Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Codificación Segura

14
CAPÍTULO

Estándar de TI: Codificación Segura

1.0 Propósito y Beneficios

Las organizaciones gubernamentales sufren constantes ciberataques que intentan explotar las vulnerabilidades de los sistemas informáticos y, por tanto, amenazan la confidencialidad, la integridad y la disponibilidad de la información. Una gran cantidad de vulnerabilidades que se explotan con éxito se deben a debilidades en la codificación del software y fallas en la implementación de la codificación.

El objetivo de este estándar de codificación es garantizar que el código escrito sea resistente a amenazas de alto riesgo y evitar la aparición de los errores de codificación más comunes que crean vulnerabilidades graves en el software. Si bien es imposible escribir código que sea completamente inmune a todos los posibles ataques, la implementación de estos estándares de codificación en todos los sistemas de información reducirá significativamente el riesgo de divulgación, alteración o destrucción de información debido a vulnerabilidades del software.

2.0 Declaración de información

Según la Política de seguridad de la información, todo el software escrito o implementado en sistemas debe incorporar prácticas de codificación segura, para evitar la aparición de vulnerabilidades de codificación comunes y ser resistente a amenazas de alto riesgo, antes de implementarse en producción.

Los elementos enumerados en este estándar no son una lista exhaustiva de ataques de alto riesgo y errores de codificación comunes, sino más bien una lista de los más dañinos y generalizados. Por lo tanto, el código escrito debe contener controles de mitigación no solo para los elementos específicamente articulados en el estándar a continuación, sino también para cualquier amenaza de riesgo medio y alto que se identifique durante el ciclo de vida de un sistema.

Las amenazas de alto riesgo incluyen, entre otras:

1. Inyección de código;
2. Secuencias de comandos entre sitios (XSS);
3. Falsificación de solicitudes entre sitios (CSRF);
4. Fuga de información y manejo inadecuado de errores;
5. Autenticación faltante para función crítica;

6. Falta de cifrado de datos confidenciales;
7. Redirección de URL a un sitio que no es de confianza (“Redirección abierta”).

Como mínimo, el código debe eliminar o mitigar las amenazas identificadas en la versión actual del *Open Web Application Security Project (OWASP) Los 10 riesgos de seguridad de aplicaciones más críticos (‘OWASP Top 10’) y la Enumeración de debilidades comunes (CWE)/SANS Los 25 errores de software más peligrosos (“CWE/SANS Top 25”).*

Tanto OWASP como CWE/SANS reeditan periódicamente sus respectivas listas en función de cambios en los patrones de vulnerabilidad y explotación. Los desarrolladores deben estar al tanto de las actualizaciones de estas listas e incorporar nuevas recomendaciones.

Se requiere el uso de bibliotecas de control de seguridad y API comunes, que hayan sido sometidas a pruebas de seguridad, para garantizar un enfoque coherente que minimice los defectos y evite la explotación. Cuando estén disponibles, se deben utilizar bibliotecas o API disponibles públicamente o proporcionadas por proveedores, a menos que haya un caso de negocio desarrollado y una excepción otorgada por el Oficial de Seguridad de la Información (ISO)/representante de seguridad designado para desarrollar una biblioteca personalizada.

Para prevenir defectos o detectarlos y eliminarlos tempranamente, logrando así beneficios significativos en costos y cronograma para la Repartición, se debe verificar el código en busca de errores durante el desarrollo y mantenimiento.

Las entidades deben verificar que el modelo de garantía de software utilizado por el proveedor esté en línea con este estándar a través de garantías del proveedor, pruebas de seguridad y/o requisitos contractuales.

3.0 Cumplimiento

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
29-07-24	Documento inicial, primera revisión.	Alejandro Castro, Pablo Zalazar

5.0 Documentos relacionados

Open Web Application Security Project (OWASP) Los 10 riesgos de seguridad de aplicaciones más críticos (‘OWASP Top 10’)

Hojas de trucos para desarrolladores del Proyecto abierto de seguridad de aplicaciones web (OWASP)

API de seguridad empresarial del Proyecto abierto de seguridad de aplicaciones web (OWASP)

Enumeración de debilidades comunes (CWE)/SANS Top 25 de los errores de software más peligrosos ‘CWE/SANS Top 25’)

Lista de enumeración de debilidades comunes (CWE)

Estándares de codificación segura CERT del Instituto de Ingeniería de Software Carnegie Mellon