades en el uso de las salas.
- Realizar verificaciones de las condiciones de los equipos de multimedia.
- Reportar fallas en los equipos de cómputo.
- Conocer e implementar las políticas de seguridad en sus actividades diarias.
- Instalar, configurar y actualizar software y hardware en las aulas.
- Atender incidentes y solicitudes de soporte en el menor tiempo posible.
- Aplicar protocolos de mantenimiento preventivo y correctivo.
- Documentar fallas y soluciones implementadas.

Conocimientos Básicos

- Sistemas operativos Windows y Linux (instalación, configuración y administración).
- Equipos de cómputo, impresoras, proyectores y periféricos.
- Software académico, utilitarios y herramientas de gestión educativa.
- Conectividad básica: redes locales, puntos de red, configuraciones de acceso.
- Herramientas de soporte técnico y control remoto.
- Procedimientos de mantenimiento preventivo y correctivo.
- Fundamentos de seguridad informática y protección de datos personales.
- Conocimiento básico de las normas ISO/IEC 20000-1:2018 e ISO/IEC 27001:2022.
- Habilidades de servicio al usuario, comunicación efectiva y trabajo en equipo.

Formación Académica

Técnico o tecnólogo en sistemas, informática, soporte de TI, redes o áreas afines. Se valora experiencia en administración de aulas informáticas o laboratorios tecnológicos. Deseable formación complementaria en seguridad informática, mantenimiento de equipos, o gestión de servicios TI (ITIL).



GESTOR OPERATIVO DE AULAS DE INFORMATICA - Auxiliar



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor operativo de aulas de informática
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
Grado	08
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	2
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Administración, mantenimiento y soporte de las aulas de informática de la Universidad, garantizando su disponibilidad, funcionalidad y seguridad.

Propósito Principal

Gestionar y asegurar la operatividad de las aulas de informática de la Universidad, mediante el mantenimiento, configuración y soporte de los equipos, software y redes locales, contribuyendo al acceso eficiente y seguro de los recursos tecnológicos por parte de estudiantes y docentes, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (SGS) y del Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Instalar, configurar y mantener operativos los equipos de cómputo y periféricos de las aulas de informática.
- Realizar mantenimientos preventivos y correctivos, asegurando la disponibilidad de los recursos tecnológicos.
- Gestionar el acceso de usuarios, perfiles, contraseñas y restricciones según normativas institucionales.
- Instalar y actualizar software educativo, sistemas operativos, antivirus y herramientas especializadas.
- Apoyar el desarrollo de clases, prácticas académicas y evaluaciones, garantizando el correcto funcionamiento de los equipos.



- Monitorear el estado de red, conectividad, impresión y disponibilidad de insumos en las aulas.
- Reportar incidentes al sistema de Mesa de Ayuda y hacer seguimiento hasta su resolución.
- Documentar procedimientos técnicos, manuales de uso y bitácoras de mantenimiento.
- Aplicar buenas prácticas en seguridad informática, protección de datos y uso responsable de los equipos.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
- Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Controlan el acceso a las aulas para que los docentes puedan ingresar en el momento adecuado.
- Verificar que tanto los docentes como los estudiantes hagan correcto uso de las salas de informática.
- Reportar incidentes o irregularidades en el uso de las salas.
- Realizar verificaciones de las condiciones de los equipos de multimedia.
- Reportar fallas en los equipos de cómputo.
- Conocer e implementar las políticas de seguridad en sus actividades diarias.
- Instalar, configurar y actualizar software y hardware en las aulas.
- Atender incidentes y solicitudes de soporte en el menor tiempo posible.
- Aplicar protocolos de mantenimiento preventivo y correctivo.
- Documentar fallas y soluciones implementadas.

Conocimientos Básicos

- Sistemas operativos Windows y Linux (instalación, configuración y administración).
- Equipos de cómputo, impresoras, proyectores y periféricos.
- Software académico, utilitarios y herramientas de gestión educativa.
- Conectividad básica: redes locales, puntos de red, configuraciones de acceso.
- Herramientas de soporte técnico y control remoto.
- Procedimientos de mantenimiento preventivo y correctivo.
- Fundamentos de seguridad informática y protección de datos personales.
- Conocimiento básico de las normas ISO/IEC 20000-1:2018 e ISO/IEC 27001:2022.
- Habilidades de servicio al usuario, comunicación efectiva y trabajo en equipo.

