D I G I T A L I Z A C I O N

PRUEBA ABIERTA 1UD6

A L U M N O C E S U R 2 4 / 2 5

Alejandro Muñoz de la Sierra

PROFESOR

Raúl Moreno Luque

0 1
I N T R O D U C C I Ó N

Nos encontramos en una era donde la digitalización ha reconfigurado no solo nuestras dinámicas laborales, sino también los desafíos que surgen en el proceso. Para los que nos desenvolvemos en el ámbito del desarrollo de software multiplataforma, esto implica un panorama crecientemente interconectado, donde cada aspecto —desde la seguridad hasta la gestión de la información— demanda una vigilancia continua. Las organizaciones ya no pueden permitirse mantener sistemas aislados o improvisar soluciones ad hoc, dado que cualquier error podría resultar en una seria pérdida de datos o un incidente de seguridad de gran impacto.

Este estudio de caso examinará cómo una empresa especializada en desarrollo de software puede abordar estos retos de manera pragmática y eficiente. Inicialmente, detectaremos algunas vulnerabilidades en áreas fundamentales como la producción, los recursos humanos, el marketing, las finanzas y los sistemas en la nube. Posteriormente, analizaremos cómo la organización administra sus datos: desde la recopilación hasta la protección y su utilización en la toma de decisiones. Finalmente, discutiremos cómo una arquitectura tecnológica bien integrada —mediante APIs, middleware y automatización— puede permitir que todos los componentes del sistema operen conjuntamente sin dificultades. Trataremos todo esto desde una óptica práctica, considerando las mejores prácticas de la industria y enfocándonos en soluciones que puedan ser implementadas en escenarios reales.

02

VULNERABILIDADES DE SEGURIDAD SEGÚN EL ÁREA OPERATIVA

En el contexto de una empresa de desarrollo de software que se embarca en la digitalización, en particular al operar en entornos cloud, la exposición a riesgos se incrementa notablemente. De hecho, en 2023, se estimó que más del 80% de las incidencias de seguridad estuvieron relacionadas con datos alojados en servicios cloud (safetica.com). Por lo tanto, resulta esencial anticipar los riesgos característicos de cada departamento e implementar medidas que los mitiguen desde el principio.

Producción de software.
Un aspecto fundamental es la protección del código fuente y del ciclo CI/CD. Si un repositorio Git no cuenta con la protección correcta, un atacante podría desde sustraer claves hasta insertar código malicioso. En este sentido, es crucial aplicar control de acceso basado en roles (RBAC), autenticación multifactor (MFA), y herramientas SAST/DAST para el análisis de seguridad del código, así como el escaneo de librerías con soluciones como Snyk o SonarQube. Igualmente, los datos confidenciales, como credenciales o tokens, deben ser cifrados, tanto en tránsito como en reposo, y se deben mantener entornos de desarrollo y pruebas aislados del entorno de producción. Además, la actualización constante de librerías y frameworks es esencial para reducir vulnerabilidades conocidas.

Recursos Humanos.
Esta área maneja información sensible, incluyendo nóminas, datos personales e incluso historiales médicos. El riesgo aquí se centra en filtraciones o accesos no autorizados. Por ello, es importante aplicar el principio de mínimo privilegio en la gestión de accesos, cifrar la información en las bases de datos y en las copias de seguridad, y garantizar que exista un protocolo riguroso para el alta y baja de personal. La formación en protección de datos, así como la identificación de correos de phishing, es un pilar fundamental para el equipo de RR. HH.

Marketing.

Al gestionar datos de clientes, leads y redes sociales, el departamento de marketing se convierte en un objetivo atractivo. Las brechas pueden originarse en formularios web inseguros o en el uso inapropiado de APIs de terceros. Se sugiere emplear autenticación robusta para todas las herramientas de marketing, validar las entradas de datos para prevenir ataques como XSS o SQL Injection, cifrar toda la información en tránsito (por ejemplo, utilizando HTTPS), y revisar meticulosamente los permisos de acceso a plataformas como Google Ads o Meta. Además, el cumplimiento de la normativa GDPR es un estándar indispensable.

