| | |
|---|---|
| ENTIDAD: | PROGRAMA NACIONAL DE COMPETITIVIDAD |
| DIRECCIÓN: | 13 Calle 3-40 zona 10, Edificio Atlantis, nivel 3, Oficina 302. |
| HORARIO DE ATENCIÓN: | 8:00 a 16:00 horas |
| TELÉFONO: | 2421-2464 |
| DIRECTORA EJECUTIVA | Vivian Marycruz Villegas Rivas |
| ENCARGADO DE ACTUALIZACIÓN: | Hilda Lucrecia Martínez Duarte |
| FECHA DE ACTUALIZACIÓN: | 03 de septiembre 2025 |
| CORRESPONDE AL MES DE: | agosto de 2025 |

## Decreto 36-2024 Artículo No.22 Publicación de informes en portales web

| No. | No. Contrato | Nombre del Asesor | Nombre de la Consultoría | Número del Producto / Informe Presentado | Monto pagado en el mes | Renglón | Fuente de Financiamiento |
|---|---|---|---|---|---|---|---|
| 1 | PNC-108-001-189-2025 | Pablo Eduardo Urías Johnson | Servicios Profesionales | Tercer Producto | Q28,100.00 | 189 | 11 |
| | | | | | | | |
| | | | | | | | |

Hilda Lucrecia Martínez Duarte
Jefe de Compras y Contrataciones
Programa Nacional de Competitividad
MINISTERIO DE ECONOMÍA

CERTIFICACIÓN DE RECEPCIÓN DE PRODUCTO

Por este medio hago CONSTAR que he recibido y leído el producto abajo indicado de los servicios prestados dentro de la contratación titulada:

**Servicios profesionales en materia de formulación de proyectos de simplificación y digitalización para el Programa Nacional de Competitividad**

Que realizó: **Pablo Eduardo Urías Johnson**

Como parte de los servicios profesionales prestados al Programa Nacional de Competitividad, el cual recibo a entera conformidad porque cumplen con los términos de referencia del contrato número: **PNC-108-001-189-2025.**

Por lo que se solicita trasladar a donde corresponda para continuar con el proceso respectivo de pago, por la cantidad de: Q. 28,100.00

Se adjunta:

Producto Número Tres: **Análisis de Soluciones Tecnológicas para Digitalización.**

Documento que contiene:

1. Resumen ejecutivo.
2. Índice.
3. Introducción.
4. Objetivos.
5. Tabla de Análisis Comparativo de Potenciales Soluciones Tecnológicas Evaluadas Para La Digitalización, que incluye variables como: costo, personal requerido, tiempo de implementación, beneficios y riesgos.
6. Recomendaciones.

Impreso en: 22 páginas.

Medio electrónico: Sí (CD)

Fecha de entrega del producto: 14 de agosto de 2025.

Aprobación del producto:

Firma y sello: _____

Licda. Vivian Marycruz Villegas Rivas
Directora Ejecutiva
Programa Nacional de Competitividad
MINISTERIO DE ECONOMÍA

PROGRAMA NACIONAL DE COMPETITIVIDAD

MINISTERIO DE ECONOMÍA

Para: Vivian Marycruz Villegas Rivas

Directora Ejecutiva

Programa Nacional de Competitividad

De: Pablo Eduardo Urias Johnson

Asesoría: Servicios profesionales en materia de formulación de proyectos de simplificación y digitalización para el Programa Nacional de Competitividad

Asunto: Producto tres: Análisis de Soluciones Tecnológicas Para Digita ización

Fecha: 14 de agosto de 2025.

(f) _____

CONSULTOR

MINISTERIO DE ECONOMÍA

VICEMINISTERIO DE INVERSIÓN Y COMPETENCIA

PROGRAMA NACIONAL DE COMPETITIVIDAD

# PRODUCTO TRES

## ANÁLISIS DE SOLUCIONES TECNOLÓGICAS PARA DIGITALIZACIÓN

CONTRATO PNC-108-001-189-2025

PABLO EDUARDO URIAS JOHNSON

DPI: 1595877940101

NIT: 3562724-7

COLEGIADO No. 19,500

COLEGIO DE ECONOMISTAS, CONTADORES PÚBLICOS Y AUDITORES Y ADMINISTRADORES DE EMPRESAS

GUATEMALA 14 DE AGOSTO DE 2025

## RESUMEN EJECUTIVO

La transformación digital del Estado guatemalteco es un pilar fundamental para mejorar la eficiencia gubernamental, promover la transparencia, y garantizar un acceso equitativo a los servicios públicos. En este contexto, el presente documento analiza las soluciones tecnológicas existentes, viables y recomendadas, a fin de apoyar la digitalización de procesos y trámites administrativos.

