Política de desarrollo seguro

INTRODUCCIÓN:

Certicamara vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requisitos de seguridad definidos basado en buenas practicas de desarrollo seguro de aplicativos, así como con metodologías para la para la realización de pruebas de aceptación y seguridad. Se asegura que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido.

ALCANCE

Los elementos de seguridad sugeridos en este documento cubren el ciclo de vida del proceso de desarrollo de software, siendo relevantes las siguientes etapas:

- ✓ Especificación de requerimientos
- ✓ Análisis y diseño
- ✓ Planeación
- ✓ Implementación
- ✓ Aseguramiento de la calidad
- ✓ Paso a producción
- ✓ Entrega de productos y componentes

MARCO LEGAL Y/O TÉCNICO

ISO/IEC 27001: Estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements), es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Política de desarrollo seguro

SEGURIDAD DEL AMBIENTE DE DESARROLLO

- Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción. El Administrador del Sistema es responsable de controlar y verificar el cumplimiento de esta política.
- En cuanto a gestión de librerías y artefactos, para lo proyectos nuevos se debe mantener un repositorio centralizado dentro de Certicámara (ejemplo Apache Archiva) que permita gestionar de manera segura los artefactos de cada proyecto. Se debe usar una herramienta tipo Apache Maven para gestionar de manera unificada las dependencias y librerías, esta herramienta debe configurarse para que apunte al repositorio de artefactos de Certicámara.
- Las máquinas de desarrollo, pruebas y producción, deberán contar con controles de acceso exclusivos a los funcionarios que deberían tener acceso a las mismas. El área de TI o Seguridad de la información deberá gestionar el acceso a dichas máquinas, velando por el cumplimiento de las políticas de seguridad y acceso a dichos recursos.
- Los procedimientos de gestión el hardware y el software desplegado en los diferentes ambientes será dado por los lineamientos de tecnología y será controlado por ellos, a menos que una situación especial demande otro tipo de control. Se recomienda:
    - Tecnología debe tener acceso exclusivo al ambiente de producción
    - Tecnología y desarrollo podrían tener acceso compartido al ambiente de desarrollo, mientras que cualquier cambio sobre el mismo se registre y coordine entre las áreas.

DIRECTRICES DE CODIFICACIÓN SEGURA

Centro de los lineamientos para codificación segura, durante el ciclo de vida de desarrollo de software, para cada componente desarrollado existen directrices frente a los siguientes aspectos: nivel de servicios, bases de datos, portales web y aplicaciones de escritorio

Política de desarrollo seguro

REPOSITORIOS SEGUROS DE CÓDIGO

Todo el código de los proyectos, para todos los ambientes (desarrollo, pruebas, producción, u otros) deberán encontrarse en el repositorio seguro de versiones. El instructivo y lineamientos sugeridos para realizar una correcta gestión de dicho repositorio se encuentra en control de versiones.

El acceso al repositorio se controlará a través de credenciales de acceso y autorización por llave RSA pública compartida entre la máquina del desarrollador y el servidor de repositorio de versiones.

Cualquier operación sobre el repositorio (consultar, adicionar o modificar) requiere autenticación y autorización, y esta será gestionada por el Gerente TIC. Teniendo por cada proyecto un esquema de usuarios y perfiles, que determinan si un recurso de la empresa tiene acceso al proyecto y qué permisos específicos posee, limitando de esta forma las personas y lo que puedan realizar con cada proyecto.

El repositorio de versiones deberá contar como mínimo con:

- ✓ Autenticación con credenciales de acceso (usuario y contraseña)
- ✓ Autenticación haciendo uso de llave RSA pública (generada clave privada en máquina, y llave pública registrada en el repositorio GIT).
- ✓ Autorización haciendo control de Acceso a proyectos, según el perfil asignado al usuario (cómo mínimo Desarrollo, QA y Director).