Marco Normativo y Regulatorio Aplicado al Proyecto "Orquestador de Infraestructura de Red"

Introducción

El **Orquestador de Infraestructura de Red** es un proyecto orientado a la automatización, monitoreo y gestión de dispositivos en una red híbrida que integra servidores físicos, entornos virtualizados y servicios en la nube mediante AWS Academy. Debido a su criticidad, el proyecto deberá enmarcarse en un conjunto de normas, leyes y marcos de referencia que aseguren la seguridad de la información, la protección de datos personales, la calidad del software y la gobernanza de TI.

1. Cumplimiento legal y protección de datos

El orquestador deberá cumplir con la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**. Para ello será obligatorio:

- Establecer políticas de retención de datos que definan un tiempo máximo de conservación de logs: 90 días en línea y 12 meses archivados.
- Implementar mecanismos de anonimización en reportes de auditoría.
- Limitar el acceso a datos sensibles mediante roles diferenciados y controlados.

En entornos internacionales, el orquestador deberá alinearse con el **Reglamento General de Protección de Datos (GDPR)**, garantizando la minimización de datos, el consentimiento explícito de usuarios, el derecho de supresión y la notificación de incidentes en un máximo de 72 horas.

Evidencia esperada en auditoría: políticas de privacidad aprobadas, registros de retención de logs, reportes con anonimización aplicada.

2. Seguridad informática y ciberseguridad

El orquestador deberá implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)** conforme a la norma **ISO/IEC 27001:2022**. Los controles mínimos exigidos serán:

- Autenticación multifactor en todos los accesos administrativos.
- Uso obligatorio de protocolos seguros (SSH, SNMPv3, TLS 1.2+).
- Generación de registros de auditoría inmutables protegidos contra alteración y **exportables a plataformas corporativas de monitoreo**.
- Pruebas periódicas de vulnerabilidades.

Asimismo, el orquestador se regirá por el **NIST Cybersecurity Framework 2.0**, adoptando sus cinco funciones: identificar, proteger, detectar, responder y recuperar. Estas funciones se traducirán en inventarios de activos, configuraciones seguras, alertas automáticas, manuales de respuesta a incidentes y planes de recuperación con RTO de 4 horas y RPO de 1 hora.

De manera complementaria, los **Controles CIS v8** serán de aplicación obligatoria, incluyendo la gestión activa de vulnerabilidades, el control de cuentas administrativas y el monitoreo constante de registros críticos.

Evidencia esperada en auditoría: reportes de autenticación multifactor, registros de auditoría firmados digitalmente, actas de pruebas de recuperación, resultados de escaneos de seguridad.

3. Seguridad en la nube

El uso de **AWS Academy** estará regido por los lineamientos de la **ISO/IEC 27017** y la **ISO/IEC 27018**. En consecuencia, el orquestador deberá:

- Administrar identidades en IAM bajo el principio de menor privilegio.
- Cifrar obligatoriamente los datos almacenados en S3 y procesados en EC2 mediante KMS.
- Mantener habilitada la auditoría de eventos con CloudTrail.
- Validar configuraciones mediante AWS Config.
- Someterse a revisiones periódicas con el AWS Well-Architected Framework.

Evidencia esperada en auditoría: políticas de IAM aprobadas, registros de CloudTrail revisados, reportes de AWS Config y Well-Architected.

4. Licenciamiento y uso de software

El orquestador deberá garantizar la legalidad en el uso de software. Será obligatorio:

- Mantener un inventario de licencias propietarias (Cisco IOS, VMware ESXi, .NET Framework, AWS).
- Documentar las dependencias de software libre (Python, GNS3, VirtualBox, C# .NET) y su cumplimiento de licencias GPL/MIT.
- Establecer procedimientos de actualización y validación de compatibilidad.

Evidencia esperada en auditoría: listado de licencias activas, inventario firmado de dependencias, documentación de parches y actualizaciones.

5. Políticas internas y continuidad de negocio

El orquestador deberá operar bajo políticas internas formales:

- **Política de accesos:** autenticación multifactor obligatoria, revisión de permisos cada 90 días, revocación inmediata de accesos inactivos.
- **Política de cambios:** todo cambio deberá ser gestionado mediante RFC documentado, probado en laboratorio y aprobado por doble autorización.
- **Política de incidentes:** cada incidente deberá registrarse y gestionarse según manuales predefinidos, con responsables y protocolos de comunicación claros.
- **Política de continuidad:** se deberán generar respaldos automáticos diarios, copias inmutables semanales y pruebas de recuperación semestrales.

Evidencia esperada en auditoría: actas de revisión de accesos, registros de cambios aprobados, manuales de incidentes vigentes, reportes de pruebas DRP.

6. Calidad y usabilidad del software

El orquestador será evaluado según la norma **ISO/IEC 25010**, cumpliendo los siguientes atributos:

- **Usabilidad:** interfaz en .NET intuitiva y accesible.
- **Fiabilidad:** backend en Python estable bajo carga.
- **Compatibilidad:** interoperabilidad con dispositivos Cisco, VMware y Windows.
- **Seguridad:** integración de pruebas SAST y DAST en cada ciclo de desarrollo.

Evidencia esperada en auditoría: reportes de QA, resultados de pruebas de carga, análisis de seguridad sobre el código.

7. Gobernanza y gestión de TI

El orquestador se regirá obligatoriamente por:

- **ITIL v4:** para estructurar la gestión de incidentes, problemas y cambios.
- **COBIT 2019:** para establecer métricas de gobernanza de TI y evaluar madurez organizacional.

Evidencia esperada en auditoría: registros de incidentes con tiempos de resolución, dashboards de disponibilidad, reportes de auditoría de madurez.

8. Integración normativa aplicada al proyecto

Norma / Marco	**Requisito clave**	**Aplicación en el Orquestador**	**Evidencia esperada**
ISO/IEC 27001	Seguridad de la información	MFA, protocolos cifrados, registros inmutables exportables	Políticas de acceso, registros de auditoría
NIST CSF 2.0	Ciclo de ciberseguridad	Inventario de activos, planes de respuesta y recuperación	Manuales y pruebas DRP
CIS Controls v8	Controles técnicos	Inventarios, gestión de vulnerabilidades, control de cuentas	Escaneos de seguridad
ISO/IEC 27017-27018	Seguridad en la nube	IAM least privilege, cifrado en S3/EC2, CloudTrail	Configuraciones AWS, reportes
LFPDPPP	Protección de datos	Retención y anonimización de logs	Política de privacidad
ISO/IEC 25010	Calidad del software	Usabilidad, fiabilidad, compatibilidad	Reportes de QA
ITIL v4	Gestión de servicios	Procesos de incidentes y cambios documentados	Registros de incidentes

COBIT 2019	Gobernanza de TI	Indicadores de control y madurez	Dashboards de auditoría