Este análisis responde a las recomendaciones planteadas en la Guía de Gobierno Digital y en los estudios del Diagnóstico de Preparación Digital (DRA), que identifican oportunidades clave en interoperabilidad, infraestructura, gestión documental, servicios digitales, participación ciudadana y protección de datos.

Soluciones Tecnológicas Claves Identificadas:

Plataformas de Interoperabilidad: la implementación de una plataforma de interoperabilidad nacional permite el intercambio seguro y eficiente de información entre instituciones. El modelo propuesto se inspira en el caso de éxito de Estonia y el del Marco de Interoperabilidad para Guatemala (MIG). Requiere una arquitectura basada en estándares abiertos, servicios web y sistemas de autenticación federada.

Gestión Documental Electrónica (GDE): se identifican herramientas como Alfresco, OpenKM y soluciones basadas en SharePoint, que permiten la automatización de expedientes electrónicos y flujos documentales, asegurando trazabilidad, integridad y acceso remoto.

Portales de Servicios Digitales: la creación de un portal unificado (modelo "ventanilla única") facilita la interacción ciudadana con el Estado. Se recomienda una solución modular basada en Drupal o Liferay, con integración a sistemas de pagos y notificaciones electrónicas, siguiendo las recomendaciones de la Guía de Servicios Digitales de la GAE.

Sistemas de Identidad Digital y Autenticación: se propone adoptar soluciones de firma electrónica avanzada e identidad digital interoperable, con base en certificados

Sistemas de Identidad Digital y Autenticación: se propone adoptar soluciones de firma electrónica avanzada e identidad digital interoperable, con base en certificados digitales y biometría, tal como lo establece el Decreto 47-2008 (Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas).

Plataformas de Datos Abiertos y Análisis de Datos: el uso de plataformas como CKAN para la publicación de datos abiertos permite mejorar la transparencia y fomentar la reutilización de la información pública. Se deben enlazar con herramientas de análisis y visualización como Power BI o Tableau.

Herramientas de Participación Electrónica: a través de encuestas, foros y presupuestos participativos digitales, se promueve la participación ciudadana. Se recomienda el uso de plataformas como CONSUL (usada por ciudades como Madrid) y otras soluciones de código abierto adaptadas al contexto local.

Consideraciones para la Implementación:

Infraestructura tecnológica: Es fundamental invertir en centros de datos, conectividad, y servicios en la nube (IaaS, PaaS, SaaS) conforme a los lineamientos del Manual de Nube del gobierno.

Normativa: Debe actualizarse el marco legal para proteger los datos personales, regular la interoperabilidad y garantizar la validez legal de trámites digitales.

Gobernanza tecnológica: Es necesaria una entidad rectora con capacidad de coordinación transversal, como fue propuesto en el Producto 2.

Capacitación y cambio cultural: El capital humano debe ser capacitado en competencias digitales y gestión del cambio.

Sostenibilidad y escalabilidad: Las soluciones seleccionadas deben ser escalables, seguras y sostenibles financieramente.

INDICE

# INTRODUCCIÓN

La transformación digital del Estado constituye un eje transversal para el fortalecimiento institucional, la eficiencia administrativa y la mejora en la prestación de servicios públicos. En este contexto, el presente documento desarrolla el Producto 3 del Proyecto de Fortalecimiento de Instituciones Nacionales, centrado en el análisis de soluciones tecnológicas para digitalización de trámites y procesos administrativos.

El propósito principal de este análisis es identificar, evaluar y seleccionar la solución tecnológica más adecuada para implementar procesos de digitalización efectivos, sostenibles y alineados con los marcos normativos y estratégicos nacionales, tales como la Ley para la Simplificación de Requisitos y Trámites Administrativos (Decreto 5-2021), el Plan de Gobierno Digital 2021-2026, y la Guía de Gobierno Digital para Guatemala.

Durante el proceso, se consideraron tres modelos tecnológicos ampliamente utilizados en la modernización de gobiernos y organizaciones:

1. Desarrollo in-house de una plataforma propia.
2. Externalización (outsourcing) del desarrollo a través de un proveedor especializado.
3. Implementación de una solución de gestión por procesos (Business Process Management – BPM).

Cada una de estas opciones fue analizada bajo criterios técnicos, funcionales, de sostenibilidad, escalabilidad, tiempo de implementación, dependencia tecnológica, costos y experiencia internacional comparada. Tras un análisis multicriterio, se concluyó que la opción más viable, en términos estratégicos y operativos, es la implementación de una solución BPM.

