# Reporte ejecutivo del desarrollo del SGSI de la Marina

*Reporte ejecutivo*

Domicilio:

- Sucursales:
  - Colima, Col.
  - Manzanillo, Col.

Teléfono: 800 232 1212

Sitio web: https://www.lamarina.com.mx/

Correo: contacto.enlinea@lamarina.com.mx


Elaborado por equipo de “BoostTI”:

Gabriela Guzman Castillo
Denisse Solorzano Perez
Diego Fernando Verduzco Castillo


27 de Noviembre del 2025

# 1. - Objetivo del proyecto:

El objetivo del proyecto es optimizar los procesos de gestión tecnológica en la empresa "*La Marina"* mediante la implementación de prácticas de **Gobernanza Corporativa** y de la **Gestión de TI**. Con ello se busca alinear las decisiones tecnológicas con los objetivos estratégicos del negocio, mejorar la eficiencia operativa, fortalecer la seguridad de la información y asegurar un uso responsable y sostenible de los recursos tecnológicos.

### Gobernanza Corporativa:

Hoy en día, "*La Marina"* enfrenta problemas que reflejan **falta de dirección clara y supervisión estratégica**, por ejemplo:

- El proceso engorroso para solicitar una tarjeta de crédito contradice su misión de "satisfacer con excelencia".

- La poca variedad de productos y la mala organización logística limitan la competitividad frente a otras cadenas.

- La experiencia omnicanal prometida en la visión no se cumple: la web es deficiente y las sucursales trabajan de forma desconectada.

La **Gobernanza Corporativa** ayudaría a:

- **Definir políticas claras** de innovación y servicio al cliente que eviten procesos burocráticos innecesarios.
- **Establecer un consejo estratégico** que supervise proyectos de TI y logística, asegurando que realmente apoyen la visión omnicanal.
- **Implementar mecanismos de rendición de cuentas** para directivos y áreas responsables, de manera que no existan incoherencias como la negativa de trasladar productos entre sucursales.

## Gestión de TI:

El desarrollo digital de La Marina comenzó durante la pandemia y ha evolucionado con funcionalidades personalizadas, para ofrecer una experiencia de compra fluida y atractiva.

### 1. Ecommerce con VTEX

La Marina utiliza la plataforma **VTEX** para su tienda en línea, lo que le permite operar como un marketplace omnicanal. Esto les ha permitido:

- Aumentar sus ventas hasta en un **600 %** con el marketplace (Del 2020 al 2025).
- Generar **30 % de ingresos** vía **Social Selling** (ventas a través de redes sociales) y **40 % de sus ingresos totales** provienen del marketplace.

### 2. Canal omnicanal y servicios complementarios

La Marina ha consolidado una estrategia de **venta omnicanal**, combinando la experiencia en tienda física con funcionalidades en línea como:

- **Clic & Recoge**: compra en línea y recogida en tienda.
- Compra por teléfono y por WhatsApp

# 2. - El organigrama (General y/o regional)

Un **organigrama** es una representación gráfica de la estructura de una organización. Muestra cómo se distribuyen las funciones, quién depende de quién y cómo fluye la comunicación dentro de la empresa u organización.

**Organigrama general:**
Representa toda la estructura de la empresa a nivel corporativo o matriz. Muestra desde la alta dirección hasta las diferentes divisiones, sucursales o departamentos.

**Organigrama regional:**
Es más específico y se enfoca en una **zona geográfica o sucursal**, como una tienda o centro de operaciones en una ciudad o estado en particular (por ejemplo, Colima).

**Organigrama General (Corporativo)**

- Subdirección Administrativa
- Subdirección Comercial
- Subdirección de Recursos Humanos
- Subdirección de Operaciones
- Subdirección de Marketing
- Departamento Legal
- Departamento de Tecnología

**Organigrama Regional (Sucursal Colima):**

**1. Gerente de Sucursal (Colima)**

- Reporta a la Dirección de Operaciones general.

**2. Subgerente de Sucursal**

- Apoya en supervisión diaria y control operativo.

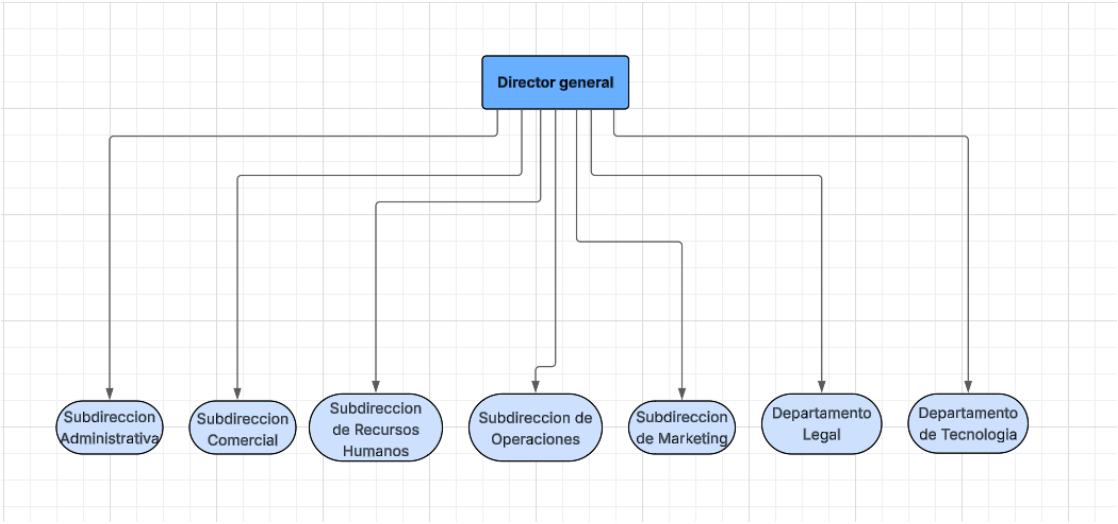
**3. Jefes de Departamento:**

- Jefe de Ventas
- Jefe de Almacén
- Jefe de Caja
- Jefe de Recursos Humanos (local)
- Jefe de Seguridad

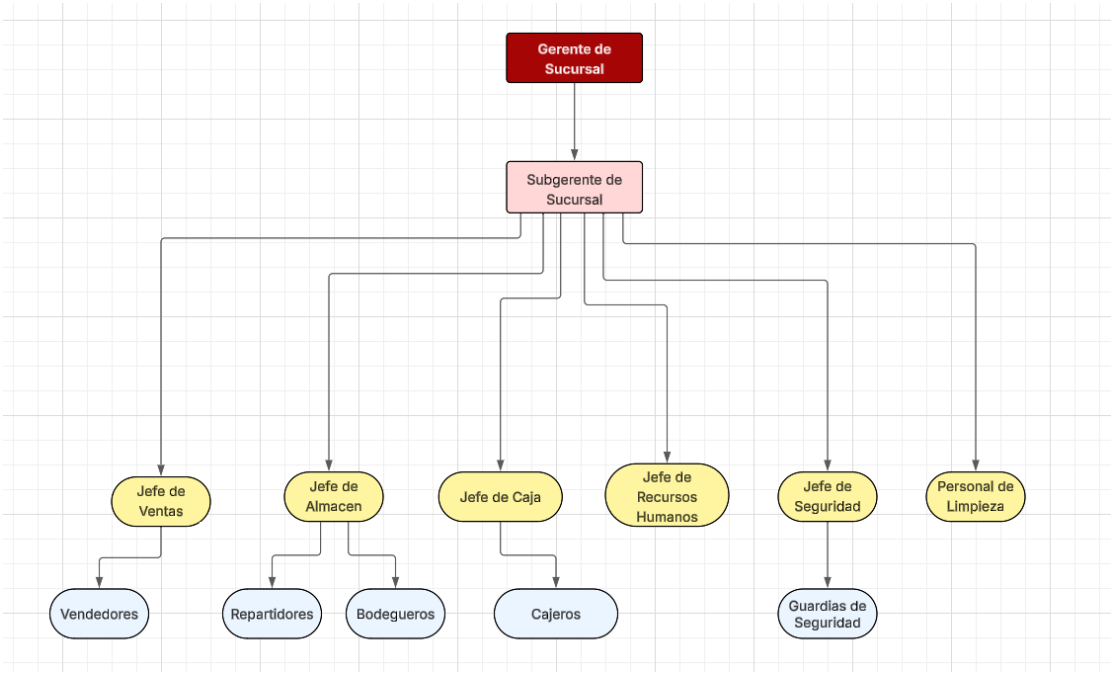
**4. Personal Operativo:**

- Cajeros
- Vendedores
- Repartidores
- Bodegueros
- Personal de Limpieza
- Guardias de Seguridad

