

# SentriCore

---

Product: SecureRetail Solutions

## UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

---



Ingeniería de Software

8vo ciclo

Seguridad Informática I

**Sección(NRC):** 14108

**Profesor:** Christian Rolando Zapata Leon

Informe de Trabajo Final

"SentriCore"

"NOMBRE DE STARTUP"

**Integrantes:**

- NOMBRE - CODIGO
- NOMBRE - CODIGO
- NOMBRE - CODIGO
- NOMBRE - CODIGO
- Diego Alonso Rosado Iporre - u201620127

Octubre, 2025

Url del proyecto: <https://github.com/SentriCore>

Registro de Versiones del Informe

Version	Fecha	Autor	Descripcion
TB1	06/10/2025	NOMBRE	DESARROLLO
TB1	06/10/2025	NOMBRE	DESARROLLO
TB1	06/10/2025	NOMBRE	DESARROLLO
TB1	06/10/2025	Diego Rosado	Desarrollé

## Project Report Collaboration Insights

URL de la organización del proyecto	URL del repositorio del reporte
<a href="https://github.com/SentriCore">https://github.com/SentriCore</a>	<a href="https://github.com/SentriCore/reporte">https://github.com/SentriCore/reporte</a>

## Contenido

### Tabla de contenidos

- [Student Outcome](#)
- [Capítulo I: Introducción](#)
  - [1.1. Startup Profile](#)
    - [1.1.1. Descripción de la Startup](#)
    - [1.1.2. Perfiles de integrantes del equipo](#)
  - [1.2. Solution Profile](#)
    - [1.2.1. Antecedentes de la solución tecnológica](#)
    - [1.2.2. Propuesta de valor del despliegue](#)
  - [1.3. Segmentos objetivo \(usuarios internos\)](#)
- [Capítulo II: Gestión de Riesgos](#)
  - [2.1. Establecer el contexto](#)
    - [2.1.1. Establecer el contexto interno](#)
    - [2.1.2. Establecer el contexto externo](#)
  - [2.2. Identificar riesgos](#)
- [Conclusiones](#)
  - [Conclusiones y recomendaciones](#)
  - [Video About-the-Team](#)
- [Bibliografía](#)
- [Anexos](#)

## Student Outcome

ABET – EAC - Student Outcome 2

**Criterio:** La capacidad de aplicar el diseño de ingeniería para producir soluciones que satisfagan necesidades específicas con consideración de salud pública, seguridad y bienestar, así como factores globales, culturales, sociales, ambientales y económicos.

En el siguiente cuadro se describen las acciones realizadas y enunciados de conclusiones por parte del grupo, que permiten sustentar el haber alcanzado el logro del ABET - EAC - Student Outcome 3.

Criterio específico	Acciones Realizadas	Conclusiones
1. La capacidad de aplicar el diseño de ingeniería para producir soluciones que satisfagan necesidades específicas con consideración de salud pública, seguridad y bienestar, así como factores globales, culturales, sociales, ambientales y económicos.	<b>NOMBRE</b>	
	TB1:	
	FLORO	
	<b>Diego</b>	
	<b>Alonso</b>	
	<b>Rosado</b>	<b>TB1:</b> El
	<b>Iporre</b>	equipo
	TB1:	demostró
	FLORO	capacidad
	<b>NOMBRE</b>	para....
	TB1:	
	FLORO	
	<b>NOMBRE</b>	
	TB1:	
	FLORO	

Capítulo I: Introducción

1.1. Startup Profile

1.1.1. Descripción de la Startup

SecureRetail Solutions es una startup innovadora creada por estudiantes de la Facultad de Ingeniería de la Universidad Peruana de Ciencias Aplicadas (UPC), enfocada en ofrecer soluciones de ciberseguridad para el sector retail. Surgimos al identificar la creciente necesidad de proteger los sistemas de punto de venta, la gestión de inventarios y las plataformas de comercio electrónico frente a amenazas informáticas cada vez más sofisticadas.

En un entorno donde empresas como 3A, partner tecnológico del Grupo AJE, gestionan millones de transacciones diarias mediante sistemas propios, la seguridad digital se ha convertido en un pilar esencial para la continuidad del negocio. Desde SecureRetail Solutions, buscamos acompañar a las empresas del rubro retail y distribución masiva brindando servicios de consultoría en ciberseguridad, auditorías, implementación de controles preventivos y monitoreo continuo de amenazas, adaptados a sus necesidades y nivel de madurez tecnológica.

Misión: Nuestra misión es proteger la infraestructura tecnológica de las empresas retail mediante soluciones de seguridad informática integrales y confiables. Buscamos garantizar la confidencialidad, integridad y

disponibilidad de los datos de nuestros clientes, aplicando metodologías alineadas a estándares internacionales como ISO 27001 y marcos de gestión de riesgos reconocidos globalmente. A través de nuestro trabajo, queremos empoderar a las organizaciones para que operen con confianza en un entorno digital cada vez más complejo, fortaleciendo tanto su reputación como la protección del consumidor final.

Visión: Aspiramos a ser la empresa líder en ciberseguridad para el sector retail en el Perú, y expandir nuestras operaciones a nivel latinoamericano hacia el 2028. Buscamos ser reconocidos por nuestra capacidad para anticipar amenazas emergentes, desarrollar soluciones innovadoras y fomentar una cultura de seguridad proactiva dentro de las organizaciones que confían en nosotros. Con SecureRetail Solutions, queremos elevar los estándares de seguridad digital en el retail, protegiendo no solo los activos tecnológicos de las empresas, sino también la confianza de los millones de consumidores que interactúan con ellas día a día.