La selección del BPM se basó en su capacidad para permitir el diseño, automatización, monitoreo y optimización continua de procesos administrativos sin requerir desarrollos

complejos ni dependencia de código fuente propietario. Esta opción facilita la construcción ágil de flujos de trabajo interoperables, fomenta la trazabilidad de trámites, mejora la experiencia del usuario y contribuye al cumplimiento de los principios de celeridad, eficacia y transparencia establecidos en la legislación guatemalteca.

Una vez definido el BPM como solución tecnológica prioritaria, se realizó un estudio comparativo de seis plataformas BPM reconocidas internacionalmente. Este estudio contempló aspectos como:

1. Grado de madurez y adopción en gobiernos y organismos multilaterales.
2. Modelos de licenciamiento (open source vs. propietarios).
3. Funcionalidades disponibles para gestión documental, integración con otros sistemas, motores de reglas, formularios y reportes.
4. Soporte para interoperabilidad, firmas electrónicas y cumplimiento normativo.
5. Flexibilidad para ser alojado en infraestructura propia o en la nube.
6. Costos asociados de implementación, mantenimiento y capacitación.

La selección final consideró no solo el desempeño técnico, sino también la viabilidad de su implementación en el contexto del Estado guatemalteco, con sus limitaciones actuales en infraestructura tecnológica, capital humano especializado y marco regulatorio aún en desarrollo.

Este producto presenta no solo el resultado del análisis comparativo, sino también recomendaciones prácticas y estratégicas para iniciar un proceso de adopción del BPM seleccionado como solución piloto, con potencial de escalamiento progresivo hacia más instituciones y servicios del Estado. El objetivo final es impulsar un modelo digital orientado al ciudadano, centrado en procesos eficientes y gobernanza basada en datos.

# OBJETIVOS

## GENERAL

Analizar y comparar diferentes soluciones tecnológicas para la digitalización de trámites administrativos en el Estado de Guatemala, con el fin de seleccionar la alternativa más adecuada que permita imp ementar procesos eficientes, interoperables y centrados en el ciudadano, priorizando la sostenibilidad, escalabilidad y cumplimiento normativo.

## ESPECÍFICOS

1. Evaluar las ventajas y limitaciones de tres modelos tecnológicos: desarrollo in-house, outsourcing y plataformas BPM, considerando criterios técnicos, económicos y estratégicos aplicables al contexto institucional del país.
2. Realizar un análisis comparativo de seis plataformas BPM reconocidas a nivel internacional, enfocado en su capacidad funcional, flexibilidad, integración, costos y alineación con la legislación guatemalteca y los principios de gobierno digital.
3. Recomendar la solución BPM más viable para su implementación inicial como piloto en instituciones del Organismo Ejecutivo, definiendo criterios de selección, condiciones de éxito y pasos estratégicos para su adopción y escalabilidad.

