

ANEXO N.º 3: ESTÁNDARES DE DESARROLLO.

3.1 AMBIENTE DE DESARROLLO Y PRUBAS

El oferente debe tener presente que el desarrollo del software debe realizarse en los ambientes de desarrollo y pruebas que la Subsecretaría disponga para ello, siendo necesario que el oferente se adhiera a las herramientas y frameworks de desarrollo de software aprobados por la Coordinación Nacional de Tecnología de la Subsecretaría de Educación, tomando especial atención a los lineamientos técnicos y restricciones de dicha infraestructura.

Será responsabilidad del oferente realizar todo el levantamiento técnico necesario para que el desarrollo del software y pruebas en los ambientes de la Subsecretaría de Educación sea una actividad fluida y constante. Además, el diseño de solución definitivo debe ser aprobado por el Área de Desarrollo de la Coordinación Nacional de Tecnología del MINEDUC.

Si el sistema utiliza o proyecta más de 1.000.000 de visitas al mes, el proyecto debe asegurar la compra de recaptcha Enterprise, de acuerdo a la proyección de carga señalada anteriormente.

3.2 SEGURIDAD

El desarrollo del sistema debe cumplir con los estándares de seguridad de la Subsecretaría, descritos en el Anexo 5.4 de este documento, los cuales se consideran parte integral de los requerimientos.

Se deben aplicar las políticas de seguridad establecidas en: REX 294 POLITICA DE REGISTRO DE LOGS indicado en el anexo de políticas de seguridad.

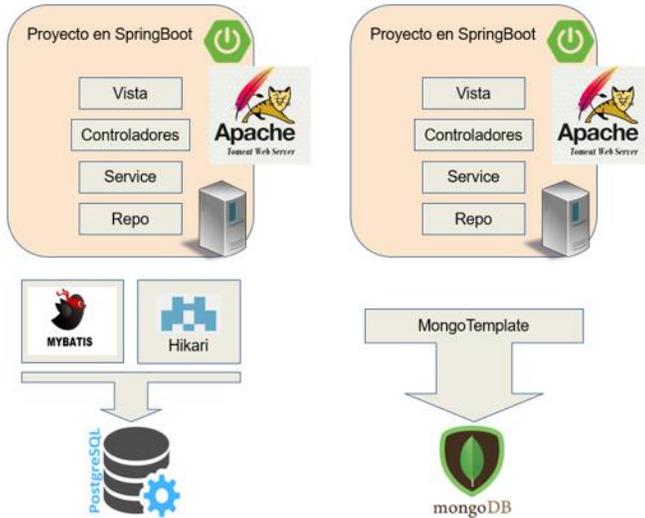
Pruebas de vulnerabilidad en CSIRT de gobierno, como resultado del informe, se deben solucionar las vulnerabilidades identificadas, se deben realizar una o más verificaciones de vulnerabilidad, las que deben ser coordinadas para levantar alertas tempranas de seguridad.

3.3 ARQUITECTURA REQUERIDA

Se describe a continuación la arquitectura de software propuesta por la Coordinación Nacional de Tecnología.

- a. Uso de tecnología Docker para realizar escalamiento horizontal (uso de contenedores)
- b. Herramienta de control de calidad del código (Sonarqube)
- c. Cumplimiento de 50% de cobertura, Sonar/Jenkins a producción.
 - Sin existencia de errores de tipo SmellCode
 - Sin Bugs
 - Sin vulnerabilidades de seguridad
- d. Herramienta de orquestación del ciclo de vida del SW (Jenkins)
- e. Repositorio que permite gestionar proyectos y controlar versiones de código: GITHUB
- f. Un repositorio de SW reutilizable (Nexus)
- g. Pruebas Automatizadas
- h. Elastic Search, Logstash y Kibana
- i. Implementar el código el Google analytics y/o TAG requeridos para el proyecto.

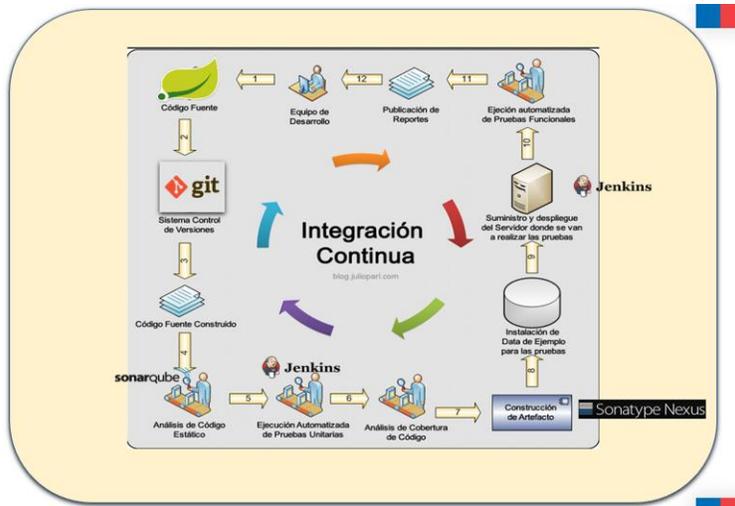
- j. Uso de base de datos Postgres y/o MongoDB
- k. Si el proyecto usa CMS, debe utilizar WordPress.



Framework Coordinación Nacional de Tecnología

3.4 MEJORA CONTINUA

El desarrollo del servicio requerido debe adaptarse al siguiente proceso de mejora continua definido por la Coordinación Nacional de Tecnología del Ministerio de Educación.



3.5 VERSIONES DE HERRAMIENTAS Y SW BASE

Versiones de herramientas y software base a utilizar por el oferente:

- Sistema operativo: CentOS 7
- Servidor de aplicación: Tomcat 8 (JDK 1.8)
- Sistema de control de versiones: GIT
- IDE para desarrollo: Eclipse NEON/Oxygen/STS
- Framework: Spring Boot 2.3.3
- Repositorio de librerías: MAVEN 2.5.1

- Plantillas presentación: Freemaker 2.3.23
- Generación de reportes: PDFMake
- Seguridad: Spring Security 4.0.1
- Ejecución de test unitarios: Junit 4.13
- ORM: MyBATIS 3.5.4
- Integración continua : Jenkins 2.150.2
- Revisión de código: SONAR 5.6.3
- Mensajería (colas): Erlang 21.1.1.

3.6 DESARROLLO DE API

Se debe considerar swagger-UI y API KONG como herramientas para la implementación de eventuales API requeridas por el sistema.

