ESCUELA
POLITÉCNICA
NACIONAL

Política de Análisis y Especificación de los Requisitos de Seguridad

Código	Política de Análisis y Especificación de los Requisitos de Seguridad
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

El objetivo de esta política es garantizar que los requisitos de seguridad para las aplicaciones y sistemas sean adecuadamente analizados y especificados, de manera que se asegure la protección de los activos involucrados y se cumpla con las normativas y estándares de seguridad establecidos.

2. Política de Análisis y Especificación de los Requisitos de Seguridad

Se debe tomar en cuenta los siguientes procedimientos durante el análisis y especificación de requisitos de seguridad.

1. Determinar el nivel de confianza que requiere la aplicación. Este análisis permitirá definir los requisitos de autenticación necesarios para proteger la información.
2. Especificar las formas de provisión de accesos para los diferentes tipos de usuarios: Usuarios, Usuarios privilegiados y técnicos de mantenimiento.
3. Analizar las funciones y responsabilidades de los usuarios y definir los requisitos de seguridad que deben cumplir.
4. Realizar un análisis de riesgos para identificar las necesidades de protección de los activos involucrados y definir los requisitos de seguridad necesarios para prevenir y mitigar los posibles riesgos.
5. Identificar los requisitos de seguridad que se derivan de los procesos del negocio y definir las medidas necesarias para garantizar la protección de la información.
6. Definir los requisitos para la gestión de registros de transacciones, supervisión y monitoreo, así como para garantizar la no-repudiación de las transacciones realizadas.
7. Especificar los controles de seguridad necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información, incluyendo interfaces para el registro y supervisión de actividades y sistemas de detección de fugas de datos.
8. Sugerir el uso de herramientas para el modelado de amenazas, como Microsoft Threat Modeling Tool, para identificar y mitigar los posibles riesgos de seguridad.

En el Anexo 1 se encuentra una carpeta con un ejemplo de uso del modelado STRIDE y la herramienta Microsoft Threat Modeling Tool, como una guía para su uso.

La implementación de esta política permitirá garantizar que los requisitos de seguridad de las aplicaciones y sistemas sean adecuadamente analizados y especificados, lo que contribuirá a la protección de los activos involucrados, la prevención de riesgos y el cumplimiento de las normativas y estándares de seguridad establecidos.

3. Anexos

Carpeta con documentos guía: STRIDE

4. 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]