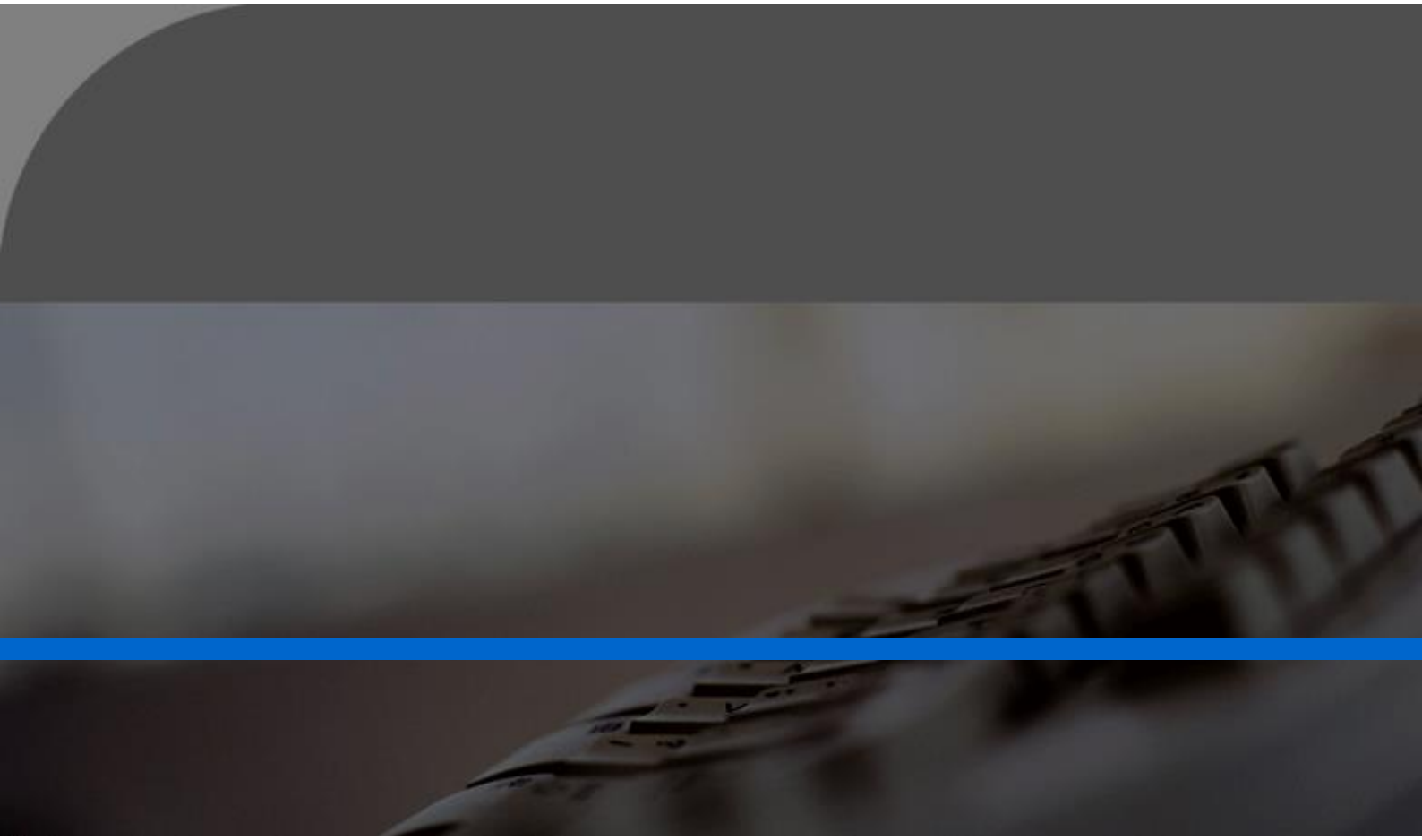
GOBIERNO de CANTABRIA
Consejería de Presidencia y Justicia