# TABLA DE ANÁLISIS COMPARATIVO DE POTENCIALES SOLUCIONES TECNOLÓGICAS EVALUADAS PARA LA DIGITALIZACIÓN

| Características Técnicas | Laserfiche | Appian | Bizagi | Sitecpro | IBM BPM |
|---|---|---|---|---|---|
| Compatibilidad BPMN 2.0 | Process Automation Designer | Appian Designer BPMN 2.0 | Bizagi Modeler BPMN 2.0 | Modelado BPMN básico | IBM BAW Designer con BPMN 2.0 completo |
| Motor de reglas de negocio | Rule Manager sin código para lógica condicional | Decision Designer + Appian SAIL rules | Business Rules Wizard | Reglas parametrizables limitadas | IBM Decision Designer / ODM integrado |
| Constructor low-code / no-code | Diseñador drag-and-drop; formularios web responsive | Low-code visual full stack | Bizagi Studio visual | Diseñador web drag-and-drop | Process Designer + Coach Views low-code |
| APIs e integraciones nativas | REST API, SDK .NET/Java, conectores SAP y Salesforce | Integration objects (REST, SOAP, RPA, Kafka) | REST/SOAP API, conectores SAP/SharePoint | SOAP/REST a sistemas internos | REST/GraphQL, Java, SAP, Salesforce, FileNet |
| Gestión documental integrada | ECM nativo con versionado y metadatos | Gestión documental básica (KMS) | Integración con SharePoint, repositorio ligado | Repositorio simple vinculado a Alfresco | FileNet Content Manager nativo |
| Automatización inteligente (RPA / OCR / IA) | RPA nativo + Smart OCR IA (Smart Capture) | Appian RPA + IA (Computer Vision) | IA vía Azure Cognitive Services (extensión) | Sin RPA/OCR nativo | IBM RPA bots, Watson AI, Datacap OCR |
| Escalabilidad horizontal | Arquitectura multitenant; escala horizontal en cluster | Auto-scaling en Appian Cloud | Escalamiento horizontal limitado | Escala vertical; clúster manual | Cluster OpenShift/Kubernetes con auto-scaling |
| Despliegue cloud / on-prem / híbrido | Laserfiche Cloud SaaS o Kubernetes on-prem/híbrido | SaaS nativo o self-managed sobre Kubernetes | On-prem o Bizagi Cloud (AWS) | Solo on-prem (Windows Server + SQL) | Cloud Pak (OpenShift on-prem) o SaaS IBM Cloud |
| Seguridad avanzada (cifrado end-to-end) | ISO/IEC 27001:2022, SOC 2 Type 2 (HIPAA), DoD 5015.2; OAuth 2.0, SAML, AES-256 | FedRAMP High, SOC 1/2/3, HIPAA; OAuth 2.0, SAML | ISO 27001:2022, FedRAMP Authorized, HIPAA, GDPR; LDAP/AD | Roles AD básicos; sin certificaciones reconocidas | FedRAMP-compliant IBM Cloud, FIPS-140-2, ISO 27001; OAuth 2.0, SAML |
| Auditoría y trazabilidad | Registro inmutable de eventos; cumplimiento HIPAA | Audit trails centralizados | BAM (Business Activity Monitoring) | Logs en BD y export CSV | Registro de eventos inmutable e informes GRC |
| Dashboards y monitoreo en tiempo real | Analytics Dashboards y KPI Runtime en tiempo real | Record analytics en tiempo real | BAM dashboards incorporados | Reportes Crystal Reports | Business Performance Center + Grafana |
| Preparado para contenedores / Kubernetes | Helm charts oficiales certificados | Appian docker images oficiales | Sin imágenes k8s oficiales (manual) | No soporta contenedores oficialmente | Helm charts en Cloud Pak Automation |
| DevOps / CI-CD integrado | CLI & REST hooks para pipelines GitHub/GitLab | Automated deployment manager API | Scripts de automatización; sin CI/CD nativo | Deploy manual; sin CI/CD | Tekton/OpenShift GitOps pipelines |
| Integración de firma electrónica | Laserfiche Sign integrado; conectores DocuSign | Appian Sign (DocuSign) | Conector DocuSign | No integra firma electrónica directamente | Conector IBM Verify; APIs DocuSign |
| Aplicaciones móviles nativas | Apps iOS/Android con captura offline | Appian Mobile offline | App móvil Bizagi (lectura y tareas) | Sin app móvil oficial | IBM MobileFirst templates responsive |

| Características Comerciales | Laserfiche | Appian | Bizagi | Sitecpro | IBM BPM |
|---|---|---|---|---|---|
| Tipo de licencia | SaaS mensual o perpetua on-prem | SaaS suscripción (por usuario/app) | Suscripción o perpetua | Perpetua servidor + clientes | Suscripción por VPC o SaaS IBM Cloud |
| Costo total de propiedad (3 años) | Bajo <1.5 millones | Alto > 3 millones de quetzales | Medio > 1.5 millones de quetzales | Medio > 1.5 millones de quetzales | Alto > 3 millones de quetzales |
| Modelo de usuarios / escalado | Usuarios concurrentes ilimitados en portal | Pago por usuario nombrado o app ilimitada | Por proceso o usuario nombrado | Licencia concurrente limitada | Ilimitado; coste por núcleos/containers |
| Opciones de despliegue comercial | SaaS Laserfiche Cloud o licencias on-prem | Appian Cloud o self-managed k8s | On-prem o Bizagi Cloud (AWS) | Solo on-prem (Windows) | Cloud Pak contenedorizado o SaaS IBM Cloud |
| Soporte y SLA incluidos | SLA 24/7 (1 h) + soporte LATAM | SLA 24/7 (4 h) | SLA 8×5 (24 h) estándar | SLA 8×5 (48 h) | IBM Support 24/7 (1 h) + GBM local |
| Referencias gubernamentales | Gob. Estados Unidos, El Salvador, Panamá, Costa Rica | NASA, USDA, UE | DIAN Colombia, Junta Andalucía | Municipalidades Guatemala | Educación USA, HMRC UK, Brasil e-Proc |
| Tiempo de implementación típico | 2-4 meses | 6-12 meses | 6-9 meses | 12+ meses | 6-12 meses |
| Capacitación y onboarding | E-learning ilimitado + LF Academy | Appian University (coste extra) | E-learning incluido; talleres premium | Capacitación presencial (coste) | IBM SkillsBuild + bootcamps GBM |
| Flexibilidad contractual | Contratos modulares, add-ons | Contrato multi-año requerido | Contrato anual mínimo | Poca flexibilidad | BYOL OpenShift, contratos Enterprise |
| Comunidad y partners regionales | 80+ partners LATAM (CDI, ABM) | 200+ partners globales | Partners locales moderados | Partners locales únicos | GBM, Kyndryl, Red Hat LATAM |
| Empresa certificada en Guatemala (NIT) | 325619 | 70154856 | 94693285 | 90996844 | No envió cotización |

