Tabla de contenido

1. INTRODUCCION

La resolución 792 expedida por el Ministerio de Transporte el 3 de abril del 2013 especifica el procedimiento y las condiciones técnicas de homologación y recertificación de los servicios web para la activación e interacción de actores con el registro único nacional de tránsito RUNT. El informe de conformidad de la auditoria de seguridad es uno de los documentos que debe anexar el interesado en homologar su sistema para interactuar con el sistema RUNT por medio de servicios.

2. OBJETIVO

El presente documento da alcance a los requisitos de cumplimiento por parte de los aspirantes a homologar su sistema para consumir los servicios web expuestos por el sistema RUNT y establece los criterios mínimos de auditoría que se deben verificar en el proceso de auditoría de seguridad de la información para dar cumplimiento a lo especificado en el numeral 1.1.3 de la parte A de Anexo único de la resolución 792 del 3 de abril de 2013 expedida por el Ministerio de Transporte.

3. AUDIENCIA

Este documento tiene como audiencia los interesados en desarrollar sistemas para interactuar con el sistema RUNT a través de servicios web y las empresas que prestan el servicio de auditoría de seguridad de la información en los términos de la resolución 792 del 3 de abril del 2013.

4. PRUEBAS DE CAJA BLANCA

Para su desarrollo la empresa auditada proveerá al auditor toda la información necesaria para evaluar la seguridad del entorno sometido a prueba incluyendo:

- Código fuente
- Archivos de configuración
- Diagramas y demás documentación.

Esto permitirá una revisión a fondo del sistema, identificando no sólo las vulnerabilidades inmediatas, sino también secciones de código y configuraciones potencialmente peligrosas, puertas traseras, y defectos de construcción. Se debe aplicar una revisión de la seguridad del código entendiéndose éste como el proceso de auditoría sobre el código fuente que verifica que los controles de seguridad en la aplicación están presentes, que funcionan como se pretende, y que han sido invocados en todas las partes necesarias. Se debe realizar de acuerdo con la metodología propuesta por OWASP "Code review guide" en su versión más reciente.

Adicionalmente se debe verificar el cumplimiento de los siguientes requisitos:

	¿Qué se evalúa?	¿Conforme?		Observaciones
		SI	NO	
1	La documentación incluye un análisis de riesgos de seguridad de la información para definir los requisitos de seguridad de la aplicación.			
2	La aplicación implementa controles de mitigación del “top ten de OWASP”			
3	El diseño contempla la mitigación de los requisitos de seguridad encontrado durante el análisis de seguridad.			
4	Garantiza que no se comparten usuarios del sistema.			
5	Las contraseñas no se utilizan en claro, en su lugar se utiliza su valor hash.			
6	Las contraseñas no se almacenan localmente ni sus valores hash.			
7	Cada trámite es firmado por el usuario que lo solicita.			
8	Los certificados digitales utilizados son expedidos por una entidad de certificación autorizada por el organismo nacional de acreditación de Colombia de acuerdo con el decreto 012 de 2012			
9	La versión de los drivers a utilizar por los biométricos corresponde a la más reciente versión solicitada por RUNT para su sistema			
10	La aplicación está diseñada para operar con HTTPS.			
11	En la aplicación se valida la vigencia del certificado del servidor y que pertenece a RUNT garantizando a que servidor se está conectando.			
12	Se tiene una dirección IP fija para acceso al RUNT.			
13	El sistema incluye un proceso de cambio de contraseña para los usuarios y verifica el cumplimiento de las políticas de usuarios y contraseñas definidas por el RUNT.			

14	La aplicación notifica previamente al usuario del vencimiento de la contraseña.			
15	La aplicación implementa un gestor de errores que controla las situaciones de error, genera los logs con información suficiente para determinar la fecha, hora y condición de error presentada sin almacenar información de contraseñas y controla la información que muestra al usuario final.			
16	La aplicación controla los mensajes de error retornados por el servidor del servicio web y entrega la información al usuario orientándolo que debe hacer sin revelar credenciales de acceso o información confidencial.			
17	La aplicación implementa controles de validación de los datos que se entregan al servicio web y de los datos entregados por el servidor.			
18	La aplicación genera registros de auditoría que permiten que cada una de las transacciones se puede reconstruir mediante los datos adecuados de manera que permita:			
	Identificar la fecha. La hora, minutos y segundos sincronizados con hora legal colombiana.			
	Identificar el usuario firmante de la transacción			
	Se pueda relacionar el usuario asignado, la firma, y el servidor desde el que se conecta.			
19	La aplicación valida los parámetros de entrada para controlar: ▪ La longitud de los datos de entrada. ▪ El Tipo de dato. ▪ ataques XPath Injection. ▪ ataques de SQL injection. ▪ caracteres no permitidos.			

5 ELEMENTOS MÍNIMOS ISO 27001

En esta sección se relacionan los controles definidos por la norma ISO 27001 que se deben implementar en el sistema cliente. Dependiendo de la versión de la norma puede estar en un numeral diferente. A continuación, se relacionan los controles de la versión 27001:2022 del anexo A.