**Organigrama General:**



## Organigrama Regional:

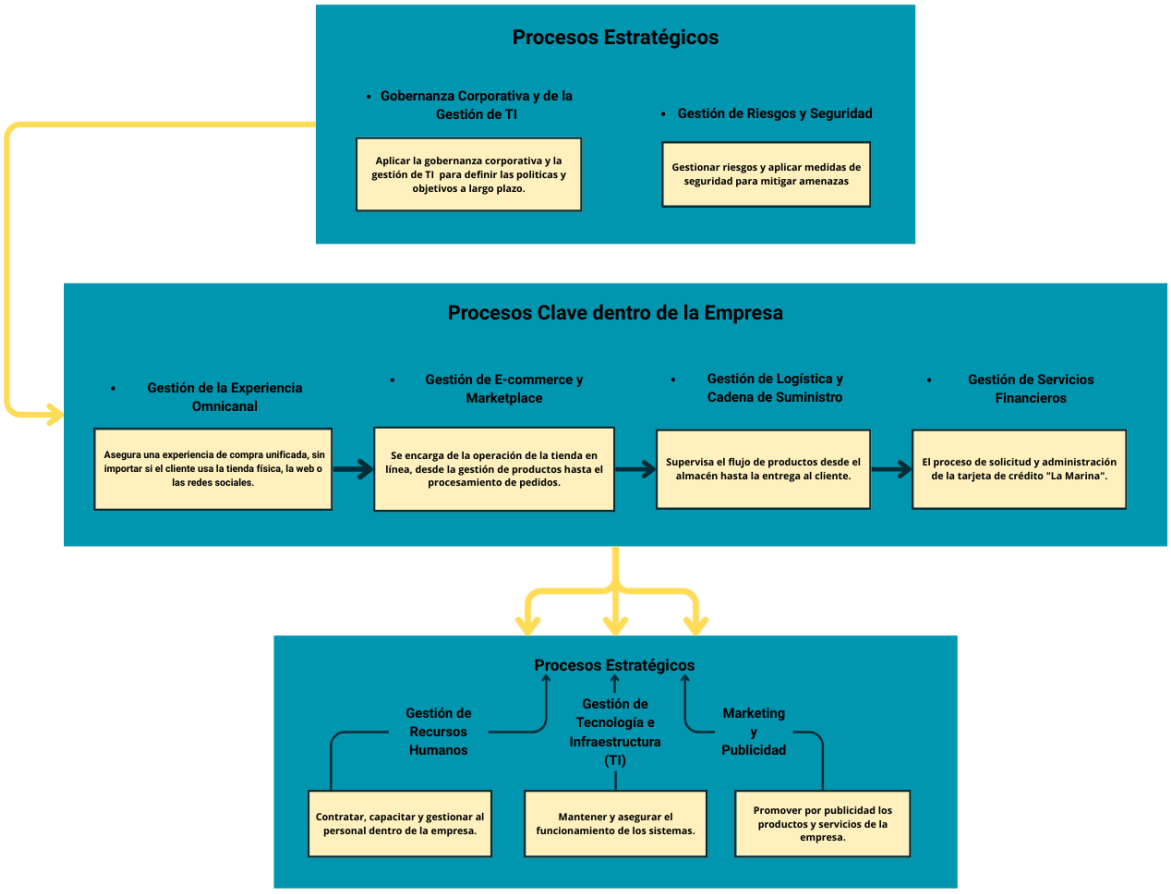


# 3. - Mapa de procesos identificando al menos los 4 procesos claves:

El mapa de procesos es una herramienta que nos permite visualizar de manera sencilla cómo se organiza y funciona una empresa, mostrando la relación entre sus áreas y las actividades que realizan.

En el caso de “La Marina”, este mapa nos podrá ayudar a reconocer los procesos que hoy en día presentan deficiencias, como la logística, la atención al cliente y la gestión tecnológica, y de esta manera poder mejorarlos.

**El mapa de procesos aplicado a “La Marina”:**



# 4. - Cédula de Procesos:

## Gestión de la Experiencia Omnicanal

- **Objetivo:** Ofrecer una experiencia de compra fluida y consistente para el cliente en todos los puntos de contacto (tienda física, web, app y redes sociales).
- **Propietario del Proceso:** Gerente de Operaciones Omnicanal.
- **Entradas:**
    - Datos del cliente (historial, preferencias).
    - Inventario de productos en tiempo real.
    - Promociones y precios unificados.
- **Salidas:**
    - Cliente satisfecho.
    - Ventas consolidadas.
    - Análisis de datos de comportamiento del cliente.
- **Procedimientos:**
    - **Sincronización de Inventario:** Mantener el inventario en línea y en tienda actualizado para evitar ventas de productos agotados.
    - **Unificación de Precios y Promociones:** Asegurar que los precios y las ofertas sean los mismos en todos los canales.
    - **Gestión de Clic & Recoge:** Procedimiento para que el cliente compre en línea y recoja su pedido en una sucursal, incluyendo la notificación de que el pedido está listo.
    - **Gestión de Devoluciones:** Procedimiento para procesar devoluciones sin importar dónde se realizó la compra.
- **Indicadores de Desempeño:**
    - Tasa de satisfacción del cliente omnicanal.
    - Tiempo promedio para completar un pedido de "Clic & Recoge".
    - Porcentaje de ventas que provienen de múltiples canales.

### Cédula de Procesos: Gestión de E-commerce y Marketplace

- **Objetivo:** Optimizar la operación de la plataforma de venta en línea, desde la UX/UI, la publicación de productos y la confirmación de la entrega.
- **Propietario del Proceso:** Gerente de E-commerce.
- **Entradas:**
    - Catálogo de productos (descripciones, imágenes, precios).

    - Pedidos de clientes en línea.
    - Datos de inventario de proveedores.
- **Salidas:**
    - Pedidos procesados y pagados.
    - Órdenes de preparación para logística.
    - Confirmación de envío para el cliente.
- **Procedimientos:**
    - **Publicación de Productos:** Cargar y actualizar productos en la plataforma VTEX, incluyendo descripciones, imágenes y precios.
    - **Procesamiento de Pedido en Línea:** El sistema recibe el pedido, verifica el pago y la disponibilidad del producto.
    - **Comunicación con el Cliente:** Enviar notificaciones automáticas por correo, WhatsApp o SMS sobre el estado del pedido.
    - **Gestión de Ventas en Redes Sociales (Social Selling):** Procedimientos para procesar pedidos iniciados a través de plataformas como Facebook o Instagram.
- **Indicadores de Desempeño:**
    - Tasa de conversión de ventas en línea.
    - Tiempo promedio de procesamiento de pedidos.
    - Porcentaje de pedidos sin errores.

**Cédula de Procesos: Gestión de Logística y Cadena de Suministro**

- **Objetivo:** Asegurar que los productos estén disponibles y sean entregados de manera eficiente a los clientes, optimizando el flujo desde el almacén hasta el punto final de entrega.
- **Propietario del Proceso:** Gerente de Operaciones y Logística.
- **Entradas:**
    - Órdenes de compra.
    - Productos de proveedores.
    - Pedidos en línea y de tiendas físicas.
- **Salidas:**
    - Productos en inventario.
    - Entregas a tiempo.
    - Datos de seguimiento de envíos.
- **Procedimientos:**
    - **Recepción y Almacenamiento:** Procedimiento para recibir, verificar y almacenar los productos de los proveedores.

    - **Preparación de Pedidos (Picking y Packing):** Proceso de seleccionar los productos del almacén y empaquetarlos para su envío.
    - **Coordinación de Transporte:** Organizar la distribución de productos a las tiendas o directamente a los clientes, asegurando que se cumplan los tiempos de entrega.
    - **Gestión de Inventarios:** Monitorear los niveles de stock para evitar desabastecimientos o excesos de inventario.
- **Indicadores de Desempeño:**
    - Tiempo promedio de entrega.
    - Precisión de inventario.
    - Costos de envío por pedido.

