El desarrollo de las aplicaciones, así como la implementación de los controles de seguridad necesarios, debe realizarse siguiendo principios de seguridad que reduzcan la probabilidad de materialización de amenazas y, en caso de producirse, mitiguen su impacto.

Los requisitos considerados son los siguientes:

- Seguridad por defecto. Toda aplicación desplegada en su entorno de producción debe configurarse de forma segura por defecto. Las opciones predeterminadas deberán incluir políticas de contraseñas robustas, caducidad periódica de credenciales, restricciones de acceso a entornos sensibles y desactivación de funcionalidades innecesarias.
- Ejecución con los mínimos privilegios. El principio de mínimos privilegios establece que las cuentas, servicios y procesos deberán operar únicamente con los permisos estrictamente necesarios para cumplir su función. Este nivel de privilegios abarca tanto permisos de usuarios como permisos sobre recursos como CPU, memoria, red, sistema de ficheros, etc.
- Defensa en profundidad. Las aplicaciones deberán incorporar medidas de seguridad en todas las capas del sistema (base de datos, servidor, red y aplicación).
  Se deben aplicar controles combinados —como validaciones de entrada, control de errores y medidas anti inyección SQL— para evitar que la vulnerabilidad de un único punto comprometa el sistema completo.
- Ciclo de vida seguro del desarrollo. En general, el desarrollo deberá realizarse en entornos diferenciados de desarrollo, pruebas y producción, asegurando que solo personal autorizado tiene acceso a cada uno de ellos. Antes del paso a producción, todo sistema o aplicación deberá ser sometido a revisiones técnicas y de seguridad, verificando la aplicación de parches, la configuración segura y la ausencia de vulnerabilidades conocidas. Los procedimientos y cambios deben documentarse para garantizar trazabilidad y facilitar auditorías posteriores.
  Cuando la naturaleza o el alcance del proyecto no requieran la implantación completa de estos entornos, se podrá aplicar un modelo de desarrollo proporcional, siempre que se mantengan los controles de seguridad mínimos y se justifique adecuadamente dicha decisión.
- Detección y gestión de incidentes de seguridad. Toda la información de seguridad relevante deberá registrarse en los logs de la aplicación y sistemas asociados.
  Se deberán establecer procedimientos para monitorizar dichos registros de manera periódica y responder adecuadamente ante la detección de incidentes o intrusiones.
- Evitar la seguridad por ocultación. La seguridad no debe depender de mantener en secreto el código fuente, la estructura interna o la configuración de la aplicación.
  El diseño seguro debe basarse en mecanismos probados y controles técnicos eficaces, no en la ocultación.
- Gestión y corrección de vulnerabilidades. Cuando se detecte una vulnerabilidad o problema de seguridad, se desarrollarán pruebas para reproducirlo y determinar su causa raíz. Las soluciones aplicadas deberán verificarse antes del despliegue, garantizando que no se introducen errores de regresión ni nuevas vulnerabilidades.

En Las Rozas de Madrid, 7 de noviembre de 2025

Juan Martitegui González
Administrador Único de Quasar Science Resources, S.L.