Área financiera.

El área financiera maneja datos especialmente sensibles: cuentas bancarias, tarjetas, facturación, entre otros. Un ataque en esta área, como un caso de phishing dirigido al CFO o un ataque de ransomware, puede tener un impacto directo en la viabilidad del negocio. Se recomienda segmentar la red, utilizar autenticación multifactor para el acceso a la banca online, cifrar las bases de datos (con AES, por ejemplo) y mantener copias de seguridad cifradas fuera de línea. Además, el cumplimiento de estándares como PCI-DSS ayuda a mitigar riesgos legales y reputacionales.

Infraestructura cloud y APIs.

Los entornos en la nube y las APIs representan una fuente recurrente de problemas si no se gestionan de forma correcta. Un bucket S3 mal configurado o un endpoint sin control de acceso puede facilitar la exfiltración de datos. Para proteger estos entornos, se deben aplicar medidas como autenticación robusta, políticas de limitación de peticiones (rate-limiting), cifrado completo (en tránsito y en reposo), y el uso de herramientas como DLP o CASB. Las buenas prácticas de seguridad de OWASP y la supervisión de logs mediante IDS/IPS son fundamentales para mitigar intentos de intrusión.

02

EL MANEJO DE LOS DATOS EN LA EMPRESA

La digitalización no se limita a trabajar en la nube o a la automatización de procesos; también implica la correcta captura, almacenamiento y uso de los datos. En una empresa tecnológica, la información proviene de diversas fuentes, incluyendo formularios. Pensemos en web, apps móviles, sistemas CRM/ERP, esos registros del servidor, las métricas de rendimiento… Todos estos datos residen en diversos sistemas: bases de datos relacionales (SQL), documentos NoSQL, repositorios Git, el almacenamiento en la nube (como AWS o Azure), entre otros. Para protegerlos, usamos cifrado TLS/SSL en las comunicaciones y cifrado en reposo para backups y bases de datos. Las credenciales y tokens también se guardan con cuidado, y controlamos el acceso mediante políticas estrictas.

Además, las copias de seguridad, periódicas y cifradas, se guardan fuera del entorno normal, listas para la restauración rápida en caso de desastre. Esta infraestructura no solo mantiene los datos seguros, sino que también permite analizarlos con herramientas de Business Intelligence (Power BI, Tableau, Grafana o Kibana) para obtener dashboards y análisis estratégicos. Se monitorizan KPIs técnicos (tiempo de respuesta, fallos por minuto) y de negocio (conversión, ROI), y se emplean lenguajes como SQL o Python, incluso machine learning, para generar predicciones y mejoras constantes.

Uno de los desafíos principales en la transformación digital es evitar que la información quede aislada en departamentos: ventas, producción, soporte técnico... Una empresa moderna necesita coordinación, y la integración es vital para lograrlo.

Diseño de APIs.
Cada servicio interno (facturación, login, analítica, etc.) debería ofrecer una API REST o GraphQL bien documentada, con autenticación (OAuth2, JWT) y control de versiones. Esto permite que las apps, como la web o las herramientas de BI, se comuniquen de forma segura.

Conexión entre sistemas empresariales.
ERP, CRM y BPM deben estar sincronizados. Un cambio en inventario se refleja en contabilidad o atención al cliente gracias a conectores, middleware o estándares de integración como SOA.

Middleware y buses de servicios.
Plataformas como Kafka o RabbitMQ permiten que eventos (alta de usuario) se propaguen a sistemas, sin comunicación directa. Esta capa de mensajería asegura el flujo de información y permite escalar.

Formatos y protocolos estándar.
Para la integración, usamos formatos como JSON, XML o CSV, y protocolos como REST, SOAP o Webhooks. También se valora gRPC o APIs para móviles o IoT.