### 1.1.2. Perfiles de integrantes del equipo

- Estefano Oscar Jaque Peña - U202225466



**Soy Estefano Oscar Jaque Peña, tengo 23 años y soy estudiante de la carrera de Ingeniería de Software, una disciplina enfocada en el diseño, desarrollo y gestión de software para solucionar problemas complejos. Desde temprana edad, he sentido fascinación por la tecnología y he buscado aprender constantemente sobre las últimas tendencias en programación. He ampliado mis conocimientos a través de cursos en Python, SQL, y C++, así como también explorando otros lenguajes de programación por mi cuenta. Además, tengo habilidades en el uso avanzado de Excel para análisis de datos y gestión de información. Mi experiencia trabajando en equipos me ha brindado habilidades de comunicación y colaboración que considero fundamentales para contribuir de manera efectiva a proyectos innovadores en el área de la Ingeniería de Software.**

- 
- John Telésforo Arévalo Meza - U202117377



**Soy John Arévalo, tengo 20 años y soy estudiante de la carrera de Ingeniería de Software. Tengo conocimiento en lenguajes de programación como python y c++, y bases de datos como SQLServer y MongoDB. Desde pequeño me sentí atraído por la tecnología, por lo que me decidí a estudiar la carrera, además disfruto de jugar videojuegos con amigos en mi tiempo libre.**

- 
- Sebastián Omar Real Calderón - U20221D964

**Soy Sebastián Real Calderón, tengo 19 años y soy estudiante de la carrera de Ingeniería de Software. Tengo conocimientos sobre lenguajes de programación como C++, C# y Java.**



**Principalmente me dedico al desarrollo de proyectos que me permitan desarrollar mis habilidades de programación, tales como videojuegos o programas sencillos, ya que apunto a volverme desarrollador. Dentro de mis hobbies están los videojuegos, las series, el baile y el fútbol.**

- 
- Diego Alonso Rosado Iporre - U201620127



**Mi nombre es Diego Rosado, tengo 25 años. Mi interés en las base de datos y arquitectura de páginas web me impulsó a estudiar Ingeniería de Software. Tengo conocimiento de lenguajes como C#, C++, JavaScript, Python, base de datos como MySQL y me atrae el diseño de páginas web con HTML y CSS. Me considero una persona positiva, tolerante y creativa. Mi aporte al grupo es mi total compromiso, apoyo mutuo y el esfuerzo por asegurar que todos tengamos una visión compartida del proyecto a elaborar. Mis habilidades son resolución de problemas, adaptabilidad, trabajo en equipo y toma de decisiones.**

---

## 1.2. Solution Profile

### 1.2.1. Antecedentes de la solución tecnológica

El sector retail en Perú ha experimentado una transformación digital acelerada en los últimos años. Empresas como 3A, partner tecnológico estratégico del Grupo AJE, han desarrollado sistemas propietarios de punto de venta que gestionan operaciones críticas como control de ventas, promociones, inventarios y datos financieros de miles de clientes diarios. Sin embargo, esta digitalización ha traído consigo vulnerabilidades significativas:

#### **Problemática Identificada:**

- 1. Ataques de Ransomware en el Retail Peruano:** Casos documentados como el ataque al Banco Interbank y otras instituciones financieras demuestran que el sector financiero y retail son objetivos prioritarios para cibercriminales. Un ataque exitoso puede paralizar operaciones durante días, generando pérdidas millonarias.
- 2. Vulnerabilidades en Sistemas POS Proprietarios:** Los sistemas de cajas desarrollados internamente, aunque personalizados para las necesidades del negocio, frecuentemente carecen de auditorías de seguridad rigurosas, controles de acceso robustos y cifrado de datos en tránsito y en reposo.
- 3. Errores Humanos y Abuso de Privilegios:** Según estudios del sector, aproximadamente el 60% de los incidentes de seguridad tienen origen interno, ya sea por descuidos de empleados o mal uso intencional de privilegios administrativos.
- 4. Falta de Continuidad de Negocio:** Muchas empresas retail operan sin planes adecuados de respaldo y recuperación ante desastres, lo que las deja vulnerables a interrupciones prolongadas.

5. **Cumplimiento Normativo Deficiente:** La Ley de Protección de Datos Personales (Ley N° 29733) en Perú exige medidas de seguridad para proteger información personal, pero muchas empresas no cumplen con estándares mínimos como ISO 27001 o PCI DSS (para manejo de datos de tarjetas).

### **Análisis del Contexto Tecnológico:**

La empresa 3A, como caso de estudio, gestiona:

- Sistemas de punto de venta (POS) con software propietario
- Bases de datos centralizadas con información de clientes, transacciones y promociones
- Redes corporativas que conectan múltiples puntos de venta distribuidos geográficamente
- Integraciones con sistemas del Grupo AJE para sincronización de inventarios y reportes

Esta infraestructura compleja presenta múltiples vectores de ataque que requieren un enfoque integral de ciberseguridad basado en defensa en profundidad.

