ASPECTOS DE SEGURIDAD, ESCALABILIDAD, USABILIDAD E INTEROPERABILIDAD DE INVIMA A UN CLIC

1. Seguridad

- Autenticación

Los usuarios se registran en un portal web, los nombres de usuarios y contraseñas proporcionadas se almacenan en el producto Red Hat Single Sing-On (RH-SSO)[1], el cual proporciona todas las funcionalidades básicas y avanzadas de seguridad que requiere una aplicación web en cuanto a autenticación se refiere[2]. La contraseña debe ser de mínimo 8 caracteres que incluyan letras en mayúscula y minúscula, números y caracteres especiales. El producto usa estándares de la industria de Tecnologías de la Información y ha sido ampliamente probado en varias soluciones de la misma naturaleza[3].

El SSO-RH tiene un componente de base de datos en el cual se almacena de forma persistente la información de los usuarios; allí las contraseñas se almacenan cifradas de modo que los administradores de bases de datos o cualquier otro usuario no puedan tener acceso a ellas.

La aplicación usa el protocolo de autenticación OAuth2, el cual es un estándar de industria, donde se crea un proveedor de seguridad externo a la aplicación, donde se gestionan las contraseñas y las aplicaciones clientes se comunican con este proveedor a través de *token* de sesión.[4]

- Autorización

Se han definido roles que determinan qué puede hacer cada usuario una vez esté autenticado en el sistema. Los accesos internos a los componentes de la solución están integrados con el directorio activo de la entidad de tal forma que al inhabilitar un usuario automáticamente se inhabilita de los componentes de la solución Invima a un clic.

- Cifrado

El componente web de la solución está expuesto al público en general, es por ello, que se utilizan protocolos de cifrado (SSL) para proteger el tráfico de datos entre el navegador del cliente y los servidores del Invima. Lo anterior teniendo en cuenta la no degradación del rendimiento del

[1] Ver la siguiente URL : http://aunclic.invima.gov.co:8182/auth/realms/InvimaExternos/protocol/openid-connect/auth?client_id=account&redirect_uri=http%3A%2F%2Faunclic.invima.gov.co%3A8080%2FInvima-portal-web%2Findex.html%3Fredirect_fragment%3D%252Fapp%252Finicio&state=b297b00c-eb5a-43d0-91b8-5be3f6c6d2d4&nonce=21f825e9-ed31-4629-8504-43941687ef7a&response_mode=fragment&response_type=code&scope=openid

[2] https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/7.2_release_notes/authentication

[3] https://www.redhat.com/en/technologies/industries/government/products

[4] https://oauth.net/2/

componente web. Adicionalmente, el certificado es protegido por un equipo de propósito específico (SSL INSPECTION) que minimiza el riesgo de un ataque sobre dicho protocolo.

Adicionalmente los archivos adjuntados son cifrados usando algoritmos AES (Advanced Encryption Standard) con bloques de 128 bits, lo que garantiza que los archivos solo pueden ser abiertos por las personas que tengan permiso a los mismos.

2. Escalabilidad, disponibilidad y rendimiento

La solución de Invima a un clic está soportada por una infraestructura de alta disponibilidad lo que permite a su vez escalar de manera fácil para soportar una alta concurrencia de usuarios.

Se cuenta con balanceadores de carga que realizan la distribución de peticiones de los usuarios entre los diferentes servidores de la solución.

La plataforma perimetral cuenta con equipos de propósito específico como: Sistema de Mitigación de Ataques (DDOS-WAF-IPS), Antimalware, Firewall UTM, entre otros. Los cuales minimizan el riesgo de un ataque cibernético.

El componente de base de datos cuenta con un esquema de alta disponibilidad y recuperación ante fallos. Se realizan copias de respaldo de los datos de modo que se puedan soportar procesos de recuperación ante pérdidas eventuales de información por causas no controlables por el negocio.

Los componentes BPM, SOA y ESB de la solución tienen configurada la alta disponibilidad que garantiza atender todas las peticiones de instancias de procesos de negocio.

El componente del ESB aplica los atributos de calidad sobre los servicios construidos en la solución, de igual manera permite realizar gestión y monitoreo de dichos servicios. Por ejemplo, en el ESB se aplican las políticas de seguridad a los servicios web de tal manera que dichos servicios no puedan ser consumidos por componentes no autorizados al interior de la entidad.

Se ha tomado ventaja de las características de los procesos de negocio (larga duración) para realizar tareas asincrónicas que aumentan el número de peticiones y de usuarios que la plataforma puede resolver por unidad de tiempo. La transferencia de documentos hacia los servidores de manejo de contenido se realiza en horas de bajo tráfico de modo que la red no se vea congestionada y por lo tanto no se afecte la disponibilidad del sistema.

3. Usabilidad

La plataforma utiliza tecnologías en el lado cliente (Angular y HTML5) que permiten reducir el tráfico en la red mediante la optimización de peticiones a los servidores del Invima, lo anterior resulta en mejor experiencia de usuario ya que no hay refresco total de páginas, se refrescan segmentos pequeños de dichas páginas.

En la plataforma web el usuario puede realizar de forma totalmente automática los trámites ante el Invima, incluso se pueden cargar los documentos, de hasta 150 MB, que soportan dichos trámites.

4. Interoperabilidad

La solución mantiene una vista holística de todo el proceso de negocio mediante la interacción segura con otros aplicativos de la entidad, lo anterior también brinda integridad de datos en cuanto a una vista de negocio. Se ha creado un modelo canónico que permite mantener una vista integrada de entidades de negocio y a la vez reduce el número de transformaciones que deben realizarse al intercambiar datos entre los diferentes componentes de la solución.