Automatización de procesos.
Flujos automatizados permiten coordinar tareas: la aprobación de un presupuesto genera una orden de compra, notifica a finanzas y actualiza el stock. Herramientas de RPA, ETL o BPM (como Bonita o Camunda) se usan para coordinar procesos.

En resumen, una empresa líder en lo digital debe ir más allá de "usar la nube". La seguridad, la integración y el uso estratégico de los datos son clave para transformar procesos, aumentar la competitividad y mejorar la toma de decisiones. Adoptar esta mentalidad y construir una arquitectura técnica coherente y segura es fundamental, casi una necesidad.

0 3
C O N C L U S I O N E S

Aunque la transformación digital ha traído grandes avances y oportunidades para muchas empresas, también nos ha hecho ver lo fácil que es caer en errores si no se hace con cabeza. Durante este caso práctico nos hemos dado cuenta de que cada departamento —producción, marketing, finanzas...— tiene sus propios puntos débiles. Y no basta con tener buenos sistemas: hacen falta medidas claras como el cifrado de la información, una buena gestión de accesos o la segmentación de redes. Además, hay algo que muchas veces se olvida: las personas. No todo depende de la tecnología. Si no se forman bien los equipos o no hay supervisión, pueden aparecer problemas serios sin que nadie se dé cuenta a tiempo.

Otro punto que nos ha parecido clave es cómo se gestionan los datos. No solo se trata de almacenarlos de forma segura, sino de saber usarlos bien. Si los datos están bien protegidos y se analizan con sentido, pueden convertirse en una herramienta muy poderosa para tomar decisiones y ganar ventaja frente a la competencia. Para que eso funcione, es importante que todas las herramientas y plataformas estén bien conectadas, y aquí entran en juego las APIs, los flujos automatizados y soluciones de integración como el middleware. Gracias a eso se evita que la información se quede “encerrada” en un solo lugar, y todo el sistema funciona de forma más coordinada y clara.

En resumen, una empresa de desarrollo de software que quiera crecer de verdad en el entorno digital no puede limitarse a comprar tecnología nueva. Tiene que pensar en seguridad desde el principio, en cómo se organizan los datos y en cómo se comunican todas sus partes. Solo así se puede construir algo que no solo sea moderno, sino también seguro, útil y sostenible en el tiempo.

R E F E R E N C I A S

https://www.safetica.com/es/recursos/blogs/seguridad-de-datos-en-la-nube-definiciones-riesgos-y-7-mejores-practicas-para-la-proteccion-de-datos-en-la-nube#:~:text=Seg%C3%BAn%20el%20informe%20sobre%20el,se%20asimile%20por%20un%20momento

https://ibernova.com/blog/trucos-para-romper-los-silos-organizacionales-con-el-sistema-de-gestion-de-la-informacion/#:~:text=Consideramos%20que%20la%20estrategia%20de,gesti%C3%B3n%20de%20la%20informaci%C3%B3n%20necesarios

https://spyrosoftware.com/api-como-establecen-comunicaciones-eficientes-entre-el-erp-y-otros-sistemas/#:~:text=Casi%20todas%20las%20empresas%20que,del%20sistema%20con%20otras%20aplicaciones

https://www.incibe.es/empresas/blog/medidas-para-proteger-la-informacion-defiende-el-principal-activo-de-tu-empresa#:~:text=Limitar%20el%20acceso%20a%20la,deben%20seguir%20los%20siguientes%20pasos

https://www.incibe.es/empresas/blog/cifrado-de-la-informacion-protege-el-principal-activo-de-tu-empresa#:~:text=Otro%20elemento%20delicado%20son%20los,consecuencias%20perjudiciales%20para%20la%20empresa

https://www.akamai.com/es/glossary/what-are-api-security-risks#:~:text=Las%20API%20procesan%20informaci%C3%B3n%20confidencial%2C,expuestos%20a%20terceros%20no%20autorizadas

https://www.eude.es/blog/5-herramientas-de-analisis-de-datos-y-business-intelligence/#:~:text=El%C2%A0Business%20Intelligence%C2%A0,internos%20y%20mejorar%20los%20resultados