**Cédula de Procesos: Gestión de Servicios Financieros (Tarjeta de Crédito)**

- **Objetivo:** Simplificar y optimizar el proceso de solicitud, aprobación y administración de la tarjeta de crédito "La Marina" para mejorar la experiencia del cliente y la rentabilidad del servicio.
- **Propietario del Proceso:** Gerente de Servicios Financieros.
- **Entradas:**
    - Solicitudes de tarjeta de crédito (datos del cliente).
    - Información de historial crediticio.
- **Salidas:**
    - Aprobaciones o rechazos de solicitudes.
    - Emisión de tarjetas de crédito.
    - Facturas y estados de cuenta.
- **Procedimientos:**
    - **Recepción de Solicitud:** Recibir y digitalizar las solicitudes de tarjeta de crédito (en línea o en tienda).
    - **Evaluación de Crédito:** Analizar la información del cliente y su historial para determinar la elegibilidad.
    - **Aprobación y Emisión:** Aprobar la solicitud y proceder a la emisión y envío de la tarjeta al cliente.
    - **Gestión de Facturación y Pagos:** Generar y enviar estados de cuenta y gestionar los pagos de los clientes.
- **Indicadores de Desempeño:**
    - Tiempo promedio de aprobación de solicitud.
    - Porcentaje de solicitudes aprobadas.
    - Tasa de morosidad.

# 5. - Matriz RACI

**Encargado de Tecnología:** Responsable de la infraestructura digital (E-commerce, integraciones).

**Encargado de Marketing:** Responsable de campañas y comunicación omnicanal.

**Encargado de Recursos Humanos (RH):** No ejecuta procesos clave aquí, pero informa y apoya en gestión de personal.

**Encargado de Ventas:** Responsable de contacto con clientes y servicios financieros.

**Encargado de Almacén:** Responsable directo de inventarios y flujo de productos.

**Encargado de Operaciones:** Supervisa, aprueba y asegura que todo funcione de manera integrada.


| Rol | Integrante |
|---|---|
| Encargado de Tecnología | Denisse Monserrat Solorzano Perez |
| Encargado de Marketing | Diego Fernando Verduzco Castillo |
| Encargado de RH | Gabriela Guzmán Castillo |

| | |
|---|---|
| Encargado de Ventas | Denisse Monserrat Solorzano Perez |
| Encargado de Almacén | Diego Fernando Verduzco Castillo |
| Encargado de Operaciones | Gabriela Guzmán Castillo |

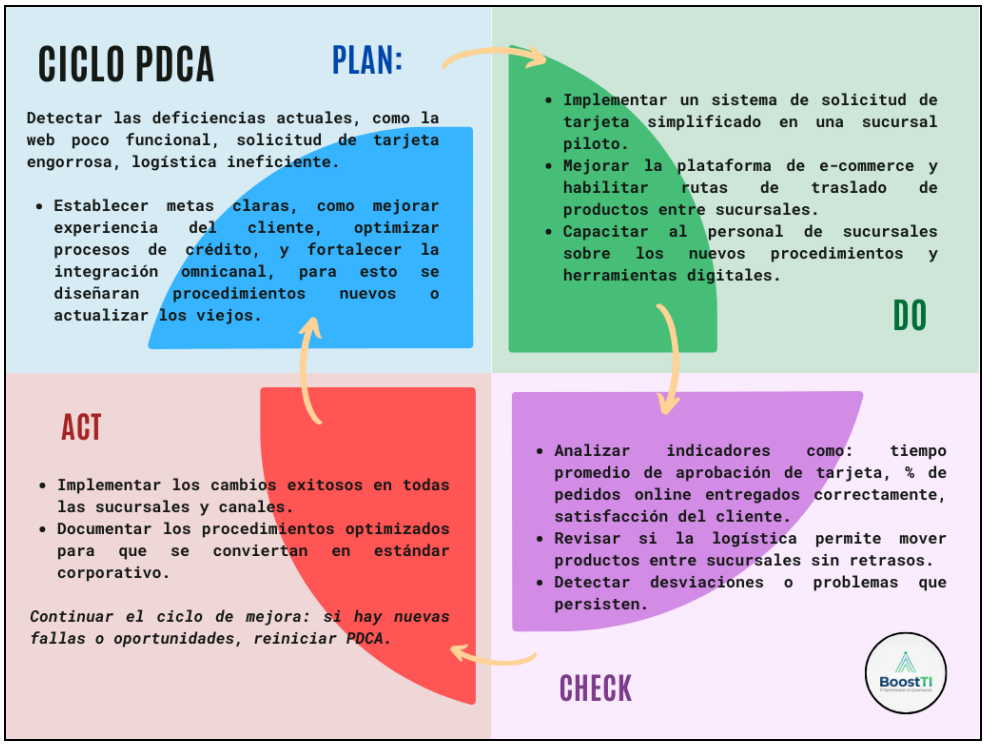
# 6. - Plan PHVA (PDCA) – Proyecto “La Marina”

El ciclo PDCA busca la mejora continua de procesos, productos o servicios, desglosando la resolución de problemas en cuatro etapas clave: identificar un problema y plantear una solución, ejecutar el plan a pequeña escala, evaluar los resultados obtenidos y, finalmente, actuar para estandarizar la mejora o ajustar el plan e iniciar un nuevo ciclo.

Se divide en 4 etapas:

- **Plan:** Se definen los objetivos,se identifican problemas y se establecen estrategias para mejorar procesos.
- **Do:** Se implementan los planes diseñados en la fase anterior, de manera piloto o completa.
- **Check:** Medimos y evaluamos los resultados obtenidos, comparándolos con los objetivos planeados.
- **Act:** Se ajustan, corrigen y estandarizan las mejoras obtenidas.

**El ciclo PDCA aplicado a “La Marina”:**



# 7. - Políticas Corporativas de Seguridad

**1. Política de Innovación y Transformación Digital:**

La empresa fomentará la adopción de tecnologías digitales y prácticas innovadoras que mejoren la experiencia omnicanal, aseguren la competitividad y permitan ofrecer un servicio eficiente y moderno a los clientes.

**2. Política de Seguridad de la Información (SGSI)**

Toda la información, en especial la relacionada con clientes, transacciones y datos financieros, deberá ser protegida bajo principios de confidencialidad, integridad y disponibilidad, aplicando medidas como cifrado, control de accesos, autenticación segura y auditorías periódicas.

**3. Política de Transparencia y Rendición de Cuentas**

Directivos, gerentes y responsables de área deberán rendir cuentas de sus decisiones y resultados. Toda acción o proyecto debe estar alineado con la visión corporativa y será monitoreado con indicadores de desempeño claros.

**4. Política de Protección de Datos del Cliente**

Los datos personales y financieros de los clientes deberán tratarse de forma legal, ética y segura, cumpliendo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y estándares internacionales.

**5. Política de Seguridad en E-commerce y Omnicanalidad**

Las plataformas de venta en línea, marketplace y servicios omnicanal deberán implementar certificados de seguridad, cifrado de transacciones, monitoreo de fraudes y pruebas periódicas de vulnerabilidad.

**6. Política de Capacitación y Concientización**

Todos los colaboradores deberán recibir formación continua en ciberseguridad, mejores prácticas en TI y protección de la información, fomentando una cultura organizacional orientada a la seguridad.

# 8. - Matriz de riesgos de “La Marina” (consecuencia y probabilidad):

Como parte del desarrollo inicial del Sistema de Gestión de Seguridad de la Información (SGSI) de *La Marina*, se elaboró una **primera matriz de riesgos** con el objetivo de identificar las principales amenazas que podrían comprometer la continuidad operativa, los datos de clientes y los servicios omnicanal de la empresa.

La matriz de riesgo para La Marina se desarrolló mediante un análisis cualitativo

basado en:

- Revisión de procesos clave: Se identificaron los cuatro procesos críticos documentados: Gestión de Experiencia Omnicanal, E-commerce y Marketplace, Logística y Cadena de Suministro, y Servicios Financieros.
- Análisis de vulnerabilidades: Se evaluaron los problemas identificados en el documento: procesos burocráticos, desconexión entre canales, falta de dirección clara y supervisión estratégica.
- Identificación de fuentes de riesgo: Considerando tecnología, operaciones, financiero, legal y reputacional.
- Valoración probabilidad-impacto: Combinación de probabilidad de ocurrencia e impacto potencial en el negocio usando la matriz de referencias de 1 a 80.

Criterios de Análisis:

- Análisis por áreas de riesgo: Tecnología e infraestructura, Procesos operacionales, Seguridad de información, Gestión financiera, y Gobernanza corporativa.
- Contexto empresarial: Se consideró que La Marina es una cadena retail con operaciones omnicanal, dependencia de plataformas como VTEX, múltiples sucursales, y servicios financieros asociados.
- Severidad potencial: Evaluando tanto el impacto inmediato como el daño a largo plazo en reputación, financieros y operacionales.