## COSTO

### Laserfiche

Según G2, el costo parte desde aproximadamente US $300 por usuario al mes para la versión básica, llegando a US $1200/mes o US $1450/mes según el paquete contratado (Starter, Professional, Business). Estos precios pueden variar según términos de contrato, escalabilidad, módulos adicionales o implementación on-premise versus nube, por lo que se recomienda solicitar cotización detallada.

### Bizagi

Bizagi no publica precios estándar; la cotización se obtiene bajo solicitud, lo cual se da para Bizagi y Appian. El modelo freemium permite usar el Bizagi Modeler y Studio sin costo, ideal para modelado y prototipado; sin embargo, la automatización completa (Automación) requiere una licencia empresarial.

### Appian

Appian también requiere cotización personalizada, aunque su enfoque empresarial e integración de IA sugiere costos elevados. Las reseñas indican que su costo es elevado, especialmente para implementaciones amplias o funcionalidades avanzadas

## PERSONAL REQUERIDO

### Laserfiche

No se dispone de cifras exactas, pero la complejidad del sistema puede exigir inversión considerable en capacitación y soporte técnico especializado. Su enfoque en gestión documental sugiere que se necesita personal con experiencia en administración de contenido, integración API y flujos de aprobación.

Bizagi

Ofrece un entorno low-code con Modeler y Studio; esto permite que los analistas de negocio estructuren y mocelen sin depender exclusivamente de desarrolladores. Para funcionalidades complejas, se requiere personal técnico que opere Studio, configure reglas, formularios, reportes e integre sistemas.

Appian

Plataforma low-code visual que facilita el diseño por usuarios de negocio, pero el desarrollo de funcionalidades avanzadas (integraciones, automatización compleja) puede requerir desarrollacores o arquitectos de soluciones BPM, con conocimientos en Appian.

## TIEMPO DE IMPLEMENTACIÓN

Laserfiche

No hay datos concretos en las fuentes, pero dado que la plataforma incluye gestión documental avanzada, los tiempos pueden variar según la madurez de la infraestructura, la integración y la capacitación.

Bizagi

Permite un diseño rápido gracias al Modeler freemium. Sin embargo, la puesta en marcha de automatización completa depende del desarrollo en Studio y despliegue en Automation, lo que puede alargar el proceso.

Appian

Su enfoque de bajo código promueve una implementación rápida, especialmente en prototipos o MVP, apoyado por su entorno visual y capacidad de construcción acelerada. Aun así, la implementación total en entornos institucionales puede requerir varios meses dependiendo de la complejidad.

## BENEFICIOS

### Laserfiche

Destaca por su robusta gestión documental, automatización de aprobación, trazabilidad y control de registros. Ofrece integraciones con plataformas empresariales comunes (Salesforce, SAP, Adobe Sign, DocuSign), facilitando flujos centrados en documentos, usuarios valoran la calidad del soporte técnico, con alta calificación en servicio de atención al cliente.

### Bizagi

Excelente modelado BPMN, bajo código con interfaz amigable, y capacidades de monitoreo, trazabilidad, movilidad e integración con ERP/CRM, Freemium permite adopción inicial sin costo, ideal para prototipos.

### Appian

Plataforma low-code enfocada en velocidad de desarrollo, automatización sólida, integración con IA y escalabilidad para uso empresarial, ofrece monitoreo de procesos en tiempo real, reportes, conectividad robusta, ideal para procesos complejos.

## RIESGOS

### Laserfiche

Interfaz percibida como menos intuitiva en algunos casos; configuración y personalización pueden requerir mucho esfuerzo técnico, Dependencia de personal técnico para set-up; costos de implementación pueden elevarse si se requiere consultoría externa.