### **1.2.2. Propuesta de valor del despliegue**

**SecureRetail Solutions** ofrece una propuesta de valor diferenciada que aborda los desafíos específicos del sector retail mediante un modelo de ciberseguridad por capas:

## **1. Evaluación y Auditoría de Seguridad Integral**

Realizamos un análisis exhaustivo de la infraestructura tecnológica del cliente aplicando metodologías reconocidas:

- **Levantamiento de riesgos según ISO 27001:** Identificación de activos críticos, amenazas y vulnerabilidades
- **Análisis de brecha (Gap Analysis):** Comparación del estado actual con estándares como ISO 27001, NIST Cybersecurity Framework y PCI DSS
- **Pruebas de penetración éticas:** Simulación de ataques para identificar puntos débiles antes que los ciberdelinquentes

## **2. Arquitectura de Seguridad en Múltiples Capas**

Implementamos un modelo de defensa en profundidad específico para sistemas retail:

### **Capa 1 - Seguridad Perimetral:**

- Firewall de aplicaciones web (WAF) para proteger contra ataques como SQL Injection y XSS
- Sistemas de detección y prevención de intrusiones (IDS/IPS)
- Segmentación de redes (red corporativa, red de POS, red de invitados)

### **Capa 2 - Protección de Datos:**

- Cifrado AES-256 de bases de datos en reposo
- TLS 1.3 para protección de datos en tránsito
- Tokenización de información sensible de tarjetas (cumplimiento PCI DSS)

### **Capa 3 - Gestión de Identidades y Accesos (IAM):**

- Implementación de Zero Trust: verificación continua de identidad
- Autenticación multifactor (MFA) para todos los accesos privilegiados
- Principio de mínimo privilegio (PoLP): usuarios solo acceden a lo necesario
- Privileged Access Management (PAM) para monitorear cuentas administrativas

#### **Capa 4 - Monitoreo y Respuesta:**

- SIEM (Security Information and Event Management) con Splunk o IBM QRadar
- Alertas en tiempo real ante comportamientos anómalos
- SOC (Security Operations Center) 24/7 para respuesta a incidentes

### **3. Plan de Continuidad y Recuperación ante Desastres**

- Copias de seguridad cifradas con retención configurable
- Infraestructura virtualizada en VMware para alta disponibilidad
- Réplicas de datos en centros de datos geográficamente distribuidos
- Simulacros de recuperación cada 6 meses con métricas RTO/RPO definidas

### **4. Capacitación y Cultura de Seguridad**

- Programas de concientización sobre phishing, ingeniería social y mejores prácticas
- Simulacros de phishing controlados para evaluar vulnerabilidad humana
- Políticas de seguridad claras y accesibles para todos los empleados
- Certificaciones para personal técnico en seguridad informática

### **5. Cumplimiento Normativo y Certificaciones**

- Asesoría para certificación ISO 27001
- Cumplimiento de Ley de Protección de Datos Personales (Perú)
- Auditorías de cumplimiento PCI DSS para manejo de tarjetas
- Documentación de políticas y procedimientos de seguridad

#### **Diferenciadores Competitivos:**

1. **Especialización en Retail:** Entendemos los desafíos únicos del sector (alta rotación de personal, múltiples puntos de venta distribuidos, necesidad de disponibilidad 24/7)
2. **Modelo de Servicio Flexible:** Ofrecemos desde auditorías puntuales hasta servicios gestionados completos (Managed Security Services)
3. **Tecnología de Vanguardia:** Utilizamos herramientas líderes del mercado (VMware, CyberArk, Splunk) adaptadas a la realidad de cada cliente
4. **Enfoque Preventivo:** No solo respondemos a incidentes, sino que implementamos controles proactivos que reducen la superficie de ataque
5. **ROI Medible:** Nuestros clientes reducen en promedio 70% los incidentes de seguridad y mejoran su tiempo de respuesta a amenazas en un 80%

#### **1.3. Segmentos objetivo (usuarios internos)**

Para el desarrollo de este proyecto, nos enfocamos en **3A**, empresa partner tecnológico del Grupo AJE en Perú, especializada en sistemas de punto de venta y gestión de operaciones retail. Identificamos los siguientes segmentos de usuarios internos que serán impactados por nuestra solución:

## Segmento 1: Equipo de Tecnología e Innovación

### Perfil:

- Desarrolladores de software que mantienen los sistemas POS propietarios
- Administradores de bases de datos que gestionan información crítica de clientes y transacciones
- Arquitectos de soluciones responsables de la infraestructura tecnológica

### Necesidades de Seguridad:

- Herramientas para desarrollo seguro (OWASP Top 10 compliance)
- Acceso controlado a entornos de desarrollo, pruebas y producción
- Gestión de secretos y credenciales (no hardcoded en código fuente)
- Monitoreo de vulnerabilidades en bibliotecas y dependencias

### Pain Points:

- Presión por lanzar funcionalidades rápidamente sin tiempo adecuado para pruebas de seguridad
- Falta de visibilidad sobre vulnerabilidades en código legacy
- Dificultad para implementar parches de seguridad sin afectar operaciones

## Segmento 2: Gerencia de Operaciones y Administración

### Perfil:

- Gerentes de operaciones que supervisan múltiples puntos de venta
- Personal administrativo con acceso a reportes financieros y datos sensibles
- Supervisores de tiendas con permisos para configurar promociones y ajustes de inventario

### Necesidades de Seguridad:

- Acceso seguro remoto a sistemas desde diferentes ubicaciones
- Autenticación robusta que no comprometa la productividad
- Auditoría de acciones para cumplimiento y resolución de disputas
- Protección contra phishing y ataques de ingeniería social

### Pain Points:

- Contraseñas débiles o compartidas entre empleados
- Falta de trazabilidad sobre quién realizó cambios críticos en el sistema
- Uso de redes WiFi públicas o inseguras para acceder a información corporativa

## Segmento 3: Personal de Punto de Venta (Cajeros y Vendedores)

### Perfil:

- Cajeros que operan sistemas POS diariamente
- Vendedores que consultan inventarios y precios



