

Requerimientos No funcionales de seguridad de la información

El sistema debe permitir la gestión de usuarios (creación, suministros de acceso, asignación de privilegios, revocatoria de accesos, etc.), roles y perfiles, grupos de usuarios, asociación de acciones para cada rol y administración exclusiva del administrador de la aplicación.

Debe permitir generar registros de los ingresos a la aplicación y las actividades realizadas por los usuarios.

El sistema debe garantizar el cumplimiento del régimen general de protección de datos personales. Cuando el sistema solicite información personal al usuario final, se debe establecer un mecanismo para obtener la autorización y tener prueba de ellos (log).

El sistema debe tener capacidad de resguardar y procesar la información generada o procesada dando cumplimiento a lo exigido por la Ley 1581 de 2012

El sistema debe cerrar las transacciones luego de máximo 10 minutos de inactividad.

El sistema debe exigir características especiales a las contraseñas: mínimo de 8 caracteres, símbolos, números, mayúsculas y minúsculas.

El sistema debe incluir controles de bloqueo de cuenta después de un máximo de 3 intentos erróneos a fin de evitar ataques de fuerza bruta.

La aplicación debe cumplir con controles de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad, integridad y disponibilidad de la información y acceso a ella.

Debe cifrar las comunicaciones de los servicios que puedan estar expuestos en redes públicas

El sistema debe permitir la implementación de certificados digitales.

El sistema debe funcionar sobre protocolo TLS versión 1.2 mínimo (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).

El proveedor del sistema de información debe permitir realizar un análisis de vulnerabilidades y corregir los defectos encontrados antes de entregar el sistema en las instancias de producción.