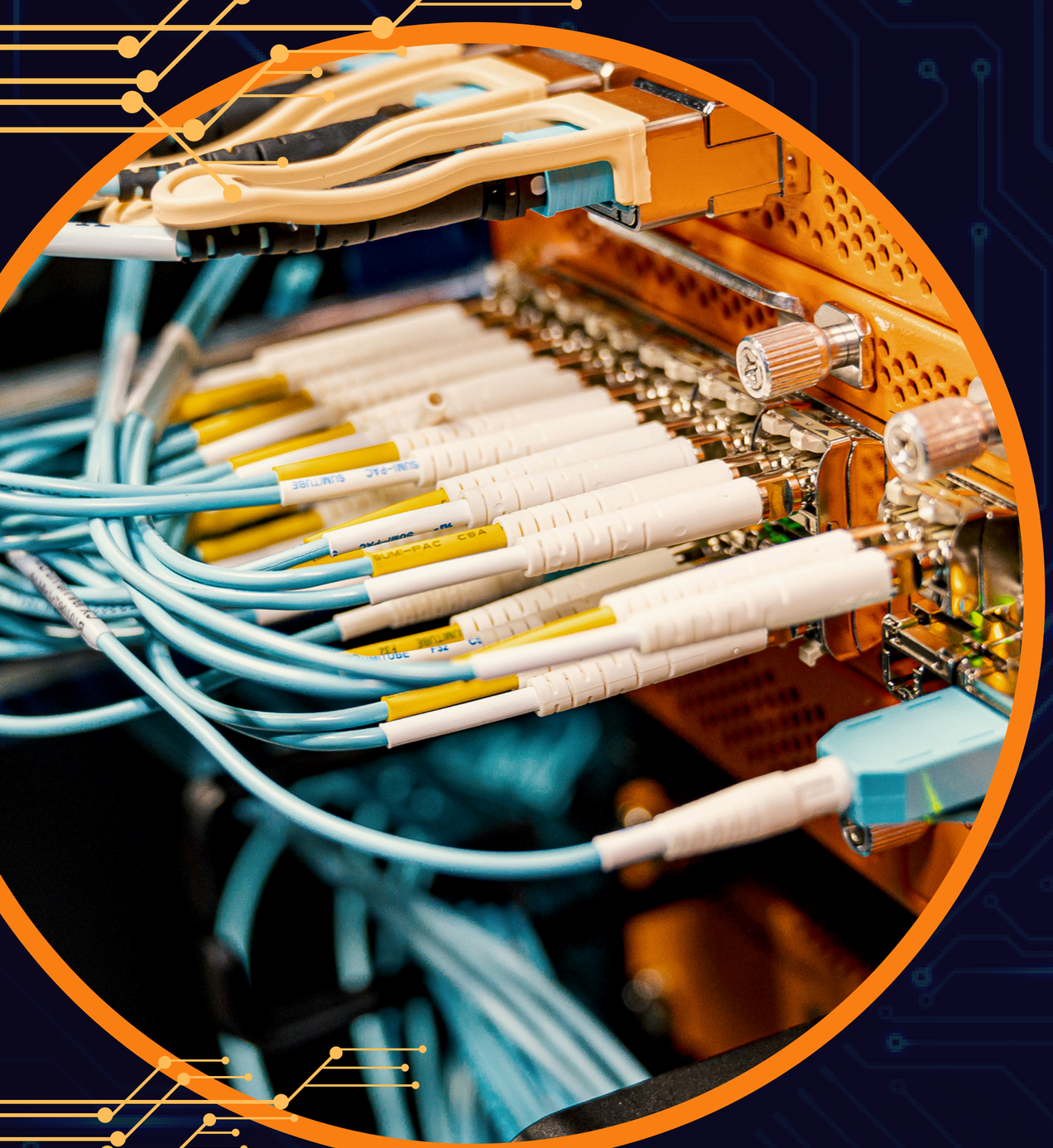

TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3 -UNIDAD 2

Universidad Tecnológica de Pereira

faceIT

Lección 3: Arquitectura segura en la nube:

La arquitectura segura en la nube es el diseño y la implementación de infraestructuras, aplicaciones y servicios en entornos en la nube, con un enfoque específico en la protección de datos, la privacidad y la resiliencia frente a amenazas. Este concepto combina prácticas de seguridad tradicionales con características propias del entorno de la nube, como la elasticidad, la multitenencia y los servicios gestionados. Diseñar una arquitectura segura implica identificar riesgos, implementar controles de seguridad y garantizar el cumplimiento normativo en todas las capas del sistema.