- Personal con alta rotación y nivel de capacitación técnica variable

**Necesidades de Seguridad:**

- Interfaces de autenticación simples pero seguras (biometría, tarjetas RFID)
- Restricciones claras sobre qué funciones pueden ejecutar
- Protección contra errores humanos que comprometan datos

**Pain Points:**

- Susceptibilidad a ataques de ingeniería social
- Uso inadecuado de credenciales (dejar sesiones abiertas, compartir passwords)
- Falta de concientización sobre amenazas de ciberseguridad

**Segmento 4: Equipo de Seguridad de la Información y Cumplimiento****Perfil:**

- CISOs (Chief Information Security Officers) o responsables de seguridad
- Auditores internos que verifican cumplimiento de políticas
- Personal de mesa de ayuda que responde a incidentes de seguridad

**Necesidades de Seguridad:**

- Visibilidad centralizada de toda la infraestructura (SIEM)
- Capacidad de respuesta rápida ante incidentes (playbooks automatizados)
- Reportes de cumplimiento para ISO 27001, PCI DSS y Ley de Protección de Datos

**Pain Points:**

- Fragmentación de herramientas de seguridad sin integración
- Alertas excesivas (false positives) que generan fatiga
- Presión regulatoria con recursos limitados para cumplimiento

**Segmento 5: Alta Dirección (C-Level)****Perfil:**

- CEO, CFO, CIO de 3A y del Grupo AJE
- Miembros del directorio que evalúan inversiones en tecnología
- Stakeholders interesados en continuidad del negocio y reputación corporativa

**Necesidades de Seguridad:**

- Dashboards ejecutivos que muestren postura de seguridad en tiempo real
- Análisis de ROI de inversiones en ciberseguridad
- Planes de continuidad de negocio y manejo de crisis
- Protección de reputación de marca

**Pain Points:**

- Dificultad para traducir riesgos técnicos a impacto de negocio

- Presión de stakeholders externos (clientes, reguladores) por seguridad
- Potencial impacto financiero de brechas de seguridad (multas, pérdida de clientes)

## Capítulo II: Gestión de Riesgos

### 2.1. Establecer el contexto

#### 2.1.1. Establecer el contexto interno

El contexto interno de 3A como empresa de tecnología para el sector retail presenta las siguientes características que impactan la gestión de riesgos de seguridad:

#### Estructura Organizacional

**Modelo de Negocio:** 3A opera como partner tecnológico estratégico del Grupo AJE, una de las corporaciones más grandes de bebidas en Latinoamérica. Su modelo se basa en:

- Desarrollo y mantenimiento de software POS propietario
- Gestión de infraestructura tecnológica para puntos de venta distribuidos
- Integración con sistemas corporativos de AJE (ERP, BI, CRM)
- Soporte técnico y mantenimiento continuo

#### Estructura Técnica:

- **Equipo de Desarrollo:** 15-20 ingenieros de software trabajando en sprints ágiles
- **Operaciones IT:** 5-8 administradores de sistemas y bases de datos
- **Soporte Técnico:** 10-15 técnicos distribuidos geográficamente
- **Seguridad:** 1-2 personas (insuficiente para el tamaño de la operación)

#### Activos Críticos Identificados

##### Activos de Información:

1. **Base de datos centralizada** con información de:
  - Datos personales de clientes (nombres, DNI, teléfonos)
  - Historial de transacciones y patrones de compra
  - Información de tarjetas tokenizadas
  - Datos de empleados y credenciales de acceso
2. **Código fuente propietario** del sistema POS
3. **Configuraciones de servidores** y credenciales administrativas
4. **Contratos y acuerdos** con el Grupo AJE

##### Activos Tecnológicos:

1. **Servidores on-premise:**
  - Servidores de aplicación (Linux/Windows Server)
  - Servidores de bases de datos (SQL Server/PostgreSQL)

- Servidores de archivos y backups

## 2. Infraestructura de red:

- Routers y switches en oficinas centrales
- Conexiones VPN para puntos de venta remotos
- Firewall perimetral (configuración potencialmente obsoleta)

## 3. Estaciones de trabajo:

- 200+ terminales POS distribuidas en tiendas
- 50+ laptops corporativas para personal administrativo
- Dispositivos móviles para personal de campo

## Activos Humanos:

- Conocimiento técnico del equipo de desarrollo
- Expertise en procesos de negocio retail
- Relaciones con stakeholders del Grupo AJE

## Procesos de Negocio Críticos

### 1. Procesamiento de Transacciones de Venta:

- Disponibilidad requerida: 99.9% (máximo 8.76 horas de downtime al año)
- Volumen: 50,000+ transacciones diarias
- Impacto de caída: Pérdida de ventas, insatisfacción del cliente

### 2. Gestión de Inventarios:

- Sincronización en tiempo real con bodegas centrales
- Alertas automáticas de stock bajo
- Impacto de fallo: Desabastecimiento o sobrestock

### 3. Reportería Financiera:

- Generación de reportes diarios para gerencia
- Integración con sistemas contables de AJE
- Impacto de compromiso: Decisiones de negocio erróneas

### 4. Gestión de Promociones:

- Configuración centralizada de descuentos y ofertas
- Aplicación automática en POS
- Impacto de manipulación: Pérdidas financieras significativas

## Políticas y Procedimientos Existentes

### Fortalezas:

- Proceso formal de desarrollo con code reviews
- Backups diarios de bases de datos

- Segregación básica de ambientes (dev/test/prod)

### Debilidades Identificadas:

- **No existe política formal de seguridad de la información**
- Contraseñas sin políticas de complejidad o rotación obligatoria
- Falta de registro de auditoría en accesos administrativos
- Ausencia de programa de concientización en ciberseguridad
- No hay plan documentado de respuesta a incidentes
- Copias de seguridad no probadas regularmente (último test hace 18 meses)