Métrica de matriz de riesgos:

| | | MATRIZ DE RIESGOS | | | | |
|---|---|---|---|---|---|---|
| | | Consecuencia | | | | |
| | | Minima | Menor | Moderada | Mayor | Maxima |
| Probabilidad | | 1 | 2 | 4 | 8 | 16 |
| Muy Alta | 5 | 5 | 10 | 20 | 40 | 80 |
| Alta | 4 | 4 | 8 | 16 | 32 | 64 |
| Media | 3 | 3 | 6 | 12 | 24 | 48 |
| Baja | 2 | 2 | 4 | 8 | 16 | 32 |
| Muy Baja | 1 | 1 | 2 | 4 | 8 | 16 |

| Nivel de riesgo | Color |
|---|---|
| Riesgo aceptable | |
| Riesgo tolerable | |
| Riesgo alto | |
| Riesgo extremo | |

Matriz de riesgo - La Marina:

| Evento | Descripcion | Probabilidad | Consecuencia | Nivel de Riesgo | Calificacion |
|---|---|---|---|---|---|
| Fallo en plataforma VTEX | Indisponibilidad de tienda en línea que genera una significante parte de los ingresos | Baja | Maxima | Riesgo extremo | 32 |
| Incidente de seguridad de datos | Brechas en datos de clientes, tarjetas de crédito o transacciones financieras | Media | Maxima | Riesgo extremo | 48 |
| Desincronización de inventarios | Inconsistencia entre tienda física y en línea genera pedidos no entregables | Media | Mayor | Riesgo alto | 24 |
| Fraude en tarjeta de crédito | Fraude electrónico en solicitudes o transacciones de la tarjeta de "La Marina" | Baja | Maxima | Riesgo extremo | 32 |
| Falta de gobernanza corporativa | Decisiones desalineadas, falta de supervisión, procesos incoherentes | Media | Maxima | Riesgo extremo | 48 |
| Proceso de tarjeta engorroso | Solicitudes complejas y lentas afectan conversión y experiencia | Alta | Mayor | Riesgo extremo | 32 |
| Problemas en logística intersucursal | Negativa a trasladar productos entre sucursales, ineficiencia operativa | Alta | Mayor | Riesgo extremo | 32 |
| Ciberataques a infraestructura | DDoS, malware, ransomware afectando operaciones omnicanal | Baja | Maxima | Riesgo extremo | 32 |

| | | | | | |
|---|---|---|---|---|---|
| Desconexión entre canales | Sucursales trabajando de forma desconectada, falta de integración | Media | Moderada | Riesgo tolerable | 12 |
| Variabilidad en disponibilidad de productos | Poca variedad, desabastecimientos limitando competitividad | Muy Baja | Moderada | Riesgo aceptable | 4 |
| Deficiencia en aplicación web | Web lenta, con errores afectando experiencia del cliente | Muy Alta | Menor | Riesgo tolerable | 10 |
| Rotación de personal clave | Pérdida de expertise en tecnología, operaciones u omnicanal | Muy Alta | Mayor | Riesgo extremo | 40 |
| Pérdida de datos por falta de backup | Perder datos de importancia por no tener un registro diario de la informacion que entra y sale de la empresa | Baja | Moderada | Riesgo tolerable | 8 |
| Retraso en envíos | Retraso en entrega de paquetes | Muy Baja | Moderada | Riesgo aceptable | 4 |

En caso de que se presente un:

- Riesgo extremo:
  - **Acción requerida:** INMEDIATA Y URGENTE
  - **Mitigación crítica:** Implementar controles sin demora
- Riesgo alto:
  - **Acción requerida:** INMEDIATA
  - **Mitigación:** Controles robustos dentro de 1-2 meses
- Riesgo tolerable:
  - **Acción requerida:** PLANEADA
  - **Mitigación:** Controles en corto-mediano plazo
- Riesgo aceptable:
  - **Acción requerida:** RUTINARIA
  - **Mitigación:** Controles estándar y monitoreo

# 9. - Matriz de riesgos de “La Marina”

Como parte del desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI), se identificaron múltiples riesgos que afectan los procesos clave de la organización: e-commerce y marketplace, omnicanalidad, logística, servicios financieros y gobernanza corporativa. Estos riesgos se clasifican y analizan con base en los principios de ISO 27001, ISO 27005 y la Ley Federal de Protección de Datos Personales.

Cada riesgo se relaciona con los pilares de seguridad de la información: Confidencialidad (C), Integridad (I), Disponibilidad (D).

## Categorías generales de riesgo identificadas

### Riesgos Tecnológicos y de Infraestructura

- **Incluyen:** Fallo de la plataforma VTEX, indisponibilidad del sitio, ciberataques, pérdida de datos, falta de backups.
- **Impacto:**
  Afectan directamente la operación del negocio en línea. Si la plataforma VTEX o los sistemas API dejan de funcionar, la empresa pierde ventas, reputación y continuidad del servicio. En el contexto omnicanal, incluso una caída temporal afecta inventarios, pedidos, pagos y logística.

### Riesgos de Seguridad de la Información y Protección de Datos

- **Incluyen:** Fuga de datos, violación de privacidad, ataques de phishing, robo de identidad, filtraciones de datos financieros o personales.
- **Impacto:**
  Este tipo de riesgo no solo provoca daño operativo, sino **legal y reputacional**, ya que involucra la protección de datos personales y financieros. Puede ocasionar sanciones bajo la **Ley Federal de Protección de Datos Personales**, pérdida de confianza del cliente y daño reputacional grave.

## Riesgos Operativos y de Procesos

- **Incluyen**: desincronización de inventarios, retrasos en entregas, fallas logísticas, variabilidad en productos, problemas en la experiencia omnicanal.
- **Impacto**:
  Generan pérdida de clientes, reembolsos, retrasos, quejas y mala experiencia, afectando directamente las ventas y cumplimiento del negocio.

## Riesgos de Fraude Digital y Servicios Financieros

- **Incluyen:** fraude electrónico, robo de identidad, manipulación de solicitudes de crédito, chargebacks, solicitudes falsas.
- **Impacto:**
  Pérdidas económicas, problemas legales, y daños a la reputación del servicio financiero de la empresa.

## Riesgos de Gobernanza y Gestión Organizacional

- **Incluyen:** falta de supervisión estratégica, decisiones no alineadas, problemas entre áreas, procesos sin responsable.
- **Impacto:**
  No son técnicos, pero afectan **la integración del SGSI, la toma de decisiones y el cumplimiento de ISO 27001**. Si no hay claridad en roles, los riesgos no se gestionan adecuadamente.

## Riesgos:

- Fallo en la plataforma VTEX que provoca la indisponibilidad de la tienda en línea.
- Incidente de seguridad de datos (exposición de datos personales o financieros).

| BoostTI | Nombre | Clave | Edición | Fecha de implantación |
|---|---|---|---|---|
| | Matriz de Contexto y Gestión del Riesgo de "La Marina" | DCI-MCGR-01 | 04 | 17 de septiembre de 2018 |

| | | | |
|---|---|---|---|
| Unidad Organizacional: | Corporativo / Dirección General | Fecha de elaboración | |
| Proceso: | Gestión Integral de Riesgos | 26/11/2025 | |

| CONTEXTO DEL PROCESO | | | | | IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROBLEMAS Y OPORTUNIDADES IDENTIFICADAS A PARTIR DE LAS CUESTIONES INTERNAS Y EXTERNAS | TIPO: INTERNA / EXTERNA | PARTE INTERESADA | NECESIDADES/EXPECTATIVAS DE LAS PARTES INTERESADAS | TIPO: REQUISITO/ EXPECTATIVA | RIESGOS | INFORMACION QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE |
| Dependencia operativa de la plataforma VTEX para la disponibilidad de la tienda en línea. | Interna | - Clientes<br>- Área de eCommerce<br>- Ventas<br>- Dirección Comercial TI | Disponibilidad continua de la tienda estabilidad del servicio cumplimiento de ventas experiencia positiva del cliente. | E | **Fallo en la plataforma VTEX que provoca la indisponibilidad de la tienda en línea.** | | | x | Área de TI / Responsable de eCommerce | - Monitoreo básico de la tienda en línea<br>- Comunicación con VTEX cuando hay fallas<br>- Revisión periódica del SLA<br>- Reporte mensual de disponibilidad | 5 | 2 |
| Alta exposición a datos sensibles (clientes, tarjetas y transacciones) que requieren medidas estrictas de protección. | Interna | - Cliente final<br>- Área de TI de La Marina<br>- Departamento financiero<br>- eCommerce<br>- Proveedor de pagos | Protección de datos personales, prevención de fraudes, integridad de transacciones y cumplimiento normativo. | E | **Incidente de seguridad de datos (exposición de datos personales o financieros).** | x | x | | TI de BoostTI / Seguridad de la Información / eCommerce | - Autenticación básica.<br>- Monitoreo limitado.<br>- Proveedor de pagos con PCI-DSS.<br>- Políticas iniciales de privacidad. | 3 | 3 |