Una arquitectura segura protege contra ciberataques, evita brechas de datos y asegura la continuidad del negocio. Además, una mala configuración, como credenciales mal gestionadas o políticas de acceso deficientes, puede convertir los entornos en la nube en un objetivo atractivo para atacantes. La seguridad en la nube no solo es esencial para la protección técnica, sino también para cumplir con normativas como el GDPR, HIPAA o ISO 27001.

Diseñar una arquitectura segura en la nube comienza con principios básicos: el modelo de responsabilidad compartida, la implementación del principio de privilegio mínimo, la segmentación de redes y la adopción de políticas de defensa en profundidad. Estos principios aseguran que cada capa del sistema (usuarios, aplicaciones, red, datos) tenga controles específicos para mitigar riesgos y limitar el impacto de cualquier ataque.

Gestión de Identidades y Accesos (IAM)

Una de las bases para una arquitectura segura es la implementación adecuada de un sistema de Gestión de Identidades y Accesos (IAM). Esto incluye el uso de autenticación multifactor (MFA), permisos basados en roles (RBAC) y revisiones regulares de accesos. Configurar credenciales únicas y restringir accesos a los recursos según las funciones de los usuarios minimiza riesgos de acceso no autorizado.

Encriptación de Datos en Tránsito y en Reposo

La encriptación es una medida esencial para proteger datos sensibles en la nube. Los datos deben estar cifrados tanto en tránsito (por ejemplo, mediante HTTPS y TLS) como en reposo, utilizando claves de cifrado gestionadas de manera segura. Además, las organizaciones deben asegurarse de que los proveedores de servicios en la nube ofrezcan herramientas integradas para gestionar claves y auditar el uso del cifrado.

Segmentación de Redes y Seguridad Perimetral

Dividir la red en segmentos lógicos y limitar la comunicación entre ellos reduce la exposición a posibles ataques. En la nube, esto se puede lograr mediante el uso de Virtual Private Clouds (VPC), firewalls, reglas de seguridad y puertas de enlace NAT. Las conexiones externas deben estar protegidas mediante VPNs o túneles seguros, y los servicios públicos deben ser monitoreados constantemente.

Monitorización y Detección de Amenazas

Un diseño seguro incluye la implementación de herramientas de monitorización continua para detectar actividades sospechosas. Los servicios en la nube suelen proporcionar herramientas como AWS CloudTrail, Azure Security Center o Google Cloud Logging, que registran y analizan eventos. La integración de sistemas de detección de intrusos (IDS) y soluciones SIEM puede ayudar a identificar y responder rápidamente a incidentes de seguridad.

Resiliencia y Recuperación ante Desastres

Una arquitectura segura no solo debe prevenir ataques, sino también garantizar la recuperación rápida ante fallos. Esto incluye la configuración de backups automáticos, replicación de datos en diferentes regiones y estrategias de recuperación ante desastres (DR). El uso de múltiples zonas de disponibilidad permite a las aplicaciones mantener operaciones incluso si ocurre un problema en una ubicación específica.

Cumplimiento Normativo y Auditorías

Los entornos en la nube deben cumplir con regulaciones y estándares específicos según la industria y la región. Diseñar la arquitectura teniendo en cuenta marcos como NIST, PCI DSS o ISO 27001 garantiza que las operaciones sean seguras y conformes. Además, las auditorías regulares ayudan a identificar brechas en la seguridad y mejorar continuamente las políticas implementadas.