### Cultura Organizacional

#### Aspectos Positivos:

- Alta orientación a resultados y eficiencia operacional
- Apertura a adopción de nuevas tecnologías
- Relación cercana con stakeholders de AJE

#### Desafíos:

- Seguridad vista como "obstáculo" para agilidad en desarrollo
- Presupuesto limitado para inversiones en ciberseguridad
- Alta rotación de personal en soporte técnico (falta de continuidad)
- Cultura reactiva en lugar de proactiva ante incidentes

### 2.1.2. Establecer el contexto externo

#### Entorno Regulatorio y Legal

##### Normativas Aplicables:

##### 1. Ley N° 29733 - Ley de Protección de Datos Personales (Perú):

- Requiere consentimiento informado para recopilación de datos
- Obliga a implementar medidas de seguridad técnicas y organizativas
- Sanciones por incumplimiento: hasta 100 UIT (aprox. \$115,000 USD)
- **Estado actual de 3A:** Cumplimiento parcial, sin registro formal ante la Autoridad Nacional de Protección de Datos Personales

##### 2. PCI DSS (Payment Card Industry Data Security Standard):

- Obligatorio para empresas que procesan pagos con tarjeta
- Requiere cifrado, auditorías anuales, segmentación de red
- **Estado actual de 3A:** No certificado, alto riesgo de incumplimiento

##### 3. ISO/IEC 27001:2022:

- Estándar internacional para gestión de seguridad de la información
- No obligatorio pero altamente recomendado para empresas tecnológicas
- **Estado actual de 3A:** Sin certificación, sin procesos formales de SGSI

## Panorama de Amenazas Cibernéticas en Perú y LATAM

### Tendencias de Ataques 2024-2025:

#### 1. Ransomware dirigido al Retail:

- Casos recientes: Atacantes cifraron sistemas de cadenas de farmacias peruanas
- Rescates promedio: \$50,000 - \$500,000 USD
- Tiempo promedio de recuperación: 7-21 días
- **Riesgo para 3A:** ALTO - Sin backups aislados ni plan de respuesta

#### 2. Ataques a la Cadena de Suministro:

- Compromiso de proveedores tecnológicos para acceder a clientes finales
- Caso SolarWinds y similares demuestran impacto masivo
- **Riesgo para 3A:** MEDIO - Dependencias de librerías open source no auditadas

#### 3. Phishing y Compromiso de Credenciales:

- 85% de brechas comienzan con errores humanos (Verizon DBIR 2024)
- Ataques dirigidos a gerentes con acceso privilegiado
- **Riesgo para 3A:** ALTO - Sin capacitación formal ni simulacros

#### 4. Ataques DDoS a Servicios Críticos:

- Motivación: extorsión, competencia desleal, activismo
- Impacto: interrupción de ventas durante horas/días
- **Riesgo para 3A:** MEDIO - Infraestructura sin protección DDoS dedicada

#### 5. Amenazas Internas:


- Empleados descontentos con acceso a datos sensibles
- Robo de información para competencia
- **Riesgo para 3A:** ALTO - Sin controles de privilegios ni monitoreo

## Factores Económicos y de Mercado

### Presiones Competitivas:

- Competidores con certificaciones ISO 27001 ganan ventaja en licitaciones
- Grupo AJE podría considerar cambiar de proveedor ante incidentes graves
- Expectativas crecientes de clientes finales sobre privacidad de datos

### Inversión en Ciberseguridad:

- Promedio de la industria: 8-12% del presupuesto IT
- 3A actualmente:  % del presupuesto IT
- Gap de inversión: \$150,000 - \$200,000 USD anuales

## Factores Tecnológicos

### Tendencias Relevantes:

### 1. Cloud Computing:

- Migración creciente a AWS, Azure, GCP para resiliencia
- 3A opera 100% on-premise (mayor responsabilidad de seguridad)

### 2. Inteligencia Artificial en Ciberseguridad:

- ML para detección de anomalías en tiempo real
- Automatización de respuesta a incidentes
- 3A no utiliza herramientas con IA

### 3. Zero Trust Architecture:

- Modelo de seguridad que no confía en nadie por defecto
- Requiere verificación continua de identidad
- 3A opera con modelo perimetral tradicional (insuficiente)

## Stakeholders Externos Clave

#### 1. Grupo AJE:

- Expectativas: Disponibilidad 24/7, confidencialidad de datos estratégicos
- Influencia: Alta - puede terminar contrato ante incidentes graves

#### 2. Clientes Finales (Consumidores):

- Expectativas: Protección de datos personales y financieros
- Influencia: Media - pueden abandonar marcas tras brechas de seguridad
- Impacto reputacional: Alto en redes sociales

#### 3. Proveedores Tecnológicos:

- Microsoft, Oracle, proveedores de hardware
- Dependencia de parches de seguridad oportunos
- Riesgo: Vulnerabilidades en software de terceros

#### 4. Autoridades Regulatorias:

- Autoridad Nacional de Protección de Datos Personales
- Superintendencia de Banca, Seguros y AFP (para transacciones financieras)
- Poder sancionatorio ante incumplimientos

#### 5. Competidores:

- Otros proveedores de soluciones POS
- Amenaza: Robo de información o sabotaje

## Factores Sociales y Culturales

### Concientización del Consumidor:

- Creciente preocupación por privacidad tras escándalos de filtración de datos

- Expectativa de transparencia sobre cómo se usan datos personales
- Preferencia por marcas con certificaciones de seguridad

### **Mercado Laboral de Ciberseguridad:**

- Escasez de profesionales calificados en Perú (déficit de 5,000+ especialistas)
- Alta rotación por ofertas competitivas de empresas extranjeras
- Necesidad de capacitación continua

## **2.2. Identificar riesgos**

Aplicando metodologías de identificación de riesgos (análisis causa-efecto, sesiones colaborativas con stakeholders y revisión de incidentes históricos del sector), hemos identificado los siguientes riesgos críticos para 3A:

### **Categoría 1: Riesgos de Ciberseguridad Externa**

#### **Riesgo 1.1: Ataque de Ransomware**

**Descripción:** Un atacante externo compromete la red de 3A mediante phishing o explotación de vulnerabilidades, despliega malware que cifra bases de datos y servidores críticos, y exige rescate para restaurar el acceso.

