PROYECTO DE APLICACIÓN

1.Explicación y descripción de los elementos clave

1.1. Arquitectura de la infraestructura

- Objetivo: Diseñar una infraestructura escalable, redundante y de alta disponibilidad.
- Componentes clave:
    - Uso de microservicios.
    - Balanceadores de carga para distribuir el tráfico.
    - Zonas de disponibilidad para evitar puntos únicos de fallo.
    - Monitoreo de la infraestructura con herramientas como Prometheus.

1.2. Seguridad en la nube

- Objetivo: Proteger los recursos alojados en la nube mediante configuraciones seguras y políticas de acceso.
- Componentes clave:
    - Configuración segura de buckets de almacenamiento (por ejemplo, S3 en AWS).
    - Seguridad en tránsito y en reposo mediante cifrado.
    - Políticas de acceso basadas en roles (IAM).

1.3. Desarrollo de aplicaciones seguras

- Objetivo: Minimizar vulnerabilidades en el ciclo de desarrollo de software.
- Componentes clave:
    - Validación de entradas para prevenir inyecciones de código.
    - Implementación de pruebas automáticas de seguridad.
    - Uso de estándares como OWASP Top 10.

1.4. Gestión de identidades y accesos

- Objetivo: Controlar y auditar el acceso a los recursos sensibles.
- Componentes clave:
    - Autenticación multifactor (MFA).
    - Políticas de contraseñas fuertes.

    - Supervisión y auditoría de accesos.

1.5. Seguridad de la red

- Objetivo: Proteger la red contra accesos no autorizados y ataques.
- Componentes clave:
    - Segmentación de red.
    - Uso de firewalls y listas de control de acceso (ACL).
    - Implementación de VPNs seguras.

1.6. Gestión de claves y cifrado

- Objetivo: Garantizar que los datos sensibles estén protegidos.
- Componentes clave:
    - Uso de módulos de seguridad de hardware (HSM).
    - Rotación periódica de claves de cifrado.
    - Gestión de certificados SSL/TLS.

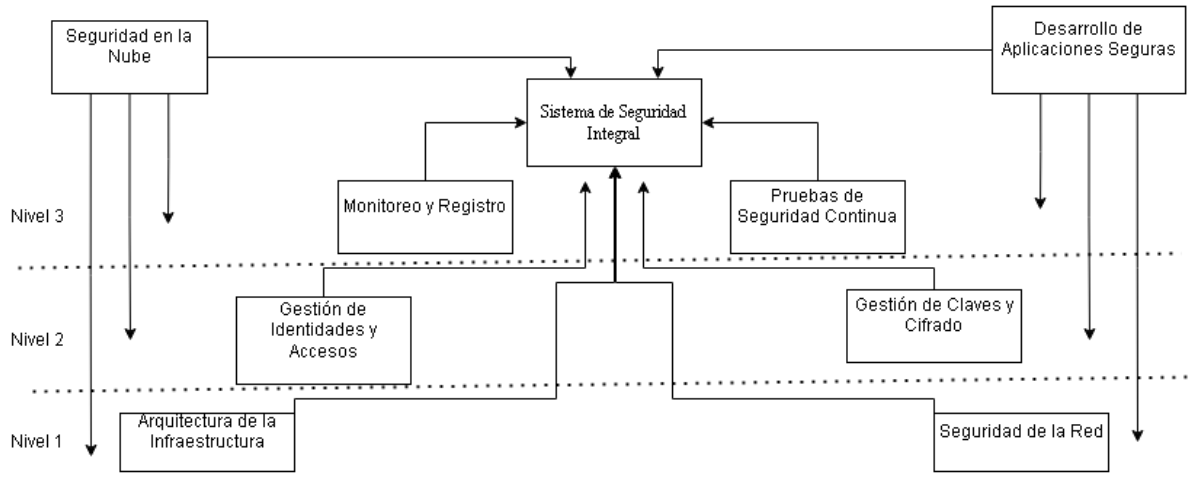
1.7. Monitoreo y registro

- Objetivo: Detectar y responder a incidentes en tiempo real.
- Componentes clave:
    - Implementación de un SIEM (Security Information and Event Management).
    - Monitoreo de logs y alertas en tiempo real.
    - Análisis forense de eventos.

1.8. Pruebas de seguridad continua

- Objetivo: Identificar vulnerabilidades de manera proactiva.
- Componentes clave:
    - Pruebas de penetración periódicas.
    - Simulaciones de ataques (red teaming).
    - Integración de pruebas de seguridad en el ciclo de desarrollo (DevSecOps).

2.Modelo



Bibliografía

Arquitectura de infraestructura tecnológica y su valor empresarial. (2020, noviembre 13). Aicad Business School. https://www.aicad.es/arquitectura-de-infraestructura-tecnologica

Articles. (s/f). CSA. Recuperado el 22 de enero de 2025, de https://cloudsecurityalliance.org/articles

Torrejón, M. (2022, noviembre 30). *Buenas prácticas para un desarrollo seguro*. El blog de Omatech; Omatech. https://www.omatech.com/blog/2022/11/30/buenas-practicas-para-un-desarrollo-seguro/