Bizagi

Implementaciones complejas pueden enfrentar bugs o errores en formularios (copias corruptas, plantillas ineficientes) según algunas reseñas, Curva de aprendizaje puede ser elevada en funcionalidad avanzada; soporte varía en calidad.

Appian

Elevado costo puede representar barrera de entrada global, Algunas funciones avanzadas pueden requerir soporte técnico especializado; curva de aprendizaje para usuarios con menos experiencia.

## EVALUACIONES DE LA HERRAMIENTA

La metodología propuesta se divide en varias Evaluaciones, cada una enfocada en recopilar, analizar y validar información para obtener una visión completa del entorno TI.

Evaluación de Infraestructura

La presente evaluación tiene como finalidad evaluar la integridad, disponibilidad, seguridad, resiliencia y cumplimiento normativo de la infraestructura tecnológica del Ministerio de Salud Pública y Asistencia Social, considerando componentes físicos, lógicos y procesos asociados.

Objetivos de la Evaluación

- Determinar el estado actual de la infraestructura física y lógica.
- Verificar la correcta implementación de controles de seguridad física y lógica.
- Evaluar la capacidad de recuperación ante fallos o desastres.
- Comprobar el cumplimiento de normativas nacionales e internacionales aplicables.
- Proporcionar un plan de acción para mitigar riesgos y optimizar la gestión de TI.

Resultados Esperados

- Lista priorizada de los eventos con su impacto y probabilidad.
- Recomendaciones viables y alineadas a buenas prácticas.
- Plan de mejora incorporable al plan estratégico de TI.

Alcance

La evaluación comprenderá la revisión de:

Componentes Físicos

- Centros de datos y salas de servidores: redundancia de operaciones, climatización, seguridad física, cableado.
- Servidores físicos y virtuales: hardware, firmware, redundancia, configuración.
- Equipos de red: switches, routers, firewalls, balanceadores, enlaces WAN y LAN.
- Sistemas de almacenamiento: SAN, NAS, DAS, configuración y políticas de acceso.
- Dispositivos de respaldo: cintas, discos externos, sistemas de backup dedicados.

Componentes Lógicos

- Sistemas operativos y middleware.
- Plataformas de virtualización y contenedores.
- Servicios en la nube (IaaS, PaaS, SaaS) y entornos híbridos.
- Bases de datos y sistemas de gestión.
- Mecanismos de control de acceso: IAM, Active Directory, MFA, SSO.

Procesos y Políticas

- Gestión de cambios y despliegues.
- Continuidad de negocio y recuperación ante desastres.

- Gestión de parches y actualizaciones.
- Procedimientos de respaldo y restauración.
- Gestión y respuesta a incidentes.
- Políticas de seguridad y clasificación de la información.

Normativa y Marcos de Referencia

- ISO 27001 / 27002: Gestión y controles de seguridad de la información.
- NIST SP 800-53 / Cybersecurity Framework: Controles y funciones de ciberseguridad.
- COBIT: Gobierno y gestión de TI.
- ITIL: Mejores prácticas para la gestión de servicios TI.

Evaluación de Arquitectura

La presente evaluación tiene como finalidad evaluar la seguridad, calidad, mantenibilidad y cumplimiento normativo de los sistemas de información desarrollados y mantenidos por la entidad, considerando código fuente, arquitectura de software, procesos de desarrollo y controles de seguridad aplicativa.

Objetivos Específicos

- Determinar el estado actual de la seguridad en aplicaciones web
- Verificar la correcta implementación de controles de desarrollo seguro
- Evaluar la calidad y mantenibilidad del código fuente
- Comprobar el cumplimiento de estándares de desarrollo y normativas aplicables
- Proporcionar un plan de acción para mitigar riesgos de desarrollo y optimizar procesos

Resultados Esperados

- Lista priorizada de vulnerabilidades y deficiencias técnicas con su impacto

- Recomendaciones viables alineadas a mejores prácticas de desarrollo seguro
- Plan de mejora técnica incorporable al ciclo de desarrollo actual

Alcance

El diagnóstico comprenderá la revisión de:

Aplicaciones y Sistemas

- Aplicaciones web internas y de cara al ciudadano
- APIs y servicios web: REST, SOAP, GraphQL
- Aplicaciones móviles (Android/iOS) si las hubiere
- Sistemas de gestión de contenido y portales
- Integraciones con sistemas externos y terceros

Código Fuente y Arquitectura

- Revisión estática del código fuente (SAST)
- Arquitectura de software y patrones de diseño
- Gestión de dependencias y librerías de terceros
- Configuraciones de frameworks y middleware
- Manejo de secretos y credenciales en código