5.15 Control de acceso: Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información

5.16 Información de autenticación: La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

5.18 Derechos de acceso: Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.

5.33 Protección de registros: Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados

5.34 Privacidad y protección de la información de identificación personal. La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales

8.4 Acceso al código fuente: El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente

8.5 Autenticación segura: Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.

8.6 Gestión de capacidad. El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.

8.7 Controles contra malware. La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario

8.8 Gestión de vulnerabilidades técnicas: Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas

8.12 Prevención de fugas de datos: Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

8.13 Copia de seguridad de la información: Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos.

8.15 Registro: Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.

8.17 Sincronización de reloj: Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas

8.19 Instalación de software en sistemas operativos. Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos

8.20 Seguridad de redes: Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.

8.24 Uso de la criptografía: Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

8.25 Ciclo de vida de desarrollo seguro: Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.

8.26 Requisitos de seguridad de las aplicaciones: Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.

8.28 Codificación segura: Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.

8.29 Pruebas de seguridad en el desarrollo y aceptación: Los procesos de ensayo de seguridad se deben definir y implementar en el ciclo de vida del desarrollo.

8.30 Desarrollo externalizado: La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

8.31 Separación de entornos de desarrollo, evidencia y producción: Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos

8.32 Gestión del cambio. Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

8.33 Información de las pruebas: La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente

En especial:

- ✓ Se debe describir el manejo de logs de los mensajes SOAP, si aplica.
- ✓ Debe disponer de un sistema de logs parametrizable donde queden almacenados los mensajes generados por la aplicación.
- ✓ Debe guardar registro de las solicitudes por web services indiferente del estado de estas, especificando fecha, hora, servicio, estado, usuario y mensaje respectivo.

Para todo trámite, se debe almacenar en el sistema la evidencia de información, trazabilidad incluyendo la información modificada y la que se incorpora (antes y después de una transacción) Debe tener un módulo de auditoria donde se contemple:

- ✓ Aspectos generales relativos a la seguridad. Se debe contemplar la seguridad operativa de los programas, seguridad en suministros, procesos entre otros.
- ✓ Aspectos relativos a la confidencialidad y seguridad de la información. Estos aspectos se refieren no solo a la protección de la información, sino también al control de acceso a esta.
- ✓ Aspectos jurídicos y económicos relativos a la seguridad de la información. En este grupo de aspectos se trata de analizar el adecuado manejo de la información, en una matriz de riesgos con los costos estimados respectivos.

5.7 Contingencia

Se debe verificar la existencia del proceso de contingencia en caso de falla de la aplicación de servicios web o infraestructura, especificando las opciones de contingencia que aseguran la disponibilidad o recuperación de este.

5.8 Copias de Seguridad

Se debe verificar que exista un procedimiento de recuperación que incluya la realización periódica de copias de seguridad para asegurar el respaldo de la información ante fallos del sistema.

Se debe verificar las políticas y manejo de copias de seguridad.

Periódicamente se debe probar el funcionamiento de las copias de seguridad

5.9 Pruebas y versiones

Cada proveedor deberá disponer de un ambiente de pruebas. Este ambiente será verificado durante la auditoria.

Se debe evidenciar el cumplimiento del protocolo de pruebas establecido para la homologación y actualización de las versiones, especificando el tipo de pruebas a realizar, escenario de pruebas y frecuencia de estas.

Durante la recertificación se debe evidenciar que se ha informado a RUNT cualquier cambio en el software tanto en su funcionalidad como en su licenciamiento.

El proveedor de servicios debe contar con una bitácora de pruebas por versión entregada, con detalle de los mensajes SOAP entrantes y salientes ejecutados.

6. CUMPLIMIENTO DE ESPECIFICACIONES TÉCNICAS DE SERVICIOS WEB.

Esta información se encuentra en el catálogo publicado para cada funcionalidad del web service y demás anexos.

7. FORMATO DE VALIDACIÓN ANEXO AL INFORME DE AUDITORIA

El informe de la auditoria debe incluir la información detallada del resultado de las verificaciones realizadas y el resultado de conformidad.

Criterio evaluado	Conforme?		Observaciones
	SI	NO	

8. ANEXO

1. Políticas de manejo de contraseñas de los usuarios

Para aquellos servicios web en los que el control de autenticación se realice mediante usuario-contraseña, éstos deben ser enrolados previamente ante el RUNT y deben estar en estado activo. Si la contraseña se encuentra vencida el usuario no podrá hacer transacciones en tanto no cambie la contraseña.

Los usuarios y contraseñas utilizados por los servicios web son gestionados por el sistema RUNT. A continuación, se definen las políticas a implementar en el servidor, y debe ser informadas al cliente pues debe tenerlas en cuenta en sus desarrollos e informarlas a sus usuarios.

	Descripción	Definición
1	Prueba de Longitud Mínima de Contraseña	10
2	Prueba de Número Mínimo de Mayúsculas	1
3	Prueba de Número Mínimo de Minúsculas	5
4	Prueba de Numero de Caracteres No Alfanuméricos	0
5	Prueba de Número Mínimo de Caracteres numéricos	2
6	Número de días de Vencimiento de Contraseña	45
7	Días de aviso de Vencimiento de Contraseña	10
8	Aviso por pantalla	Si
10	Cambiar al restablecer la contraseña	SI
11	Historial de Contraseñas	2
12	Número de intentos de conexión fallidos	6
13	Duración de Bloqueo por intentos fallidos	1d
14	Restablecimiento de Intentos de Conexión	1d

8.1 Algoritmos sugeridos

Algoritmos hash

Para el cálculo de valores hash se deben utilizar el algoritmo SHA2. SHA1 se debe utilizar únicamente por razones de compatibilidad. Evite utilizar el algoritmo MD5 pues su seguridad ya ha sido comprometida.

Algoritmos de cifrado

Evite utilizar el algoritmo DES. Prefiera utilizar algoritmos como el AES o el 3-DES. No utilice algoritmos propietarios pues generalmente no han sido sometidos a pruebas de criptoanálisis como los algoritmos públicos y su seguridad puede ser menor.