Formación Académica

Técnico o tecnólogo en sistemas, informática, soporte de TI, redes o áreas afines. Se valora experiencia en administración de aulas informáticas o laboratorios tecnológicos. Deseable formación complementaria en seguridad informática, mantenimiento de equipos, o gestión de servicios TI (ITIL).

ADMINISTRADOR DE SOFTWARE – Técnico



Dirección de Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Administrador de Software
Nivel	Técnico
Categoría	Carrera administrativa
Código	3132
Grado	13
Nombre del cargo	Técnico operativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión, administración y soporte del software institucional, garantizando su disponibilidad, cumplimiento normativo, actualización y alineación con las necesidades misionales y de gestión de la Universidad.

Propósito Principal

Asegurar el correcto funcionamiento, disponibilidad y actualización del software utilizado en la Universidad, incluyendo aplicaciones institucionales, licenciamiento, instalación y soporte, garantizando su adecuada gestión bajo criterios de calidad, seguridad de la información y continuidad del servicio, en cumplimiento con los lineamientos del Sistema de Gestión de Servicios (SGS) y el Sistema de Gestión de Seguridad de la Información (SGSI).

Funciones Esenciales

- Administrar y mantener actualizadas las aplicaciones y sistemas de software institucional, tanto en equipos individuales como en servidores.
- Coordinar la instalación, configuración y actualización de software bajo parámetros técnicos y de seguridad definidos por la DTIC.
- Gestionar y hacer seguimiento al licenciamiento de software institucional, asegurando el cumplimiento legal y técnico.



- Brindar soporte técnico relacionado con el uso, fallas o conflictos de software a usuarios internos.
- Documentar procedimientos, configuraciones y manuales de uso del software administrado.
- Participar en procesos de evaluación, adquisición y prueba de nuevas herramientas o soluciones tecnológicas.
- Aplicar buenas prácticas de seguridad en la administración del software, evitando vulnerabilidades.
- Apoyar auditorías internas y externas en temas relacionados con licenciamiento, gestión de activos y seguridad del software.
- Monitorear el desempeño y uso de las herramientas digitales instaladas para identificar oportunidades de mejora.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
- Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Gestionar y supervisar el uso del software institucional, garantizando su correcta implementación.
- Asegurar que todo el software cumpla con normativas de seguridad de la información (ISO 27001, Ley 1581 de 2012, etc.).
- Supervisar la adquisición y renovación de licencias de software, evitando el uso indebido de herramientas tecnológicas.
- Implementar controles para evitar el uso de software no autorizado o sin licencia.
- Garantizar que las actualizaciones de software se realicen de manera controlada y segura.
- Aprobar o restringir el acceso a software según políticas de seguridad y necesidades de los usuarios.
- Realizar inventarios periódicos del software instalado y en uso.



Conocimientos Básicos

- Instalación y configuración de software en plataformas Windows y Linux.
- Gestión de licencias y activos de software.
- Herramientas de distribución remota de software (ej. WSUS, SCCM, Ansible, etc.).
- Gestión de incidencias mediante plataformas como GLPI, OTRS o similares.
- Principios de seguridad en software: actualizaciones, parches, control de versiones.
- Fundamentos de ISO/IEC 20000-1 e ISO/IEC 27001 aplicados a la gestión de software.
- Buenas prácticas en documentación técnica y atención al usuario.

Formación Académica

Técnico, tecnólogo en Ingeniería de Sistemas, Ingeniería de Software, Informática, Soporte de Tecnologías de la Información, Programación de Software, Administración de Sistemas, Desarrollo de Aplicaciones, Informática o carreras técnicas afines al área TIC. Se valoran certificaciones o formación complementaria en administración de software, licenciamiento, ITIL, seguridad de la información o gestión de servicios TI.



LIDER EN EVALUACIÓN Y CONCEPTUALIZACIÓN TÉCNICA – Profesional



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Líder en evaluación y conceptualización técnica
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	05
Nombre del cargo	Profesional universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del manual de funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Evaluación, análisis, formulación y estructuración técnica de requerimientos tecnológicos, asegurando la viabilidad técnica, normativa y operativa de los proyectos y servicios de TI institucionales.

