



Política de desarrollo seguro

Certicámara dentro de su marco de gobierno tiene por premisa el reconocimiento a la información como activo fundamental, por tal razón propende por ofrecer mecanismos para que esta sea asegurable como parte integral de los sistemas de información durante todo su ciclo de vida.

Para tal fin, Certicámara:

- Suministra un ambiente de desarrollo de software de uso exclusivo de los responsables de realizar esta actividad, asegurando este ambiente bajo el cumplimiento de estándares reconocidos internacionalmente.
- Exige el cumplimiento de metodologías de desarrollo seguro como por ejemplo OWASP.
- Incluye requisitos de seguridad para los nuevos sistemas de información o para realizar mejoras a los existentes.
- Monitorea el cumplimiento de los requisitos de seguridad en los diferentes hitos del proyecto.
- Mantiene registro de versiones sobre los códigos fuente.
- Implementa planes de capacitación y formación para el personal responsable del proceso de desarrollo de sistemas de información, de manera que tengan las habilidades para evitar, identificar y mitigar las vulnerabilidades que se puedan presentar en los sistemas de información desarrollados.

Objetivos de la política de desarrollo seguro:

- Establecer mecanismos de control y protección para garantizar las condiciones de seguridad en el proceso de desarrollo, este control se mide tanto para los desarrollos internos como externos.
- Cumplir con los requisitos legales y regulatorios aplicables a Certicámara en materia de desarrollo seguro de aplicaciones.



Política de desarrollo seguro

RESPONSABLES:

- La **Gerencia Soluciones de Negocio** es la responsable de:
 - Cumplir las directrices mencionadas en este documento, implementando los mecanismos necesarios para la operación adecuada del proceso de desarrollo seguro.
 - Definir y formalizar los procedimientos para la implementación del proceso de control de cambios.
 - Realizar revisiones técnicas a las aplicaciones después de la implementación de cambios en la infraestructura.
- La **Gerencia de Gobierno Riesgo y Cumplimiento** es responsable de monitorear el cumplimiento de los controles definidos para la ejecución del proceso de desarrollo seguro.

Los colaboradores responsables del cumplimiento de esta política deben asegurar la implementación de los controles establecidos para la adquisición, desarrollo y mantenimiento de los sistemas de información que soportan la operación de Certicámara de manera integral durante todo el ciclo de vida del software.