Procesos de Desarrollo

- Metodologías de desarrollo y control de versiones
- Procesos de testing y aseguramiento de calidad
- Gestión de ambientes (desarrollo, testing, producción)
- Procedimientos de deployment y rollback
- Gestión de cambios y documentación técnica

Seguridad Aplicativa

- Controles de autenticación y autorización
- Validación de entradas y prevención de inyecciones
- Gestión de sesiones y tokens de acceso
- Cifrado de datos sensibles y comunicaciones
- Headers de seguridad y configuraciones del servidor web

Normativa y Marcos de Referencia

- OWASP Top 10: Vulnerabilidades más críticas en aplicaciones web
- OWASP ASVS: Estándar de verificación de seguridad en aplicaciones
- CWE Top 25: Debilidades de software más peligrosas
- ISO 27001/27002: Gestión de seguridad de la información
- NIST Secure Software Development Framework (SSDF)
- Normativas locales: Ley de protección de datos personales

Evaluación de Seguridad Integral

Esta sección detalla el proceso y las fases para ejecutar una evaluación de seguridad completa, describiendo los objetivos, las herramientas y las técnicas a emplear en cada etapa.

Consideraciones Éticas y Legales

Es imperativo subrayar que todas las actividades descritas en este manual deben ejecutarse bajo un estricto marco ético y con autorización previa y explícita del propietario de los activos a evaluar. La simulación de ataques, la explotación de vulnerabilidades y cualquier otra acción intrusiva deben realizarse de forma controlada, sin causar daño a los entornos productivos y respetando los límites acordados. La ausencia de un consentimiento por escrito invalida la legitimidad de la auditoría.

Fases de la Evaluación

La evaluación se estructura en las siguientes fases secuenciales, cada una con objetivos definidos y herramientas específicas.

Fase 1: Reconocimiento y Descubrimiento

Objetivo: Recopilar la máxima cantidad de información sobre la infraestructura del objetivo, tanto de forma pasiva como activa, para mapear la superficie de ataque.

- Técnicas y Herramientas:
  - WHOIS: Para obtener datos de registro de dominios, contactos y direcciones IP.
  - OSINT (Inteligencia de Fuentes Abiertas): Uso de Shodan y Google Dorks para encontrar dispositivos expuestos o archivos sensibles.
  - Enumeración de subdominios: Con herramientas como Sublist3r o TheHarvester para descubrir la estructura de dominios y correos electrónicos asociados.

Fase 2: Escaneo y Enumeración

Objetivo: Mapear la infraestructura identificada para descubrir puertos abiertos, servicios en ejecución, versiones de software y posibles puntos de entrada.

- Técnicas y Herramientas:
  - Escaneo de Puertos y Servicios (Nmap): Se ejecuta un escaneo para identificar puertos abiertos, versiones de servicios y el sistema operativo, lo que ayuda a encontrar servicios antiguos o sistemas sin parches.
  - Enumeración de Aplicaciones Web (Gobuster/Dirb): Se buscan por fuerza bruta directorios y archivos ocultos en servidores web para encontrar páginas de administración o archivos de configuración expuestos.

Fase 3: Análisis de Vulnerabilidades

Objetivo: Correlacionar la información recopilada con bases de datos de vulnerabilidades conocidas para identificar fallas potenciales de forma automatizada y manual.

- Técnicas y Herramientas:
  - Escaneo Automatizado (Nessus/OpenVAS): Se ejecutan escaneos para detectar software desactualizado, configuraciones erróneas y vulnerabilidades con identificadores CVE.
  - Análisis de Aplicaciones Web (Burp Suite/OWASP ZAP): Se intercepta y analiza el tráfico web para probar manualmente vulnerabilidades de alto impacto como Inyección SQL, Cross-Site Scripting (XSS) e Inclusión de Archivos.

Fase 4: Explotación Controlada

Objetivo: Demostrar el impacto real de una vulnerabilidad de forma controlada y sin causar daños al entorno.

- Técnicas y Herramientas:
  - Explotación de Servicios (Metasploit Framework): Se usan exploits públicos para verificar si una vulnerabilidad permite tomar control de un servicio o sistema.
  - Ataques de Fuerza Bruta (Hydra): Se prueba la fortaleza de las contraseñas en servicios expuestos como SSH o FTP.
  - Explotación de Bases de Datos (Sqlmap): Se automatiza la detección y explotación de inyecciones SQL para demostrar la posible extracción de datos sensibles.