| Fecha de implantación | Fecha de revisión |
|---|---|
| 17 de septiembre de 2018 | 22 de agosto de 2023(Revisión del formato) |
| **Fecha de elaboración** | **Código de clasificación de documento** |
| 26/11/2025 | 11C.1.1/34200/105/2025 |

| EVALUACIÓN DEL RIESGO | | | | | | | TRATAMIENTO |
|---|---|---|---|---|---|---|---|
| N QUE TARSE: Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE | NIVEL DE RIESGO RESIDUAL | CONTROLES ADICIONALES | PLAN DE TRATAMIENTO (INDICAR OPCIÓN DE TRATAMIENTO ELEGIDA) |
| x | Área de TI / Responsable de eCommerce | - Monitoreo básico de la tienda en línea<br>- Comunicación con VTEX cuando hay fallas<br>- Revisión periódica del SLA<br>- Reporte mensual de disponibilidad | 5 | 2 | 10 | - Implementar monitoreo activo 24/7 con alertas<br>- Crear un procedimiento de contingencia para caídas de VTEX<br>- Establecer canales alternos de venta en emergencias<br>- Proporcionar reportes de rendimiento a La Marina | **Opción elegida: "Mitigar el riesgo".**<br>Debido al impacto extremo asociado a fuga de datos financieros y personales, no es posible aceptar, evitar ni retener el riesgo. La única opción viable es mitigarlo mediante controles avanzados de seguridad.<br>**Acciones del plan de tratamiento:**<br>Implementar un plan de continuidad para fallos en VTEX, reforzar el SLA con el proveedor, establecer mecanismos de contingencia para ventas, habilitar monitoreo activo y mantener alternativas de venta temporal en caso de caída.<br>**Evidencias esperadas:** Registros de monitoreo, reportes de pruebas de seguridad, bitácoras de incidentes, documentación actualizada del procedimiento, evidencia de capacitaciones. |
| | TI de BoostTI / Seguridad de la Información / eCommerce | - Autenticación básica.<br>- Monitoreo limitado.<br>- Proveedor de pagos con PCI-DSS.<br>- Políticas iniciales de privacidad. | 3 | 3 | 9 | A.5.14 – Protección de la información<br>A.5.15 – Control de acceso basado en privilegios<br>A.5.23 – Seguridad en servicios de la nube<br>A.8.7 – Protección contra malware<br>A.8.8 – Gestión de vulnerabilidades técnicas<br>A.8.9 – Registro de actividades (logs)<br>A.8.10 – Monitoreo<br>A.8.11 – Detección de incidentes<br>A.8.12 – Respuesta a incidentes<br>A.8.13 – Copias de seguridad<br>A.8.16 – Cifrado<br>A.5.36 – Obligaciones de privacidad y protección de datos/informacion | **Opción elegida: "Mitigar el riesgo".**<br>Debido al impacto extremo asociado a fuga de datos financieros y personales, no es posible aceptar, evitar ni retener el riesgo. La única opción viable es mitigarlo mediante controles avanzados de seguridad.<br>**Acciones del plan de tratamiento:**<br>BoostTI implementará un sistema avanzado de detección de incidentes, fortalecerá controles de cifrado, autenticación y monitoreo continuo, integrará validaciones antifraude y configurará alertas en tiempo real ante accesos y transacciones sospechosas. Se desarrollará un procedimiento formal de respuesta a incidentes y se realizarán pruebas periódicas de vulnerabilidades y de seguridad en aplicaciones.<br>**Evidencias esperadas:** Registros de monitoreo, reportes de pruebas de seguridad, bitácoras de incidentes, documentación actualizada del procedimiento, evidencia de capacitaciones. |

## Riesgos:

- Desincronización de inventarios entre canal físico y online.
- Fraude electrónico en solicitudes o transacciones de la tarjeta de "La Marina"
- Falta de gobernanza corporativa.

| CONTEXTO DEL PROCESO | | | | | IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROBLEMAS Y OPORTUNIDADES IDENTIFICADAS A PARTIR DE LAS CUESTIONES INTERNAS Y EXTERNAS | TIPO: INTERNA / EXTERNA | PARTE INTERESADA | NECESIDADES/EXPECTATIVAS DE LAS PARTES INTERESADAS | TIPO: REQUISITO/ EXPECTATIVA | RIESGOS | INFORMACIÓN QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE |
| Dependencia de múltiples sistemas de inventario que requieren sincronización continua entre tienda física y online. | Interna | - Clientes<br>- Área de ventas<br>- Logística<br>- eCommerce<br>- TI<br>- Sucursales físicas | Inventarios precisos, pedidos entregables, sincronización confiable entre canales y experiencia omnicanal consistente. | R | **Desincronización de inventarios entre canal físico y online.** | | x | | TI / Logística / eCommerce / BoostTI | - Sincronización programada.<br>- Monitoreo básico<br>- Revisión manual de inventarios<br>- Validación diaria en tiendas. | 4 | 3 |
| Transacciones financieras y solicitudes de tarjeta expuestas a intentos de fraude electrónico. | Externa | - Clientes<br>- Área financiera<br>- eCommerce<br>- TI<br>- Proveedor de pagos<br>- La Marina | Transacciones seguras, protección contra fraude, procesos confiables de solicitud y cargos correctos. | E | **Fraude electrónico en solicitudes o transacciones de la tarjeta de "La Marina"** | x | x | | Área financiera / Seguridad de la información / BoostTI / Proveedor de pagos | - Sistema antifraude básico del proveedor de pagos<br>- Verificación manual de transacciones.<br>- Autenticación estándar. | 5 | 2 |
| Ausencia de procesos claros, roles definidos y supervisión estructurada, lo que ocasiona decisiones desalineadas y falta de coherencia organizacional. | Interna | - Dirección General.<br>- Comité Directivo<br>- Seguridad de la Información<br>- Todas las áreas operativas<br>- BoostTI | Estructura de gobierno clara, procesos formales, supervisión efectiva y toma de decisiones alineada con los objetivos estratégicos. | R | **Falta de gobernanza corporativa.** | | x | | Dirección General / Comité Directivo / Seguridad de la Información / BoostTI | - Juntas ejecutivas esporádicas<br>- Políticas básicas no estandarizadas<br>- Procesos definidos de manera informal<br>- Comunicación interna mínima. | 5 | 3 |

| IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | | | TRATAMIENTO |
|---|---|---|---|---|---|---|---|---|---|
| RIESGOS | INFORMACIÓN QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE | NIVEL DE RIESGO RESIDUAL | CONTROLES ADICIONALES | PLAN DE TRATAMIENTO (INDICAR OPCIÓN DE TRATAMIENTO ELEGIDA) |
| **Desincronización de inventarios entre canal físico y online.** | | x | | TI / Logística / eCommerce / BoostTI | - Sincronización programada.<br>- Monitoreo básico<br>- Revisión manual de inventarios<br>- Validación diaria en tiendas. | 4 | 3 | 12 | A.5.12 —Clasificación de la informaciónn<br>A.8.16 — Seguimiento de actividades<br>A.5.23 — Seguridad en servicios en la nube (si los sistemas se integran por API)<br>A.8.8 — Gestión de vulnerabilidades (si la falla es técnica)<br>A.8.32 — Gestión de cambios<br>A.5.32 — Relaciones con proveedores (si inventarios dependen de terceros)<br>A.5.20 — Diseño seguro de sistemas<br>A.8.12 — Respuesta a incidentes (para errores masivos de inventario) | **Opción elegida: "Modificar la probabilidad y el impacto del riesgo".**<br>Este riesgo no puede evitarse porque forma parte natural de la operación omnicanal, pero sí puede reducirse mediante controles automáticos de integridad y sincronización.<br>**Acciones del plan de tratamiento:**<br>BoostTI implementará validaciones automáticas entre sistemas, monitoreo en tiempo real, alertas por inconsistencias, estandarización del flujo de actualización y pruebas periódicas de sincronización. Se reforzará la gestión de cambios y se documentarán procesos logísticos para evitar errores manuales.<br>**Evidencias esperadas:** Logs de sincronización, dashboards de monitoreo, reportes de inconsistencias corregidas, documentación de procesos, evidencia de pruebas. |
| **Fraude electrónico en solicitudes o transacciones de la tarjeta de "La Marina"** | x | x | | Área financiera / Seguridad de la información / BoostTI / Proveedor de pagos | - Sistema antifraude básico del proveedor de pagos<br>- Verificación manual de transacciones.<br>- Autenticación estándar. | 5 | 2 | 10 | A.5.14 — Transferencia de la información<br>A.5.15 — Control de acceso<br>A.8.7 — Protección contra código malicioso<br>A.8.8 — Gestión de vulnerabilidades<br>A.8.11 — Identificación de incidentes<br>A.5.24 — Planificación y preparación de la gestión de incidentes de seguridad de información.<br>A.5.34 — Privacidad y protección de datos de carácter personal (DCP)<br>A.5.23 — Seguridad en servicios en la nube (pasarela, API) | **Opción elegida: "Mitigar el riesgo".**<br>El fraude financiero tiene impacto extremo legal, económico y reputacional, por lo que debe mitigarse aplicando controles antifraude y seguridad reforzada.<br>**Acciones del plan de tratamiento:**<br>BoostTI implementará sistemas avanzados de detección antifraude, doble autenticación, monitoreo continuo de transacciones, validaciones reforzadas en solicitudes y generación de alertas automáticas. Se reforzará el cifrado y los registros de auditoría y se verificará el cumplimiento con PCI-DSS.<br>**Evidencias esperadas:** Logs de transacciones, reportes de fraude detectado, diagnósticos PCI-DSS, documentación de controles, registros de monitoreo. |
| **Falta de gobernanza corporativa.** | | x | | Dirección General / Comité Directivo / Seguridad de la Información / BoostTI | - Juntas ejecutivas esporádicas<br>- Políticas básicas no estandarizadas<br>- Procesos definidos de manera informal<br>- Comunicación interna mínima. | 5 | 3 | 15 | A.5.1 — Políticas de seguridad de la información<br>A.5.2 — Roles y responsabilidades en seguridad<br>A.5.3 — Segregación de tareas<br>A.5.4 — Responsabilidades de la dirección<br>A.5.35 — Revisión independiente de la seguridad de la información<br>A.6.3 — Concienciación, educación y formación en seguridad de la información<br>A.6.4 — Proceso disciplinario<br>A.8.15 — Registros de eventos | **Opción elegida: "Modificar probabilidad e impacto".**<br>La gobernanza no puede eliminarse ni compartirse, pero sí puede fortalecerse mediante procesos formales, roles claros y supervisión estructurada.<br>**Acciones del plan de tratamiento:**<br>BoostTI apoyará en la creación de un marco de gobernanza, definición de roles, procesos documentados, establecimiento de comités, métricas e indicadores de supervisión. Se integrarán controles de gestión del SGSI, revisiones periódicas y mecanismos de escalación.<br>**Evidencias esperadas:** Actas del comité, políticas aprobadas, matriz de roles, documentación de procesos, reportes de supervisión. |

## Riesgos:

- Proceso de solicitud de tarjeta complejo y lento.
- Problemas de logística intersucursal que impiden el traslado de productos y afectan la entrega.
- Ciberataques a infraestructura tecnológica (DDoS, malware, ransomware).

| CONTEXTO DEL PROCESO | | | | | IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROBLEMAS Y OPORTUNIDADES IDENTIFICADAS A PARTIR DE LAS CUESTIONES INTERNAS Y EXTERNAS | TIPO: INTERNA / EXTERNA | PARTE INTERESADA | NECESIDADES/EXPECTATIVAS DE LAS PARTES INTERESADAS | TIPO: REQUISITO/ EXPECTATIVA | RIESGOS | INFORMACIÓN QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE |
| Proceso de solicitud de tarjeta con pasos excesivos, tiempos largos de validación, falta de claridad y gestión inconsistente, afectando la conversión y percepción del cliente. | Interna | - Clientes<br>- Área financiera<br>- Atención al cliente<br>- eCommerce<br>- TI<br>- BoostTI | Proceso ágil, seguro, claro y eficiente para solicitar la tarjeta; validaciones confiables y reducción de fricción en la experiencia del cliente. | I | **Proceso de solicitud de tarjeta complejo y lento.** | | x | | Área financiera / Atención al cliente / eCommerce / BoostTI | - Formulario actual;<br>- Validaciones manuales<br>- Revisión por analistas<br>- Sistema de captura estándar<br>- Pasos tradicionales antes de aprobación. | 4 | 4 |
| Falta de coordinación logística entre sucursales, resistencia a trasladar productos y procesos ineficientes que limitan la operación omnicanal. | Interna | - Logística<br>- Sucursales físicas<br>- eCommerce<br>- Atención al cliente<br>- BoostTI<br>- Clientes | Traslado eficiente entre sucursales, disponibilidad de productos, cumplimiento de pedidos y procesos logísticos ágiles. | R | **Problemas de logística intersucursal que impiden el traslado de productos y afectan la entrega.** | | x | | - Logística es responsable del traslado entre sucursales<br>- Operaciones define políticas y supervisión<br>- eCommerce depende de la disponibilidad intersucursal<br>- BoostTI asegura integraciones, sincronizaciones y procesos | - Traslados manuales bajo solicitud<br>- Comunicación entre sucursales<br>-Validación manual de disponibilidad<br>- Procesos no estandarizados. | 4 | 4 |
| La infraestructura tecnológica enfrenta amenazas externas como DDoS, malware y ransomware que pueden detener operaciones omnicanal y exponer información crítica. | Externa | - Clientes<br>- eCommerce<br>- TI<br>- Seguridad de la Información<br>- Dirección<br>- BoostTI<br>- Proveedores cloud | Protección de los servicios, disponibilidad continua, datos seguros, mitigación de ataques y capacidad de respuesta efectiva. | R | **Ciberataques a infraestructura tecnológica (DDoS, malware, ransomware).** | x | x | x | - Seguridad de la Información administra los controles<br>- TI gestiona servidores, redes e infraestructura<br>- Proveedor cloud (ej. AWS, Azure) debe mantener medidas antiddos y seguridad<br>- BoostTI colabora en integraciones, monitoreo y respuesta | - Firewall<br>- Antivirus básico<br>- Proveedor cloud con mitigación DDoS<br>- Respaldos<br>- Supervisión en horario laboral. | 5 | 2 |

| IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | | | | TRATAMIENTO |
|---|---|---|---|---|---|---|---|---|---|---|
| RIESGOS | INFORMACIÓN QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE | NIVEL DE RIESGO RESIDUAL | CONTROLES ADICIONALES | PLAN DE TRATAMIENTO (INDICAR OPCIÓN DE TRATAMIENTO ELEGIDA) |
| **Proceso de solicitud de tarjeta complejo y lento.** | | x | | Área financiera / Atención al cliente / eCommerce / BoostTI | - Formulario actual;<br>- Validaciones manuales<br>- Revisión por analistas<br>- Sistema de captura estándar<br>- Pasos tradicionales antes de aprobación. | 4 | 4 | 16 | A.5.19 — Seguridad de la información en las relaciones con los proveedores<br>A.8.15 — Registros de actividades<br>A.5.26 — Respuesta a incidentes de seguridad de la información<br>A.5.24 — Planificación y preparación de la gestión de incidentes de seguridad de información<br>A.5.8 — Seguridad de la información en la gestión de proyectos | **Opción elegida: "Modificar probabilidad e impacto".**<br>El proceso de tarjeta no puede eliminarse ni evitarse, pero puede rediseñarse para reducir fricción y mejorar tiempos.<br>**Acciones del plan de tratamiento:**<br>BoostTI rediseñará el flujo de solicitud, automatizará validaciones, reducirá pasos innecesarios, implementará análisis UX y monitoreo de métricas de conversión. Se documentarán procesos y se establecerá control de cambios.<br>**Evidencias esperadas:** Nuevos flujos implementados, métricas de conversión, documentación de proceso, evidencias de pruebas de usuario. |
| **Problemas de logística intersucursal que impiden el traslado de productos y afectan la entrega.** | | x | | - Logística es responsable del traslado entre sucursales<br>- Operaciones define políticas y supervisión<br>- eCommerce depende de la disponibilidad intersucursal<br>- BoostTI asegura integraciones, sincronizaciones y procesos | - Traslados manuales bajo solicitud<br>- Comunicación entre sucursales<br>-Validación manual de disponibilidad<br>- Procesos no estandarizados. | 4 | 4 | 16 | A.5.8 — Seguridad de la información en la gestión de proyectos<br>A.8.15 — Registros de eventos<br>A.8.32 — Gestión de cambios<br>A.5.19 — Seguridad de la información en las relaciones con los proveedores<br>A.5.24 — Planificación y preparación de la gestión de incidentes de seguridad de información.<br>A.6.4 — Seguridad en proyectos (si se moderniza la logística) | **Opción elegida: "Modificar probabilidad e impacto".**<br>La operación logística es necesaria, pero se puede mejorar mediante procesos estandarizados y automatización.<br>**Acciones del plan de tratamiento:**<br>BoostTI diseñará un sistema centralizado de traslado con trazabilidad, indicadores de desempeño, alertas en tiempo real y políticas logísticas uniformes. También apoyará en capacitación y estandarización.<br>**Evidencias esperadas:** Sistema implementado, KPIs registrados, documentación logística, reportes de traslado. |
| **Ciberataques a infraestructura tecnológica (DDoS, malware, ransomware).** | x | x | x | - Seguridad de la Información administra los controles<br>- TI gestiona servidores, redes e infraestructura<br>- Proveedor cloud (ej. AWS, Azure) debe mantener medidas antiddos y seguridad<br>- BoostTI colabora en integraciones, monitoreo y respuesta | - Firewall<br>- Antivirus básico<br>- Proveedor cloud con mitigación DDoS<br>- Respaldos<br>- Supervisión en horario laboral. | 5 | 2 | 10 | A.8.7 — Controles contra el código malicioso<br>A.8.8 — Gestión de vulnerabilidades tecnicas<br>A.5.23 — Seguridad de la información para el uso de servicios en la nube<br>A7.4 — Monitorización de la seguridad física<br>A.5.26 — Respuesta a incidentes de seguridad de la información<br>A.7.13 — Mantenimiento de los equipos<br>A.8.7 – Protección contra malware.<br>A.8.11 – Enmascaramiento de datos<br>A.8.13 – Copias de seguridad de la información.<br>A.8.5 – Autenticación segura<br>A.8.12 – Prevención de fugas de datos | **Opción elegida: "Mitigar el riesgo".**<br>Dado que el impacto es máximo y la probabilidad no se puede reducir a cero, la única opción viable es implementar controles técnicos avanzados para mitigar el ataque.<br>**Acciones del plan de tratamiento:**<br>BoostTI implementará defensa avanzada contra DDoS, EDR, monitoreo 24/7, gestión de vulnerabilidades, segmentación de red, copias inmutables y plan de respuesta a incidentes.<br>**Evidencias esperadas:** Reportes de seguridad, bitácoras, evidencia de backups, registros del SOC, documentación de respuesta a incidentes. |