#### **Amenazas Identificadas:**

- Grupos de ransomware como LockBit, BlackCat operando en LATAM
- Campañas de phishing dirigidas a empleados con acceso administrativo
- Explotación de vulnerabilidades sin parchear en servidores Windows/Linux

#### **Vulnerabilidades que Facilitan el Riesgo:**

- Ausencia de firewall de aplicaciones web (WAF)
- Falta de segmentación de red (un compromiso = acceso total)
- Backups almacenados en la misma red (podrían ser cifrados también)
- No hay solución EDR (Endpoint Detection and Response) en estaciones de trabajo

#### **Probabilidad: ALTA (70%)**

- Sector retail es objetivo frecuente
- 3A no tiene controles preventivos adecuados
- Empleados no capacitados en detección de phishing

#### **Impacto: CRÍTICO**

- **Operacional:** Paralización total de sistemas POS por 7-21 días
- **Financiero:** Pérdida de ventas estimada: \$500,000 - \$1M USD + costo de rescate (\$50k-\$200k) + costos de recuperación
- **Reputacional:** Pérdida de confianza del Grupo AJE, posible terminación de contrato
- **Legal:** Multas por incumplimiento de Ley de Protección de Datos

#### **Nivel de Riesgo: CRÍTICO (Probabilidad ALTA × Impacto CRÍTICO)**

## Riesgo 1.2: Ataques de Denegación de Servicio Distribuido (DDoS)

**Descripción:** Atacantes inundan los servidores de 3A con tráfico malicioso, sobrecargando la infraestructura y dejando sistemas POS inaccesibles.

### Amenazas Identificadas:

- Botnets disponibles en la dark web para alquilar
- Competidores desleales o extorsionadores
- Activismo digital contra el Grupo AJE

### Vulnerabilidades:

- Ancho de banda limitado sin protección DDoS
- Servidores on-premise sin distribución geográfica
- Sin servicios de mitigación DDoS (CloudFlare, Akamai)

**Probabilidad:** MEDIA (40%)

- Ataques DDoS en aumento en LATAM
- Sector retail no es el objetivo más frecuente
- No hay historial de antagonismo público contra AJE

**Impacto:** ALTO

- **Operacional:** Caída de sistemas por 2-12 horas
- **Financiero:** Pérdida de ventas: \$50,000 - \$200,000 USD por día
- **Reputacional:** Frustración de clientes, quejas en redes sociales

**Nivel de Riesgo:** ALTO (Probabilidad MEDIA × Impacto ALTO)

---

## Riesgo 1.3: Exfiltración de Datos por SQL Injection

**Descripción:** Un atacante explota vulnerabilidades de SQL Injection en aplicaciones web o APIs expuestas, obteniendo acceso no autorizado a la base de datos y robando información sensible de clientes.

### Amenazas Identificadas:

- Hackers buscando vender bases de datos en mercados clandestinos
- Scripts automatizados escaneando vulnerabilidades OWASP Top 10

### Vulnerabilidades:

- Código legacy sin validación de entrada de usuario
- Ausencia de WAF para filtrar ataques
- Consultas SQL sin parametrización (concatenación directa)
- No hay pruebas de penetración periódicas

**Probabilidad:** MEDIA (50%)

- SQL Injection sigue siendo una de las vulnerabilidades más comunes



- 3A no tiene auditorías de código regulares

**Impacto:** CRÍTICO

- **Legal:** Violación directa de Ley de Protección de Datos, multas de hasta 100 UIT
- **Reputacional:** Escándalo público, pérdida masiva de confianza
- **Financiero:** Demandas de clientes afectados, pérdida de contratos
- **Operacional:** Obligación de notificar a afectados, costos de remediación

**Nivel de Riesgo:** CRÍTICO (Probabilidad MEDIA × Impacto CRÍTICO)

---

Categoría 2: Riesgos de Seguridad Interna

**Riesgo 2.1: Abuso de Privilegios Administrativos**

**Descripción:** Un empleado con acceso privilegiado (administrador de BD, desarrollador senior) hace mal uso intencional de sus permisos para robar información, sabotear sistemas o modificar datos financieros.

**Amenazas Identificadas:**

- Empleado descontento por conflictos laborales
- Soborno por competidores o cibercriminales
- Acceso persistente de ex-empleados (credenciales no revocadas)

**Vulnerabilidades:**

- Sin implementación de principio de mínimo privilegio
- No hay auditoría de acciones de usuarios privilegiados
- Credenciales compartidas entre múltiples administradores
- Falta de segregación de funciones (SoD)

**Probabilidad:** MEDIA (35%)

- Historial de rotación de personal técnico
- Sector tecnológico con tensiones laborales ocasionales

**Impacto:** ALTO

- **Financiero:** Fraude potencial en promociones/descuentos
- **Operacional:** Sabotaje de sistemas críticos
- **Legal:** Dificultad para demostrar responsabilidad sin auditoría

**Nivel de Riesgo:** ALTO (Probabilidad MEDIA × Impacto ALTO)

---

**Riesgo 2.2: Errores Humanos en Configuración de Seguridad**

**Descripción:** Personal técnico comete errores al configurar firewalls, bases de datos o permisos, dejando sistemas expuestos sin intención maliciosa.