Propósito Principal

Diseñar y validar conceptos técnicos que respalden la adquisición, implementación y evolución de soluciones tecnológicas, asegurando su alineación con los objetivos institucionales, la normatividad vigente y las buenas prácticas definidas en los sistemas de gestión de servicios (SGS) y seguridad de la información (SGSI).

Funciones Esenciales

- Evaluar requerimientos tecnológicos de proyectos institucionales, validando su viabilidad técnica y operativa.
- Elaborar conceptos técnicos para procesos de contratación, adquisiciones y desarrollos tecnológicos.
- Realizar análisis comparativos de tecnologías, soluciones y arquitecturas, con base en estándares y criterios objetivos.
- Participar en el diseño de arquitecturas de software, hardware e infraestructura que soporten servicios institucionales.
- Apoyar la toma de decisiones tecnológicas a través de informes técnicos, recomendaciones y modelos de evaluación.



- Asegurar que los requerimientos técnicos cumplan con los criterios de calidad, seguridad, escalabilidad y continuidad.
- Coordinar con equipos de desarrollo, infraestructura y seguridad para validar la factibilidad técnica de proyectos.
- Contribuir a la actualización de lineamientos técnicos, políticas y estándares institucionales en TIC.
- Participar en auditorías técnicas, procesos de evaluación y revisión de propuestas tecnológicas externas.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Emitir conceptos técnicos para la compra de Software y hardware asegurando su compatibilidad con la infraestructura tecnológica.
- Garantizar el cumplimiento de normativas de seguridad de la Información.
- Verificar las especificaciones técnicas del equipo o sistema donde se realizará la instalación de software o hardware, asegurando su compatibilidad y correcto funcionamiento.
- Emitir un concepto técnico fundamentado para la baja de software o hardware, evaluando su estado, utilidad y cumplimiento de normativas vigentes.



- Asegurar que el concepto cumpla con los estándares de seguridad y normativas vigentes.

Conocimientos Básicos

- Principios de arquitectura tecnológica (infraestructura, software, redes, nube).
- Evaluación de propuestas técnicas y análisis de viabilidad.
- Redacción de conceptos técnicos y términos de referencia.
- Normativas relacionadas con contratación pública y compras TIC.
- Conocimientos en estándares ISO/IEC 20000-1 e ISO/IEC 27001.
- Habilidades de análisis, redacción técnica y pensamiento crítico.

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería en Telecomunicaciones, Ingeniería Informática, o áreas afines en tecnologías de la información y las comunicaciones (TIC), o carreras afines. Deseable formación o certificación en evaluación de proyectos TIC, arquitectura empresarial, gestión de servicios o seguridad de la información.

GESTOR GOBIERNO DIGITAL – Profesional



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones
 ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Gestor de Gobierno Digital
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	5
Nombre del cargo	Profesional universitaria
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Planeación, seguimiento y articulación de las estrategias de Gobierno Digital en la Universidad, en cumplimiento de las directrices del Ministerio TIC y las normas de gestión de servicios y seguridad de la información.

Propósito Principal

Diseñar, coordinar y hacer seguimiento a la implementación de la estrategia de Gobierno Digital en la Universidad, fomentando la transformación digital institucional, la eficiencia administrativa, la transparencia, la participación ciudadana, la interoperabilidad y el aprovechamiento de las TIC como herramientas para la gestión pública y la mejora del servicio a la comunidad universitaria.

Funciones Esenciales

- Liderar la formulación e implementación del Plan de Gobierno Digital institucional.
- Coordinar el cumplimiento de las políticas, lineamientos y marcos de referencia establecidos por el MinTIC.
- Articular acciones con dependencias internas para el desarrollo de proyectos en los ejes de servicios digitales, TIC para la gestión, seguridad digital, arquitectura empresarial, y datos abiertos.
- Realizar seguimiento y reporte a herramientas como el **FURAG**, Tablero de Gobierno Digital, y otros instrumentos de evaluación.