## Riesgos:

- Desconexión entre canales físico, digital, logística y atención al cliente.
- Variabilidad en disponibilidad de productos.
- Deficiencia en aplicación web.

| CONTEXTO DEL PROCESO | | | | | IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROBLEMAS Y OPORTUNIDADES IDENTIFICADAS A PARTIR DE LAS CUESTIONES INTERNAS Y EXTERNAS | TIPO: INTERNA / EXTERNA | PARTE INTERESADA | NECESIDADES/EXPECTATIVAS DE LAS PARTES INTERESADAS | TIPO: REQUISITO/ EXPECTATIVA | RIESGOS | INFORMACION QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE |
| Los canales físico, online y de atención operan de forma aislada, generando inconsistencias en procesos, información y experiencia del cliente. | Interna | - Clientes<br>- Sucursales<br>- eCommerce<br>- Atención al cliente<br>- TI<br>- BoostTI | Integración completa entre canales, consistencia en inventarios, procesos sincronizados y experiencia omnicanal fluida. | R | **Desconexión entre canales físico, digital, logística y atención al cliente.** | | x | | - TI mantiene integraciones<br>- Operaciones coordina canales<br>- eCommerce depende de la sincronización<br>- BoostTI asegura integraciones y conectividad técnica | - Procesos actuales de comunicación entre áreas.<br>- Sincronizaciones parciales<br>- Revisión manual de información entre canales. | 3 | 3 |
| Variaciones en disponibilidad de productos, desabastecimientos y poca variedad que limitan competitividad comercial y experiencia del cliente. | Interna | - Clientes<br>- Área de Compras<br>- Logística<br>- Comercial<br>- eCommerce<br>- BoostTI | Disponibilidad de productos, variedad adecuada, cumplimiento de pedidos y experiencia de compra satisfactoria. | R | **Variabilidad en disponibilidad de productos.** | | x | x | - Área de Compras<br>- Logística<br>- Comercial<br>- BoostTI (en integración tecnológica) | - Gestión de stock manual<br>- Reportes de inventario<br>- Compras periódicas<br>- Revisión visual y comunicación entre áreas. | 3 | 1 |
| Deficiencias en la aplicación web (lentitud, errores, fallas técnicas) que afectan la experiencia de los clientes y las conversiones en línea. | Interna | - Clientes<br>- Área de eCommerce<br>- TI<br>- BoostTI<br>- Dirección Comercial | Que la aplicación web sea rápida, funcional, estable y brinde una experiencia de compra adecuada. | R | **Deficiencia en aplicación web** | | x | x | -TI<br>-eCommerce<br>-BoostTI | - Monitoreo básico del sitio<br>- Soporte técnico reactivo<br>- Hosting estándar<br>- Revisiones ocasionales de desempeño | 2 | 5 |
| Pérdida de personal clave con conocimiento crítico que afecta la continuidad operativa, la calidad de servicios tecnológicos y la ejecución de procesos estratégicos. | Interna | -Recursos Humanos<br>- Dirección<br>-TI<br>-Operaciones<br>-BoostTI<br>-Clientes | Disponibilidad de personal capacitado, continuidad operativa, estabilidad en procesos, transferencia efectiva de conocimiento crítico. | R | **Rotación de personal clave** | | x | x | -Recursos Humanos<br>- Dirección General<br>-TI<br>-BoostTI | -Capacitación informal<br>-Documentación parcial<br>-Procesos de onboarding<br>-Supervisión básica del desempeño | 4 | 5 |

| IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | | | | TRATAMIENTO |
|---|---|---|---|---|---|---|---|---|---|
| RIESGOS | INFORMACION QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE | NIVEL DE RIESGO RESIDUAL | CONTROLES ADICIONALES | PLAN DE TRATAMIENTO (INDICAR OPCIÓN DE TRATAMIENTO ELEGIDA) |
| **Desconexión entre canales físico, digital, logística y atención al cliente.** | | x | | - TI mantiene integraciones<br>- Operaciones coordina canales<br>- eCommerce depende de la sincronización<br>- BoostTI asegura integraciones y conectividad técnica | - Procesos actuales de comunicación entre áreas.<br>- Sincronizaciones parciales<br>- Revisión manual de información entre canales. | 3 | 3 | 9 | A.8.15 — Registros de eventos<br>A.8.32 — Gestión de cambios<br>A.5.19 — Seguridad de la información en las relaciones con los proveedores<br>A.5.22 — Seguimiento, revisión y gestión del cambio de los servicios de proveedores<br>A.7.4 — Monitorización de la seguridad física | **Opción elegida: "Modificar probabilidad e impacto".**<br>Este riesgo no puede eliminarse ni evitarse, ya que depende de la estructura operativa y tecnológica de los canales. Sin embargo, sí es posible reducir su impacto mediante integración y sincronización entre sistemas.<br>**Acciones del plan de tratamiento:**<br>BoostTI desarrollará una integración central entre sistemas físicos y digitales (API / ERP), incluirá alertas ante inconsistencias operativas, sincronización automática de inventarios, procesos y datos entre canales, y documentación de flujos omnicanal. Se establecerán indicadores de integración, pruebas periódicas de sincronización y consolidación de procesos entre sucursales.<br>**Evidencias esperadas:** Logs de integración, reportes de sincronización, documentación de procesos, evidencia de pruebas y dashboards unificados. |
| **Variabilidad en disponibilidad de productos.** | | x | x | - Área de Compras<br>- Logística<br>- Comercial<br>- BoostTI (en integración tecnológica) | - Gestión de stock manual<br>- Reportes de inventario<br>- Compras periódicas<br>- Revisión visual y comunicación entre áreas. | 3 | 1 | 3 | A.8.1 — Planificación y control operacional<br>A.5.11 — Seguridad en procesos de negocio<br>A.5.19 — Seguridad de la información en las relaciones con los proveedores<br>A.6.3 — Seguridad en la planificación<br>A.5.32 — Gestión de proveedores<br>A.8.32 — Gestión de cambios<br>A.7.4 — Monitorización de la seguridad física | **Opción elegida: "Aceptar el riesgo".**<br>El riesgo presenta baja probabilidad y bajo impacto; existen controles operativos suficientes para monitorearlo y no requiere inversión o cambio estructural.<br>**Acciones del plan de tratamiento:**<br>Se mantiene monitoreo regular de inventarios, análisis de abastecimiento, seguimiento de indicadores de disponibilidad y revisión semestral del comportamiento comercial. No se aplicarán controles técnicos adicionales, solo supervisión.<br>**Evidencias esperadas:** Reportes de abastecimiento, dashboards de disponibilidad, registros de stock, informes semestrales. |
| **Deficiencia en aplicación web** | | x | x | -TI<br>-eCommerce<br>-BoostTI | - Monitoreo básico del sitio<br>- Soporte técnico reactivo<br>- Hosting estándar<br>- Revisiones ocasionales de desempeño | 2 | 5 | 10 | A.8.17 — Seguridad en pruebas<br>A.8.19 — Monitoreo de performance<br>A.5.28 — Gestión de cambios<br>A.5.20 — Diseño seguro<br>A.5.25 — Seguridad en la adquisición/desarrollo<br>A.8.10 — Monitoreo continuo | **Opción elegida: "Reducir el riesgo".**<br>La probabilidad es muy alta y afecta directamente las ventas y experiencia del cliente; requiere acciones de mejora en la operación del sitio web.<br>**Acciones del plan de tratamiento:**<br>Implementar monitoreo avanzado de performance, pruebas automatizadas antes de cada despliegue, controles de calidad en desarrollo, mejoras de infraestructura y optimización del código. Aplicar proceso formal de gestión de cambios y fortalecer pruebas de carga.<br>**Evidencias esperadas:** Logs de monitoreo, reportes de performance, resultados de pruebas, flujos de despliegue, documentación de cambios, reportes de fallas corregidas. |
| **Rotación de personal clave** | | x | x | -Recursos Humanos<br>- Dirección General<br>-TI<br>-BoostTI | -Capacitación informal<br>-Documentación parcial<br>-Procesos de onboarding<br>-Supervisión básica del desempeño | 4 | 5 | 20 | A.7.2 — Toma de conciencia, educación y capacitación<br>A.5.30 — Revisión independiente del SGSI<br>A.5.11 — Seguridad en procesos de negocio<br>A.8.5 — Eliminación segura de activos (cuando personal sale)<br>A.5.28 — Gestión de cambios<br>A.6.3 — Seguridad en la planificación<br>A.6.4 — Seguridad en proyectos | **Opción elegida: "Modificar probabilidad e impacto".**<br>La rotación no se puede evitar, pero sí reducir su impacto mediante documentación, capacitación, continuidad operativa y gestión del conocimiento.<br>**Acciones del plan de tratamiento:**<br>BoostTI apoyará en la creación de un plan de sucesión, documentación de procesos críticos, capacitación cruzada, creación de manuales operativos, base de conocimiento centralizada y procedimientos formales para transferencias de rol. Se aplicarán métricas de rotación y seguimiento a personal estratégico. |

