

Política de Desarrollo Seguro

El propósito de esta política es asegurar que todos los desarrollos de sistemas y aplicaciones que realiza ACL Tecnología se realizan bajo estrictas medidas de seguridad, protegiendo los sistemas y datos frente a accesos no autorizados, y adoptando las mejores prácticas de desarrollo seguro para garantizar la seguridad, integridad y confidencialidad de la información.

Esta política es aplicable a todo el personal involucrado en el desarrollo, prueba, implementación y mantenimiento de sistemas de información en ACL Tecnología, incluyendo desarrolladores internos y en cliente, así como a los sistemas y entornos utilizados en estos procesos.

Los objetivos principales de esta política son:

- Implementar controles efectivos para proteger los entornos de desarrollo, pruebas y producción contra accesos no autorizados, garantizando que solo el personal autorizado tenga acceso a cada uno de estos entornos.
- Mantener entornos de desarrollo, pruebas y producción separados tanto a nivel físico como lógico, asegurando que cada uno cuente con plataformas, servidores, aplicaciones y versiones independientes, minimizando así el riesgo de que las actividades de desarrollo y pruebas comprometan los datos de producción.
- Asegurar que los desarrolladores apliquen técnicas de codificación y diseño seguros, mitigando posibles vulnerabilidades desde la fase de desarrollo.
- Implementar un control riguroso sobre las versiones del software, utilizando repositorios con acceso controlado y limitando el acceso a los datos y archivos en ambientes de producción.

Política de **Desarrollo Seguro**

Aseguramos la segregación entre los entornos de desarrollo, pruebas y producción, promoviendo el uso de credenciales diferenciadas por entorno para reducir riesgos operativos y de seguridad. Se establecen procedimientos estrictos para el acceso a ambientes de producción, garantizando que los desarrolladores, tanto internos como en cliente, cuenten únicamente con permisos limitados y controlados. Asimismo, los repositorios se mantienen con acceso restringido y con registro completo de todas las interacciones, asegurando trazabilidad y cumplimiento de los controles establecidos.

El Área de Desarrollo es responsable de versionar todos los desarrollos en las herramientas designadas, garantizando un control efectivo de versiones. Además, se capacita al personal en diseño y codificación segura, tanto al momento de su incorporación como de forma periódica (al menos una vez al año).

Asimismo, implementamos mecanismos de autenticación robustos en todos los sistemas de información, con el fin de minimizar el riesgo de accesos no autorizados. Del mismo modo, es necesario asegurar que las contraseñas no se visualicen en pantalla y que las funciones de “recordar contraseña” permanezcan deshabilitadas.

Los procedimientos para la reasignación de contraseñas deben ser seguros, utilizando enlaces temporales o claves enviadas a correos previamente registrados, con plazos de validez claramente definidos.

Jorge Portus Ortega

Gerente General
ACL Tecnología SPA
Enero 2025