3 de Junio de 2019

Versión 1.0.3

APLICACIÓN MIGRADA

CONVENCIONES DE CÓDIGO EN DESARROLLO JEE	
Se le ha asignado a la aplicación un código identificativo único	
OTRAS CONSIDERACIONES	
FICHERO DE LOG	
Se especifica el logging-profile en el fichero MANIFEST.MF	
FICHERO DE PROPIEDADES	
Las propiedades relacionadas con sistemas se guardan en un fichero de propiedades externo a la aplicación	
La nomenclatura del fichero es la adecuada.	
La nomenclatura de las propiedades es la adecuada.	
DATASOURCES	
El datasource se define vía jndi	
La variable jndi sigue la nomenclatura especificada	
VERSIONADO	
El software entregado especifica un número de versión y corresponde con el versionado del código fuente. Esta versión deberá ser posterior a la del último despliegue en producción.	
EMPAQUETADO	
El nombre del distribuible sigue la nomenclatura especificada.	
El nombre del contexto web debe coincidir con el nombre de la aplicación o en su defecto, estar notificado y registrado en el inventario de aplicaciones.	
CÓDIGO FUENTE	
Se ha proporcionado el código fuente	
El ear proporcionado coincide con el ear generado desde el código fuente.	
DOCUMENTACIÓN	
Existencia de DRF y Análisis con información coherente como indican las normas de AMAP	
Existencia de documentación de pruebas y Manual de usuario como indican las normas de AMAP (no necesario si no es despliegue de producción)	
En el Inventario de Aplicaciones (INVAPP) se debe indicar todos los componentes amap utilizados	
CONSULTAS A BASE DE DATOS	

Las consultas serán de un rendimiento razonable, en caso de requerirse consultas que requieran de una cantidad masiva de registros o con una mezcla de tablas poco convencional (no unida por claves ajenas, campos indexados o similares) deberán ser indicadas al grupo de arquitectura para su validación.	
VERSIÓN DE LOS COMPONENTES AMAP	
Los componentes AMAP empleados en las aplicaciones que estén recogidos en el POM padre, no deberán indicar la versión. Para los componente no recogidos en el POM padre, será recomendable el uso de un rango para indicar la versión.	
AMAP-GESTOR-DOCUMENTAL	
Se debe utilizar el gestor documental versión 2.x (indicar en el resumen el incumplimiento)	
SEGURIDAD	
INYECCIÓN SQL	
No deben existir generación de consultas SQL basada en la concatenación directa (sin comprobación) de parámetros obtenidos de la petición. Utilizar en su lugar procedimientos preparados con variables parametrizadas.	
CROSS-SITE SCRIPTING (XSS)	
No deben existir generación de elementos de presentación (html y javascript especialmente) basada en la utilización directa (sin comprobación) de parámetros obtenidos de la petición.	
JSESSIONID	
En el web.xml para que no aparezca en la url el valor jsessionid, deberá haber una entrada como sigue: **<session-config>** **<tracking-mode>COOKIE</tracking-mode>** **</session-config>** **No aplica para aplicaciones que no tengan sesión (ejem: web services)**	
CROSS-SITE REQUEST FORGERY (CSRF) / PUBLICACIÓN DE INFORMACIÓN SENSIBLE	
Las operaciones marcadas como críticas por parte del analista/usuario (que comprometa los datos más sensibles o impliquen una operación que tenga implicaciones importantes) se añadirá a la petición un captcha, token aleatorio o mecanismo de seguridad adicional similar que será comprobado en la parte servidora, para asegurar el origen no fraudulento de la petición.	
REFERENCIAS A OBJETOS INSEGURAS	
Para los datos críticos indicados por el analista/usuario no debe haber	

parámetros (GET o POST) con información directa de la base de datos (IDs de BBDD, ficheros, directorios, claves, etc.) sin que el usuario tenga autorización suficiente para los mismos.	
Conexión con LDAP	
Comprobar que al conectar con LDAP se le pasa el usuario y contraseña para evitar Anonimous Binding	

* NOTA: las normas en negrita son bloqueantes

1.1. RESUMEN