**Amenazas Identificadas:**

- Falta de capacitación técnica actualizada
- Presión por deadlines que lleva a atajos
- Rotación de personal sin documentación adecuada

**Vulnerabilidades:**

- Sin proceso formal de change management
- Configuraciones no revisadas por pares
- Documentación técnica desactualizada o inexistente
- Sin herramientas de validación automática de configuraciones seguras

**Probabilidad:** ALTA (60%)

- Errores humanos son la causa #1 de incidentes según Verizon DBIR
- 3A tiene personal junior en roles críticos

**Impacto:** MEDIO-ALTO

- **Operacional:** Exposición accidental de servicios a internet
- **Seguridad:** Bases de datos sin cifrar, puertos abiertos innecesarios
- **Financiero:** Costo de remediar configuraciones inseguras

**Nivel de Riesgo:** ALTO (Probabilidad ALTA × Impacto MEDIO-ALTO)

---

**Riesgo 2.3: Ingeniería Social y Phishing Interno**

**Descripción:** Atacantes externos engañan a empleados mediante correos fraudulentos, llamadas falsas (vishing) o mensajes de texto (smishing) para obtener credenciales o instalar malware.

**Amenazas Identificadas:**

- Campañas de phishing cada vez más sofisticadas
- Spoofing de correos de gerencia solicitando transferencias urgentes
- Fake IT support solicitando credenciales

**Vulnerabilidades:**

- Sin capacitación en concientización de seguridad
- No hay simulacros de phishing
- Ausencia de banner de advertencia en correos externos
- MFA no implementado en cuentas corporativas

**Probabilidad:** ALTA (65%)

- 85% de brechas comienzan con phishing exitoso
- Empleados sin entrenamiento son objetivo fácil

**Impacto:** ALTO

- **Acceso Inicial:** Compromiso de credenciales abre puerta a ataques mayores
- **Financiero:** Fraudes por transferencias engañosas (BEC - Business Email Compromise)

- **Operacional:** Instalación de malware que compromete sistemas

**Nivel de Riesgo:** CRÍTICO (Probabilidad ALTA × Impacto ALTO)

---

### Categoría 3: Riesgos de Infraestructura y Disponibilidad

#### Riesgo 3.1: Fallo de Infraestructura Sin Plan de Recuperación

**Descripción:** Fallo de hardware crítico (servidor de BD, storage, routers) o desastre natural (terremoto, inundación en datacenter) deja sistemas inoperables sin capacidad de recuperación rápida.

**Amenazas Identificadas:**

- Terremotos en Lima (alta sismicidad)
- Incendios en datacenter
- Fallo de discos duros sin redundancia
- Cortes eléctricos prolongados sin UPS suficiente

**Vulnerabilidades:**

- Backups no probados regularmente (último test: 18 meses atrás)
- Sin datacenter secundario para alta disponibilidad
- RTO/RPO no definidos formalmente
- Sin virtualización que permita migración rápida

**Probabilidad:** MEDIA (30%)

- Perú es zona sísmica, pero infraestructura en Lima relativamente estable
- Hardware empresarial con baja tasa de fallo

**Impacto:** CRÍTICO

- **Operacional:** Paralización total hasta recuperar infraestructura (días/semanas)
- **Financiero:** Pérdida de ingresos + costo de hardware nuevo
- **Contractual:** Incumplimiento de SLA con Grupo AJE

**Nivel de Riesgo:** ALTO (Probabilidad MEDIA × Impacto CRÍTICO)

---

#### Riesgo 3.2: Pérdida de Datos por Backups Inadecuados

**Descripción:** Los backups existentes fallan al momento de restaurar por corrupción de datos, proceso incompleto o cifrado por ransomware.

**Amenazas Identificadas:**

- Ransomware que cifra también los backups en red
- Corrupción silenciosa de archivos de backup
- Error humano en proceso de backup

**Vulnerabilidades:**

- Backups almacenados en la misma red que sistemas productivos
- Sin backups inmutables (air-gapped)
- Proceso de backup no monitoreado adecuadamente
- Sin cifrado de backups (riesgo si son robados físicamente)

**Probabilidad:** MEDIA (40%)

- Muchas empresas descubren que backups no funcionan cuando los necesitan
- 3A no prueba restauraciones regularmente

**Impacto:** CRÍTICO

- **Datos:** Pérdida permanente de información histórica
- **Operacional:** Imposibilidad de recuperar sistemas post-incidente
- **Legal:** Incumplimiento de obligación de preservar datos

**Nivel de Riesgo:** ALTO (Probabilidad MEDIA × Impacto CRÍTICO)

---

## Categoría 4: Riesgos de Cumplimiento y Legal

### Riesgo 4.1: Incumplimiento de Ley de Protección de Datos Personales

**Descripción:** 3A procesa datos personales sin cumplir requisitos legales (consentimiento, medidas de seguridad, registro ante autoridad), resultando en sanciones y demandas.