- Identificar oportunidades de mejora e innovación digital en procesos institucionales.
- Promover la sensibilización, formación y cultura de transformación digital entre los funcionarios y usuarios.
- Garantizar la alineación del Gobierno Digital con el SGS (ISO 20000-1) y el SGSI (ISO 27001).
- Coordinar la recolección de evidencias, indicadores y resultados relacionados con la implementación del marco de Gobierno Digital.
- Representar institucionalmente a la DTIC en espacios interinstitucionales relacionados con transformación digital.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Coordinar la implementación de la **Política de Gobierno Digital** en la entidad.
- Liderar la formulación y actualización del **Plan de Acción de Gobierno Digital**, alineado al Plan Estratégico Institucional.
- Velar por el cumplimiento de los componentes y habilitadores del Modelo de Gobierno Digital: TIC para la gestión, TIC para la sociedad, seguridad y privacidad de la información, gestión de datos, servicios ciudadanos digitales, etc.
- Promover el desarrollo y mejora de servicios digitales, asegurando su accesibilidad, disponibilidad y usabilidad.
- Coordinar la implementación de políticas y prácticas de **Seguridad y Privacidad de la Información**, en articulación con el Oficial de Seguridad de la Información y el Oficial de Protección de Datos Personales.
- Promover la cultura de innovación pública y uso ético de las TIC.
- Organizar jornadas de capacitación y sensibilización en temas de Gobierno Digital.



- Realizar seguimiento periódico a los indicadores y metas del Plan de Gobierno Digital.
- Implementar acciones de mejora continua basadas en auditorías, evaluaciones y retroalimentación ciudadana.

Conocimientos Básicos

- Política de Gobierno Digital (MinTIC) y marcos de referencia internacionales en transformación digital.
- Normas ISO/IEC 20000-1:2018 y ISO/IEC 27001:2022.
- Herramientas de gestión estratégica y evaluación institucional (FURAG, MECI, MIPG).
- Principios de interoperabilidad, datos abiertos, seguridad digital y servicios ciudadanos digitales.
- Planeación y formulación de proyectos TIC.
- Comunicación efectiva, trabajo interinstitucional y liderazgo estratégico.

Formación Académica

Profesional en Ingeniería de Sistemas, Administración Pública, Ciencia de Datos, Gestión TIC, o afines. Deseable especialización o maestría en Gobierno Digital, Gestión Pública, Transformación Digital o Arquitectura Empresarial. Se valoran certificaciones o formación en marcos como ITIL, TOGAF, COBIT o Seguridad de la Información.



OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – Profesional



**Dirección de las Tecnologías y Sistemas de la
 Información y de las Comunicaciones**

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Oficial de Seguridad de la Información
Nivel	Profesional
Categoría	Carrera administrativa
Código	2044
Grado	5
Nombre del cargo	Profesional universitario
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 del 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión de la seguridad de la información institucional, implementación del Sistema de Gestión de Seguridad de la Información (SGSI), tratamiento de riesgos y aseguramiento de la confidencialidad, integridad y disponibilidad de los activos informacionales.

Propósito Principal

Diseñar, coordinar e implementar estrategias y controles para proteger los activos de información de la Universidad, garantizando el cumplimiento de la norma **ISO/IEC 27001:2022**, así como las políticas internas de seguridad digital, gestión de riesgos y continuidad del servicio. Velar por el desarrollo, mejora continua y sostenibilidad del SGSI institucional.

Funciones Esenciales

- Liderar el diseño, implementación y mantenimiento del **Sistema de Gestión de Seguridad de la Información (SGSI)** de acuerdo con ISO/IEC 27001.
- Identificar, analizar y gestionar riesgos relacionados con la seguridad de la información.
- Elaborar, actualizar y divulgar políticas, procedimientos y controles de seguridad.



