Programa de Concurso Categoría 3 Tics

PROGRAMA

Unidad 1 – Universidad Tecnológica Nacional.

Temas:

Estatuto de la Universidad Tecnológica Nacional. Convenio Colectivo de Trabajo para el Personal Nodocente de la UTN. Estructura organizativa de las áreas de Tic de Rectorado y Facultad Regional Rosario UTN.

Unidad 2 - Infraestructura y redes.

Temas:

Diseño e implementación de servidores. Implementación de servidores físicos o virtuales. Configuración de servicios DNS y DHCP. Implementación de servidor de correo electrónico. Implementación de servidor de páginas web. Implementación de un servidor Proxy. Cifrado Ssl y certificados digitales. Implementación de la gestión de identidades y accesos, e implementación y gestión de políticas de seguridad para el control de acceso a los recursos mediante Active Directory. Implementación de servidor de archivos y servidor de impresión. Diseño de bases de datos relacionales. Implementación de servidor de bases de datos con Microsoft SQL. Diseño de consultas SQL complejas. Aplicación de técnicas para la optimización de consultas y mejora del rendimiento de bases de datos SQL. Replicación de datos. Implementación de servicio de aplicativos Sysacad, Sysdasuten y Sysadmin. Implementación de tecnologías de virtualización Vmware, Proxmox y Hyper-V. Implementación y gestión de redes (Utp, fibra óptica e inalámbricas). Configuración de routers y switches. Implementación de Vlan y enrutamiento entre ellas. Implementación de herramientas de monitoreo de red. Implementación y gestión de sistemas de almacenamiento (raid, clusters, luns y sistemas de almacenamiento en red). Implementación y gestión de copias de seguridad. Recuperación de la información. Gestión de la CMDB (hardware, software, licencias y su ciclo de vida).

Unidad 3 - Seguridad de la información.

Temas:

Políticas y procedimientos de seguridad. Mantenimiento de políticas y procedimientos de seguridad de la información. Identificación y análisis de riesgos de seguridad. Auditoría de los sistemas de seguridad. Gestión de vulnerabilidades. Uso de herramientas de escaneo de vulnerabilidades. Implementación de parches y actualizaciones de software. Implementación de políticas de privacidad, gestión de datos personales y sensibles. Técnicas de encriptación y anonimización. Gestión de acceso a los sistemas académicos, administrativo y aplicaciones de la Universidad. Implementación de políticas de control de acceso, gestión de contraseñas, roles y permisos. Gestión de incidentes de seguridad. Identificación y análisis de incidentes. Implementación de planes de respuesta a incidentes, notificación y documentación. Implementación de medidas correctivas y preventivas. Cumplimiento normativo: cumplimiento de normativas y regulaciones de seguridad de la información contempladas en la Ley de Protección de Datos Personales, Norma ISO 27001 y Resoluciones UTN N.º 135/2020, 213, 977/2022, 1374/2022.

Unidad 4 - Desarrollo de software.

Temas:

Implementación de buenas prácticas de desarrollo de software. Desarrollo mediante metodologías ágiles, modelos de cascada con pruebas continuas, diseño centrado en el usuario y pruebas de software. Conocimientos generales de lenguajes de programación y herramientas utilizadas en el desarrollo de software, incluyendo Php, Java, C++, Python, JavaScript. Gestión de proyectos de software. Planificación de proyectos, la gestión de recursos y presupuestos. Documentación de proyectos. Herramientas y metodologías para el control de versiones de software, la gestión de ramas y la integración continua. Diseño e implementación de pruebas y depuración de software.

Unidad 5 - Soluciones de nube.

Temas:

Diseño, implementación y mantenimiento de infraestructuras de nube. Docker, Kubernetes, Ansible. Implementación de seguridad en la nube, autenticación, autorización, cifrado de la información, control de acceso y auditoría. Regulación General de Protección de Datos (GDPR), Health Insurance Portability and Accountability Act (HIPAA), ISO/IEC 27001 y SOC 2. Gestión de identidades y accesos para los recursos en la nube. Autenticación multifactorial. Monitoreo y detección de amenazas, detección de anomalías y la respuesta a incidentes.

Unidad 6 - Continuidad del servicio.

Temas:

Conocimiento de los procesos y sistemas críticos que afecten a los servicios de Tic. Identificación y evaluación de los riesgos que afecten la continuidad del funcionamiento de los servicios de Tic. Definir medidas de prevención y mitigación de los riesgos. Definición y documentación de planes de continuidad del servicio. Establecimiento de objetivos, metas, definición de roles, y responsabilidades del personal de Tic. Creación de un plan de contingencia y de recuperación de desastres. Análisis de riesgos y vulnerabilidades de los servicios de Tic. Identificación de amenazas potenciales a la infraestructura de TI. Estrategias de coordinación del personal de TI durante la implementación de planes de contingencia. Norma ISO 22301.

Unidad 7 – Atención y satisfacción del usuario.

Gestión y liderazgo de equipos de soporte técnico y atención al cliente. Uso de herramientas para gestión de incidentes y requerimientos de soporte. Uso de herramientas y prácticas para medir y mejorar la satisfacción del cliente.

Bibliografía

- “Redes De Computadoras 5 Edición”, Andrew S. Tanenbaum, Editorial Pearson, ISBN: 9786073208178.
- "Redes de Computadoras: Un enfoque descendente 71 edición" de James F. Kurose y Keith W. Ross, Editorial Pearson, ISBN: 978- 84- 9035- 528- 2.
- "Seguridad Informática: Una visión práctica" de Alfredo Andrés y Antonio Sanz.
- “Bases de datos”, Mercedes Marqués, Editorial Col·lecció Sapientia, ISBN: 978-84-693-0146-3