Fase 5: Post-Explotación

Objetivo: Evaluar qué podría hacer un atacante una vez que ha comprometido un sistema, documentando el alcance y el impacto potencial del compromiso.

- Puntos de Evaluación:
  - Escalada de Privilegios: Verificar si es posible obtener permisos de administrador desde una cuenta de usuario estándar.
  - Reconocimiento Interno: Mapear la red interna desde el equipo comprometido para identificar otros activos vulnerables.
  - Captura de Evidencia: Tomar capturas de pantalla de datos sensibles a los que se tuvo acceso para documentar el impacto.

Fase 6: Evaluación de Controles de Seguridad

Objetivo: Revisar la postura de seguridad de la organización desde la perspectiva de las políticas y defensas implementadas.

- Áreas de Revisión:
  - Políticas y Controles de Acceso: Evaluar la implementación de contraseñas robustas, MFA, el principio de mínimo privilegio y analizar rutas de escalada con herramientas como BloodHound.
  - Segmentación de Red: Revisar la configuración de VLANs, DMZ y reglas de firewall.
  - Protecciones Perimetrales: Evaluar la configuración de firewalls, IDS/IPS y WAF.
  - Gestión de Vulnerabilidades y Parcheo: Examinar los procesos y políticas para escanear, priorizar y aplicar parches de seguridad.
  - Cifrado de Datos: Verificar el uso de cifrado en tránsito (TLS) y en reposo.
  - Seguridad Física: Auditar los controles de acceso a centros de datos y la vigilancia por CCTV.

Fase 7: Detección y Respuesta a Incidentes (D&RI)

Objetivo: Evaluar la capacidad de la organización para detectar y reaccionar eficazmente ante una brecha de seguridad.

- Capacidades a Evaluar:
  - Plan de Respuesta a Incidentes (IRP): Revisar si existe un plan documentado con roles y procedimientos definidos. Su ausencia es una debilidad crítica.
  - Monitoreo y Detección (SIEM): Verificar la existencia de un sistema SIEM para centralizar y correlacionar logs, así como alertas proactivas.
  - Análisis Forense: Validar si la organización tiene la capacidad (interna o externa) para determinar la causa raíz y el alcance de un compromiso.

# RECOMENDACIONES

A partir del análisis comparativo de las soluciones BPM evaluadas (Laserfiche, Bizagi y Appian), se presentan las siguientes recomendaciones para la selección, implementación y escalamiento de la herramienta más adecuada en el contexto de la digitalización de procesos del Estado de Guatemala:

### Priorizar soluciones escalables y sostenibles

Se recomienda optar por una plataforma BPM que ofrezca licenciamiento flexible y costos sostenibles en el tiempo. En este sentido, Bizagi presenta ventajas por su modelo freemium inicial y sus capacidades de crecimiento progresivo, ideal para proyectos piloto en instituciones públicas.

### Elegir herramientas con soporte a bajo código (low-code)

El enfoque low-code facilita la participación de perfiles no técnicos en la construcción de procesos, disminuye la dependencia de desarrolladores y acelera la implementación. Tanto Bizagi como Appian ofrecen entornos visuales que permiten esta modalidad, aunque Appian puede implicar mayores costos.

### Iniciar con un piloto de bajo riesgo y alta visibilidad

Se sugiere comenzar con un trámite administrativo interno de mediana complejidad, con impacto directo en la eficiencia operativa. Esto permitirá validar la herramienta seleccionada, medir tiempos de implementación y ajustes necesarios antes de escalar a otros procesos más complejos o sensibles.

### Invertir en formación de personal clave

Independientemente de la herramienta seleccionada, se debe formar a un equipo técnico y funcional interno en diseño de procesos, modelado BPMN, administración de la plataforma y gestión del cambio. Esto reduce la dependencia de proveedores externos y fortalece capacidades institucionales.

### Evaluar las condiciones de interoperabilidad

La solución BPM debe integrarse con los sistemas existentes y futuros del Estado, como el portal de servicios digitales, sistemas de autenticación y firma electrónica. Por ello, se debe verificar que la herramienta seleccionada cuente con APIs robustas y compatibilidad con estándares abiertos.

### Establecer una hoja de ruta institucional para escalamiento

Finalmente, se recomienda que la institución defina una estrategia a mediano plazo para la adopción progresiva de BPM en otras áreas, alineada al Plan de Gobierno Digital y al Decreto 5-2021 Ley para la Simplificación de Requisitos y Trámites Administrativos. Esta hoja de ruta debe incluir hitos, responsables, presupuesto y mecanismos de monitoreo.