- Coordinar auditorías internas y externas en materia de seguridad de la información.
- Atender y dar respuesta a incidentes de seguridad, investigando causas y mitigando impactos.
- Promover la concienciación y formación del personal en temas de ciberseguridad y buenas prácticas.
- Asegurar el cumplimiento normativo en materia de protección de datos personales, privacidad y uso de activos tecnológicos.
- Supervisar la gestión de accesos, respaldos, control de cambios, y otros aspectos técnicos y administrativos de la seguridad.
- Participar en la planeación de continuidad del negocio y recuperación ante desastres.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
- Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Liderar la implementación, mantenimiento y mejora del **Sistema de Gestión de Seguridad de la Información (SGSI)** según ISO/IEC 27001.
- Asegurar que las políticas, procedimientos y controles de seguridad y privacidad estén alineados con los objetivos institucionales, el análisis de riesgos y la legislación vigente.
- Dirigir la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información.
- Mantener actualizados **la matriz de riesgos de seguridad y privacidad** y el plan de tratamiento de riesgos.
- Garantizar que la entidad cumpla con:
 - Ley 1581 de 2012 y Decreto 1377 de 2013 (Protección de datos personales).
 - Ley 1266 de 2008 (Habeas Data financiero, si aplica).
 - Normatividad sectorial y políticas del MintIC.
- Gestionar el **Registro Nacional de Bases de Datos (RNBD)** ante la SIC.

- Supervisar la aplicación de controles técnicos y organizativos para proteger la confidencialidad, integridad y disponibilidad de la información.
- Validar que los proveedores cumplan con los requisitos de seguridad de la información.
- Coordinar la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.
- Participar en la planificación y pruebas de continuidad y recuperación ante desastres, garantizando que incluyan aspectos de seguridad y privacidad.
- Desarrollar e implementar programas de capacitación y concienciación en seguridad y privacidad para todos los funcionarios.
- Promover la cultura de ciberseguridad y protección de datos dentro de la entidad.
- Medir la eficacia de los controles de seguridad y privacidad.
- Proponer acciones correctivas y preventivas derivadas de incidentes, hallazgos o cambios normativos.

Conocimientos Básicos

- Norma ISO/IEC 27001:2022 y controles de la ISO/IEC 27002.
- Evaluación de riesgos de seguridad de la información.
- Gestión de incidentes y planes de respuesta.
- Protección de datos personales (Ley 1581 de 2012 - Colombia).
- Técnicas de ciberseguridad, control de accesos, cifrado, auditoría de sistemas.
- Herramientas de monitoreo, respaldo, control de cambios y gestión de vulnerabilidades.
- Normas ISO/IEC 20000-1, NIST, ITIL y buenas prácticas en gestión de servicios TI.
- Redacción de políticas, análisis de cumplimiento y comunicación institucional.

Formación Académica

Profesional en Ingeniería de Sistemas, Ingeniería de Seguridad Informática, Telecomunicaciones, o afines. Con conocimientos en Automatización y certificación en auditoría de Seguridad de la Información, Auditoría de Sistemas, Gobierno de TI o Gestión del Riesgo. Se valoran certificaciones como **ISO 27001** o similares.



OFICIAL DE PROTECCIÓN DE DATOS PERSONALES – Profesional Especializado



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Oficial de Protección de Datos Personales
Nivel	Profesional
Categoría	Carrera administrativa
Código	2028
Grado	14
Nombre del cargo	Profesional Especializado
Dependencia	Dirección Jurídica
Nro. de cargos	1
Cargo de jefe inmediato	Director Jurídico

Área Funcional

Gestión de la privacidad y protección de los datos personales tratados por la Universidad, asegurando el cumplimiento del marco legal colombiano, las políticas institucionales y los principios de seguridad de la información.

Propósito Principal

Velar por el cumplimiento de la normativa vigente en materia de protección de datos personales, liderar las estrategias institucionales para la gestión responsable de la información personal y articular acciones con el SGSI para garantizar la privacidad, legalidad, confidencialidad y transparencia en el tratamiento de los datos personales de estudiantes, empleados, proveedores y demás partes interesadas.

Funciones Esenciales

- Coordinar la implementación, mantenimiento y mejora del **Programa de Gestión de Datos Personales** de la Universidad.
- Asegurar el cumplimiento de la **Ley 1581 de 2012**, sus decretos reglamentarios y otras disposiciones aplicables.
- Elaborar, actualizar y promover políticas, procedimientos y formatos para el tratamiento adecuado de datos personales.



