Liberada versión v03r03 de la normativa "Gestión de entregas"

Directrices para Aplicaciones Dockerizadas: Un Entorno Seguro y Controlado

En esta entrada, informamos sobre las directrices esenciales para las aplicaciones dockerizadas, aplicables a los proyectos que, según acuerdos previos, deben entregar su propio Docker. Esta información se detalla en el artículo "Archivos de las aplicaciones. Consideraciones generales", específicamente en el apartado dedicado a las directrices para aplicaciones dockerizadas.

La información detallada está incluida en el artículo Archivos de las aplicaciones. Consideraciones generales donde se ha incluido el apartado con las directrices que se han de aplicar en aplicaciones dockerizadas.

Alcance de la versión normativa "Gestión de entregas"

Aplicaciones Dockerizadas

Para los productos que, bajo acuerdo con el Área de Gobernanza, entregan su propio Docker, es imprescindible cumplir con las siguientes directrices:

1. **Origen de la Imagen**: La imagen especificada en el Dockerfile debe ser exclusiva del registry DML de la STIC. Se prohíbe el uso de repositorios externos para evitar inconvenientes con Docker Hub.
2. **Especificación de la Imagen Fuente**: La instrucción `FROM` en el Dockerfile debe reflejar la ruta exacta de la imagen fuente dentro de la DML. Ejemplo: `FROM ${REGISTRY}/apine:3.20.0`.
3. **Incorporación de Nuevas Imágenes**: Si la imagen requerida no está disponible en la DML, se debe solicitar su inclusión en el repositorio correspondiente.
4. **Referencia al Registry**: El Dockerfile debe incluir una referencia al registry, proporcionada vía build argument con el nombre `REGISTRY` .

Estas medidas están diseñadas para garantizar un entorno controlado y seguro, facilitando así el desarrollo y despliegue eficiente de aplicaciones dockerizadas.