ESCUELA
POLITÉCNICA
NACIONAL

Política de principios de la ingeniería de sistemas seguros

Código	Política de principios de la ingeniería de sistemas seguros
Versión:	1.0.0
Fecha de la versión:	23-02-2023
Creado por:	Grupo
Aprobado por:	Líder
Nivel de confidencialidad:	Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
23/02/2023	1.0.0	Grupo	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

Establecer procesos y procedimientos seguros en la ingeniería de sistemas para garantizar la seguridad de los sistemas de la organización. Esta política tiene como objetivo principal proteger los sistemas de la organización contra posibles amenazas de seguridad, como la inyección de código malicioso, la exposición de datos sensibles y el acceso no autorizado a los sistemas.

2. Política de principios de la ingeniería de sistemas seguros

Se deberá incluir los siguientes aspectos para garantizar la seguridad de los sistemas:

1. Procedimientos seguros para el diseño y codificación: Se deberán establecer procedimientos seguros para el diseño y la codificación de los sistemas para garantizar la seguridad del software. Esto incluye la adopción de estándares de programación segura, la identificación y corrección de vulnerabilidades de seguridad y la implementación de pruebas de seguridad.
2. Procesos de diseño de mecanismos de autenticación: Se deberán implementar mecanismos de autenticación seguros para proteger los sistemas contra el acceso no autorizado. Estos mecanismos deberán ser difíciles de vulnerar y deberán incluir medidas de seguridad, como contraseñas fuertes y autenticación de dos factores.
3. Procesos de somatización de variables: Se deberán establecer procesos de somatización de variables para evitar la exposición de datos sensibles y prevenir la inyección de código malicioso en los sistemas. Esto incluye la validación de entradas de datos y la utilización de mecanismos de protección contra la inyección de código malicioso.
4. Procedimientos para el uso correcto de la criptografía: Se deberán establecer procedimientos para el uso correcto de la criptografía, lo que incluye la selección de algoritmos seguros, la implementación de medidas de protección de claves y el uso de técnicas de encriptación adecuadas.

Además, se sugiere la adopción de estándares para la programación segura, como el CWE (Common Weakness Enumeration) y el OWASP (Open Web Application Security Project), para garantizar que los sistemas cumplan con las mejores prácticas de seguridad y se eviten vulnerabilidades conocidas.

La adopción de esta política permitirá a la organización garantizar la seguridad de sus sistemas mediante la implementación de procesos y procedimientos seguros en la ingeniería de sistemas. Esto reducirá los riesgos de seguridad asociados con los sistemas y mejorará la capacidad de la organización para detectar y mitigar amenazas de seguridad.

3. Validez y gestión de documentos

Este documento es válido hasta el año 2026.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de obligaciones de la organización que ya existían pero que no fueron identificadas.
- Cantidad o monto de multas pagadas por el no cumplimiento de obligaciones.
- Cantidad de días de atraso en el cumplimiento de la obligación.

Líder
[firma]