- Actuar como punto de contacto entre la Universidad y los titulares de la información para atender consultas, reclamos y solicitudes de derechos.
- Identificar y evaluar riesgos asociados al tratamiento de datos personales y proponer controles preventivos.
- Coordinar con el **Oficial de Seguridad de la Información** y otras áreas para implementar medidas técnicas y organizativas de protección.
- Gestionar el Registro Nacional de Bases de Datos ante la **Superintendencia de Industria y Comercio (SIC)**.
- Sensibilizar y capacitar a funcionarios y contratistas sobre el adecuado tratamiento de datos personales.
- Participar en auditorías y reportes de cumplimiento normativo en privacidad.
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Garantizar que la Universidad cumpla con la ley 1581 de 2012 (**protección de datos personales**).
- Supervisar y coordinar la respuesta ante incidentes de seguridad relacionados con fuga, pérdida o acceso no autorizado de datos personales.
- Implementar estrategias para mitigar amenazas a la confidencialidad, integridad y disponibilidad de los datos.



Conocimientos Básicos

- Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1266 de 2008 y regulación internacional (GDPR – si aplica).
- Normas ISO/IEC 27001 y 27701 (extensión de privacidad).
- Principios de seguridad de la información: confidencialidad, integridad y disponibilidad.
- Evaluaciones de impacto en privacidad (PIA/DPIA).
- Gestión de riesgos y tratamiento de datos sensibles.
- Derecho informático, gobierno de datos y ética digital.
- Herramientas de gestión de bases de datos y plataformas de consentimiento.
- Atención a derechos de los titulares (consulta, supresión, corrección, revocatoria del consentimiento).

Formación Académica

Profesional en Derecho, Ingeniería de Sistemas, Administración o áreas afines, con especialización o formación certificada en **Protección de Datos Personales, Derecho Informático, Seguridad de la Información o Gobierno Digital**. Deseable certificación nacional o internacional en gestión de privacidad (Ej. DPD, CDPP, ISO 27701).



ADMINISTRADOR DE CORREOS ELECTRÓNICOS – Auxiliar



Dirección de las Tecnologías y Sistemas de la Información y de las Comunicaciones

ISO 20000-1:2018 e ISO 27001:2022

Rol del cargo	Administrador de correos electrónicos
Nivel	Auxiliar
Categoría	Carrera administrativa
Código	4044
grado	16
Nombre del cargo	Auxiliar administrativo
Dependencia	Dirección de las Tecnologías y Sistemas de Información y las Comunicaciones
Nro. de cargos	1
Cargo del Manual de Funciones	Resolución 1050 de 2018
Cargo de jefe inmediato	Director de TIC

Área Funcional

Gestión, administración, soporte y monitoreo del servicio institucional de correo electrónico, asegurando su disponibilidad, seguridad, continuidad y buen uso por parte de la comunidad universitaria.

Propósito Principal

Administrar y asegurar el funcionamiento eficiente y seguro de la plataforma de correo electrónico institucional, garantizando la disponibilidad del servicio, la correcta configuración de cuentas, la aplicación de políticas de seguridad y el soporte a usuarios, en concordancia con los principios del Sistema de Gestión de Servicios (SGS) e ISO/IEC 27001:2022.

Funciones Esenciales

- Administrar la plataforma de correo electrónico institucional (Google Workspace, Microsoft 365 u otra solución en uso).
- Gestionar la creación, configuración, modificación y eliminación de cuentas de correo para estudiantes, docentes, administrativos y contratistas.
- Aplicar y actualizar políticas de seguridad del correo electrónico: contraseñas, autenticación, filtros de spam, alertas, etc.



