OBJETIVO: Establecer lineamientos mínimos de seguridad para desarrollo e implementación de api y servicios web.

1. REQUISITOS DE VERIFICACIÓN DE API Y SERVICIO WEB

Objetivo de control

Asegúrese que la aplicación verificada que use API de capa de servicio (comúnmente usando JSON o XML o GraphQL) tenga:

- Autenticación adecuada, gestión de sesiones y autorización de todos los servicios web.
- Validación de entrada de todos los parámetros que transitan de un nivel de confianza más bajo a más alto.
- Controles de seguridad efectivos para todos los tipos de API, incluidas API en la nube y sin servidor

2. REQUISITOS DE VERIFICACIÓN DE SEGURIDAD DEL SERVICIO WEB GENÉRICO

- Verifique que todos los componentes de la aplicación usen las mismas codificaciones y analizadores para evitar ataques de análisis que exploten diferentes comportamientos de análisis de URI o archivos que podrían usarse en ataques SSRF y RFI.
- Verifique que el acceso a las funciones de administración y administración esté limitado a los administradores autorizados.
- Verifique que las URL de API no expongan información confidencial, como la clave de API, los tokens de sesión, etc.
- Verifique que las decisiones de autorización se tomen tanto en la URL, aplicadas por seguridad programática o declarativa en el controlador o enrutador, como a nivel de recursos, aplicadas por permisos basados en modelos.
- Verifique que las solicitudes que contengan tipos de contenido inesperados o faltantes sean rechazadas con encabezados apropiados (estado de respuesta HTTP 406 Inaceptable o 415 Tipo de medio no admitido).

3. REQUISITOS DE VERIFICACIÓN DEL SERVICIO WEB RESTFUL V13.2

Cuando se use la validación de esquema JSON(en borrador), la cual es la mejor práctica para los servicios web SOAP, considere usar estas estrategias de validación de datos adicionales en combinación con la validación de esquema JSON:

- Validación de análisis del objeto JSON, tal como si faltaran elementos o elementos adicionales.

- Validación de los valores del objeto JSON utilizando métodos de validación de entrada estándar, como tipo de datos, formato de datos, longitud, etc.
- Validación formal del esquema JSON.
- Supervise cuidadosamente cualquier biblioteca de validación de esquemas JSON en uso, ya que deberán actualizarse regularmente hasta que se formalice el estándar y se eliminen los errores de las implementaciones.
- Verifique que los métodos RESTful HTTP habilitados sean una opción válida para el usuario o la acción, como evitar que los usuarios normales usen DELETE o PUT en API o recursos protegidos.
- Verifique que la validación del esquema JSON esté completa y verificada antes de aceptar la entrada.
- Verifique que los servicios web RESTful que utilizan cookies estén protegidos contra Cross-Site Request Forgery mediante el uso de al menos uno o más de los siguientes: triple or double submit cookie pattern, CSRF nonces, or ORIGIN request header checks.
- Verifique que los servicios REST tengan controles anti-automatización para proteger contra llamadas excesivas, especialmente si la API no está autenticada.
- Verifique que los servicios REST verifiquen explícitamente el tipo de contenido entrante como el esperado, como application / xml o application / JSON.
- Verifique que los encabezados y la carga útil del mensaje sean confiables y no estén modificados en tránsito. Requerir un cifrado seguro para el transporte (solo TLS) puede ser suficiente en muchos casos, ya que proporciona protección tanto de confidencialidad como de integridad. Las firmas digitales por mensaje pueden proporcionar una garantía adicional además de las protecciones de transporte para aplicaciones de alta seguridad, pero conllevan una complejidad y riesgos adicionales que sopesan los beneficios.

4. REQUISITOS DE VERIFICACIÓN DEL SERVICIO WEB SOAP V13.3

- Verifique que la validación del esquema XSD se realice para garantizar un documento XML correctamente formado, seguido de la validación de cada campo de entrada antes de que tenga lugar el procesamiento de esos datos.
- Verifique que la carga útil del mensaje esté firmada utilizando WS-Security para garantizar un transporte confiable entre el cliente y el servicio.

Nota: Debido a problemas con los ataques XXE contra DTD, no se debe usar la validación de DTD y deshabilitar la evaluación de DTD de marco según los requisitos establecidos en la Configuración V14.

5. GRAPHQL Y OTROS REQUISITOS DE SEGURIDAD DE LA CAPA DE DATOS DEL SERVICIO WEB

- Verifique que se utiliza una lista blanca de consultas, una combinación de limitación de profundidad y limitación de cantidad para prevenir la denegación de servicio (DoS) en expresiones de capa de datos como resultado de consultas grandes y anidadas.

- Verifique que se implemente GraphQL u otra lógica de autorización de la capa de datos en la capa de lógica de negocios.

6. GESTIÓN DE ERRORES

Se debe evitar mostrar información de herramientas de software y sus versiones a usuarios finales, cuando al presentarse un error en alguna aplicación web.

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE (S)	SANDRA CEDIEL BRAVO	SANDRA CEDIEL BRAVO	MARIA MARGARITA GONZÁLEZ
CARGO (S)	Especialista	Especialista	Gerencia de Riesgos

CONTROL DE CAMBIOS	
VERSIÓN	**CAMBIO REALIZADO**
1	Creación del Documento
2	Migración al proceso SSI