**Amenazas Identificadas:**

- Auditorías sorpresa de autoridad regulatoria
- Denuncias de consumidores o empleados
- Activismo digital exigiendo transparencia

**Vulnerabilidades:**

- Sin registro formal como banco de datos personales
- Ausencia de políticas de privacidad claras
- No hay proceso de consentimiento informado documentado
- Datos personales sin cifrado

**Probabilidad:** MEDIA (45%)

- Enforcement de ley ha aumentado en Perú últimos años
- Sector tecnológico bajo escrutinio creciente

**Impacto:** ALTO

- **Legal:** Multas de hasta 100 UIT (~\$115,000 USD)
- **Reputacional:** Publicación de sanción en medios
- **Operacional:** Obligación de suspender procesamiento de datos hasta cumplir

**Nivel de Riesgo:** ALTO (Probabilidad MEDIA × Impacto ALTO)

---

## Riesgo 4.2: Falta de Certificación PCI DSS

**Descripción:** 3A procesa pagos con tarjeta sin cumplir estándares PCI DSS, exponiendo a clientes a fraude y a la empresa a sanciones de procesadores de pago.

### Amenazas Identificadas:

- Auditoría de Visa/Mastercard o bancos emisores
- Fraude con tarjetas por datos robados
- Terminación de capacidad de procesar tarjetas

### Vulnerabilidades:

- Datos de tarjetas no tokenizados adecuadamente
- Red de POS no segmentada de red corporativa
- Sin cifrado end-to-end en transacciones
- No hay auditorías anuales PCI DSS

### Probabilidad: ALTA (55%)

- Requisito contractual con procesadores de pago
- Tendencia a enforcement más estricto

### Impacto: CRÍTICO

- **Operacional:** Pérdida de capacidad de procesar tarjetas = cierre de negocio
- **Legal:** Multas de hasta \$500,000 USD por incumplimiento
- **Financiero:** Responsabilidad por fraudes (~\$50-\$100 por transacción fraudulenta)

### Nivel de Riesgo: CRÍTICO (Probabilidad ALTA × Impacto CRÍTICO)

---

## Categoría 5: Riesgos de Cadena de Suministro

### Riesgo 5.1: Vulnerabilidades en Dependencias de Software

**Descripción:** Bibliotecas open source o componentes de terceros utilizados en el sistema POS contienen vulnerabilidades conocidas (CVEs) que atacantes pueden explotar.

### Amenazas Identificadas:

- Vulnerabilidades críticas como Log4Shell (CVE-2021-44228)
- Supply chain attacks como Codecov, SolarWinds
- Malware en paquetes NPM, PyPI comprometidos

### Vulnerabilidades:

- Sin inventario de dependencias (SBOM - Software Bill of Materials)
- No hay escaneo automatizado de vulnerabilidades
- Proceso lento de actualización de librerías
- Uso de versiones legacy sin soporte

**Probabilidad:** MEDIA (50%)

- Vulnerabilidades en open source se descubren constantemente
- 3A usa múltiples librerías sin auditoría

**Impacto:** ALTO

- **Seguridad:** Explotación remota de código (RCE)
- **Operacional:** Necesidad de parches urgentes que interrumpen desarrollo
- **Reputacional:** Asociación con incidentes públicos (ej. si usan Log4J vulnerable)

**Nivel de Riesgo:** ALTO (Probabilidad MEDIA × Impacto ALTO)

Resumen: Matriz de Riesgos Priorizados

ID	Riesgo	Probabilidad	Impacto	Nivel	Prioridad
1.1	Ransomware	ALTA (70%)	CRÍTICO	CRÍTICO	1
4.2	Incumplimiento PCI DSS	ALTA (55%)	CRÍTICO	CRÍTICO	2
2.3	Phishing/Ingeniería Social	ALTA (65%)	ALTO	CRÍTICO	3
1.3	SQL Injection	MEDIA (50%)	CRÍTICO	CRÍTICO	4
2.2	Errores Humanos	ALTA (60%)	MEDIO-ALTO	ALTO	5
3.1	Fallo de Infraestructura	MEDIA (30%)	CRÍTICO	ALTO	6
3.2	Pérdida de Datos	MEDIA (40%)	CRÍTICO	ALTO	7
1.2	Ataques DDoS	MEDIA (40%)	ALTO	ALTO	8
2.1	Abuso de Privilegios	MEDIA (35%)	ALTO	ALTO	9
4.1	Incumplimiento Ley Datos	MEDIA (45%)	ALTO	ALTO	10
5.1	Vulnerabilidades Dependencias	MEDIA (50%)	ALTO	ALTO	11

Bibliografía

1. **ISO/IEC 27001:2022** - Information Security Management Systems - Requirements. International Organization for Standardization.
2. **PCI Security Standards Council** (2024). *Payment Card Industry Data Security Standard v4.0*. <https://www.pcisecuritystandards.org/>
3. **Congreso de la República del Perú** (2011). *Ley N° 29733 - Ley de Protección de Datos Personales*. El Peruano.
4. **Verizon** (2024). *Data Breach Investigations Report*. Verizon Business.
5. **OWASP Foundation** (2021). *OWASP Top Ten Web Application Security Risks*. <https://owasp.org/www-project-top-ten/>

6. **NIST** (2018). *Framework for Improving Critical Infrastructure Cybersecurity v1.1*. National Institute of Standards and Technology.
7. **MITRE ATTACK** (2024). *MITRE ATTACK Framework for Enterprise*. <https://attack.mitre.org/>
8. **Zapata León, Christian** (2025). *Apuntes del curso Seguridad Informática I*. Universidad Peruana de Ciencias Aplicadas.
9. **CyberArk** (2024). *Privileged Access Management Best Practices*. CyberArk Software Ltd.
10. **Gartner** (2024). *Market Guide for Security Information and Event Management*. Gartner, Inc.