- Atender incidentes, solicitudes y problemas relacionados con el acceso y uso del correo electrónico.
- Realizar monitoreo y seguimiento al rendimiento, disponibilidad y posibles amenazas relacionadas con el correo institucional.
- Implementar controles que garanticen la confidencialidad, integridad y disponibilidad de la información que circula por este medio.
- Generar reportes técnicos y estadísticas del uso del correo institucional y entregar soporte a auditorías internas o externas.
- Apoyar campañas de sensibilización y buenas prácticas en el uso seguro del correo electrónico institucional.
- Coordinar con el proveedor o integrador contratado los aspectos técnicos y de soporte del servicio (cuando aplique).
- (Plan de continuidad) Valorar los planes de continuidad para demostrar la responsabilidad y el compromiso en la prestación de los servicios en caso de que ocurra una eventualidad y la importancia de los planes de acción para ser tenidos en cuenta dentro del presupuesto de la universidad.
- La información de contacto de los integrantes de la Dirección de TIC se revisará y actualizará cuando sea necesario.
- Los niveles de prioridad de la atención a la emergencia e incidentes que tendrá en cuenta la DTIC son:
 - Garantizar la seguridad y protección de los seres humanos.
 - Proteger los datos e información de los procesos críticos de la Entidad, considerados estos como los que garantizan el cumplimiento de la misión institucional.
 - Proteger otros datos e información considerada importante para la Entidad
 - Evitar pérdida, alteración o daño a los activos de información producto de los procedimientos de recuperación.
 - Optimizar los procedimientos para minimizar el tiempo de suspensión de los procesos.

Responsabilidades

- Administrar las cuentas de correo electrónico institucionales (creación, modificación, eliminación).
- Asignar permisos y roles de acceso conforme a las políticas de control de acceso (A.8.2 de ISO 27002).
- Configurar y mantener buzones compartidos, listas de distribución y grupos.
- Gestionar alias, reenvíos automáticos y reglas de filtrado.



- Implementar y mantener medidas de seguridad en el servicio de correo:
 - Autenticación multifactor (MFA).
 - Protocolos seguros (TLS, HTTPS).
 - Configuraciones SPF, DKIM y DMARC para validación de remitentes.

- Configurar filtros anti spam y antimalware.
- Supervisar e investigar alertas de correos sospechosos (phishing, suplantación).
- Garantizar el cumplimiento de las políticas de uso aceptable del correo institucional.
- Mantener registros y respaldos conforme a los requisitos legales y regulatorios.
- Monitorear la disponibilidad y el rendimiento del servicio de correo electrónico.
- Revisar y optimizar la capacidad de almacenamiento de buzones.
- Gestionar alertas y notificaciones del sistema para prevenir interrupciones.
- Elaborar reportes periódicos de uso, incidentes y tendencias.
- Atender y resolver incidentes y solicitudes relacionados con el correo electrónico.
- Brindar soporte en la configuración de clientes de correo (Outlook, Thunderbird, apps móviles).
- Capacitar a los usuarios en buenas prácticas de uso seguro del correo.
- Coordinar con el área de infraestructura o nube para asegurar respaldos periódicos de buzones.
- Implementar y probar planes de recuperación ante desastres para el servicio de correo.
- Documentar procedimientos o guías para restauración de cuentas o correos.
- Mantener el software, parches y licencias actualizados (Exchange, Microsoft 365, Google Workspace, Zimbra, etc.).
- Evaluar nuevas funcionalidades y mejoras en el servicio.
- Proponer medidas de optimización y eficiencia en el uso del correo institucional.

Conocimientos Básicos

- Plataformas de correo electrónico institucional (Google Workspace, Microsoft Exchange, Zimbra, etc.).
- DNS, registros SPF, DKIM y DMARC para autenticación de correos.
- Seguridad en el correo electrónico: filtrado anti spam, phishing, malware, control de accesos.
- Herramientas de monitoreo, alertamiento y auditoría de servicios de correo.

- Gestión de cuentas, grupos y políticas de uso.
- Principios de protección de datos personales y cumplimiento normativo.
- Fundamentos de ISO/IEC 27001 (Seguridad de la Información) e ISO/IEC 20000-1 (Gestión de servicios TI).
- Habilidades de soporte técnico, atención al usuario y documentación de procesos.

Formación Académica

Técnico, tecnólogo o profesional en Ingeniería de Sistemas, Informática, Redes o áreas afines. Se valoran certificaciones o formación complementaria en administración de plataformas de correo electrónico, seguridad en redes, o gestión de servicios TI.





Dirección de las Tecnologías y
Sistemas de Información y
de las Comunicaciones

MANUAL DE ROLES Y RESPONSABILIDADES DE LOS FUNCIONARIOS DE DTIC ISO 200001 E ISO 27001



 Gestion.dtic@uptc.edu.co

 <https://www.uptc.edu.co/>