## Riesgos:

- Pérdida de datos por falta de backup.
- Retraso en envíos.

| CONTEXTO DEL PROCESO | | | | | IDENTIFICACIÓN DEL RIESGO | EVALUACIÓN DEL RIESGO | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PROBLEMAS Y OPORTUNIDADES IDENTIFICADAS A PARTIR DE LAS CUESTIONES INTERNAS Y EXTERNAS | TIPO: INTERNA / EXTERNA | PARTE INTERESADA | NECESIDADES/EXPECTATIVAS DE LAS PARTES INTERESADAS | TIPO: REQUISITO/ EXPECTATIVA | RIESGOS | INFORMACIÓN QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACIÓN RIESGO: IMPACTO DEL RIESGO / POSIBILIDAD DE |
| Ausencia o mala gestión de respaldos diarios que puede ocasionar pérdida de información crítica, afectando operaciones, reportes, procesos de venta y análisis interno. | Interna | -TI<br>- Dirección<br>- eCommerce<br>- Finanzas<br>- Operaciones<br>- BoostTI<br>- Clientes indirectamente | Respaldo confiable de la información, recuperación rápida ante pérdidas, continuidad operativa garantizada. | R | **Pérdida de datos por falta de backup** | | x | x | -TI<br>- BoostTI<br>-Dirección | -Respaldo ocasional<br>-Almacenamiento parcial en equipos locales<br>-Prácticas informales de guardado<br>-Algunos respaldos manuales. | 3 / 2 |
| Retrasos en la entrega de paquetes que afectan la experiencia del cliente, la percepción del servicio y la satisfacción postventa. | Interna | -Clientes<br>-Logística<br>-Ventas<br>-eCommerce<br>-Atención al cliente<br>-BoostTI | Entregas puntuales, trazabilidad de paquetes, comunicación clara sobre tiempos y cumplimiento del servicio. | E | **Retraso en envíos** | | | x | -Logística<br>-Ventas<br>-eCommerce<br>-Atención al cliente<br>-BoostTI | -Uso de paqueterías externas<br>-Seguimiento manual de envíos<br>-Comunicación con clientes cuando se detectan retrasos. | 3 / 1 |

| EVALUACIÓN DEL RIESGO | | | | | | | | TRATAMIENTO |
|---|---|---|---|---|---|---|---|---|
| INFORMACION QUE PODRÍA AFECTARSE: Confidencialidad | Integridad | Disponibilidad | PROPIETARIO(S) DEL RIESGO | CONTROLES EXISTENTES | VALORACION DEL RIESGO: IMPACTO DEL RIESGO | POSIBILIDAD DE | NIVEL DE RIESGO RESIDUAL | CONTROLES ADICIONALES | PLAN DE TRATAMIENTO (INDICAR OPCIÓN DE TRATAMIENTO ELEGIDA) |

# 7. Sistema o Herramienta SGSI Implementada

Se desarrolló un Módulo Web de Documentación y Monitoreo SGSI, funcional como sistema centralizado para supervisión del estado del sistema, hallazgos, indicadores, documentación y políticas.


Optimizar el proceso logístico digital para garantizar entregas puntuales, trazabilidad completa y comunicación transparente con los clientes.

## Objetivos del SGSI

1. **Proteger la información utilizada en los procesos de eCommerce y Marketplace de La Marina:** Salvaguardar los datos críticos de negocio en todas las plataformas digitales.
2. **Garantizar la confidencialidad, integridad y disponibilidad de los datos de clientes, pedidos, inventarios, transacciones y proveedores:** Mantener los tres pilares fundamentales de la seguridad de la información.
3. **Asegurar el funcionamiento confiable de las plataformas digitales:** Incluyendo la tienda en línea, integraciones con VTEX, marketplaces y sistemas logísticos.
4. **Reducir los riesgos tecnológicos:** Mitigar ciberataques, fraude, fallas de plataforma y desincronización de inventarios.
5. **Establecer controles de seguridad:** Implementar medidas que permitan operaciones digitales estables, seguras y alineadas al negocio.
6. **Fortalecer la continuidad operativa:** Garantizar que las ventas, envíos y procesos digitales funcionen sin interrupciones significativas.
7. **Promover la mejora continua:** En los procesos de seguridad, integraciones tecnológicas y servicio al cliente.

Cada objetivo cuenta con métricas e indicadores asociados que permiten monitorear el cumplimiento y efectividad de los controles implementados.

## Procesos

Proceso funcional implementado: gestión de e-commerce y marketplace.

### Proceso: Gestión e-commerce y Marketplace (PROC-ECOMM)

**Objetivo del proceso:** Asegurar que la plataforma de e-commerce y marketplace opere con seguridad, disponibilidad y confianza para clientes y vendedores, mitigando riesgos como fraude, fallos en pagos, pérdida de pedidos o interrupciones del servicio.

**Indicadores del proceso (obligatorio medir):**

| Indicador | Descripción | Meta | Último valor |
|---|---|---|---|
| % Transacciones exitosas | % de pagos completados sin error sobre el total de intentos | ≥ 98% | 96% |
| Tiempo medio de entrega | Tiempo medio (horas) desde confirmación hasta entrega al cliente | ≤ 48h | 54h |
| Tasa de fraude | % de transacciones identificadas como fraude o chargeback | ≤ 0.5% | 0.9% |

# 8. Beneficios Técnicos Alcanzados

Los principales beneficios técnicos alcanzados mediante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en La Marina. Estos beneficios se derivan de la incorporación de controles técnicos, políticas operativas, monitoreo automatizado, mecanismos de trazabilidad y herramientas de seguridad aplicadas sobre los procesos críticos del negocio (e-commerce, inventarios, logística y servicios financieros). La tabla resume los beneficios obtenidos, explicando su impacto, cómo se lograron y qué mejoras aportan a la organización.

| Beneficio | Detalle |
|---|---|
| Mejora en disponibilidad | Creación de protocolos de continuidad y recuperación ante fallos VTEX |
| Trazabilidad | Registro de hallazgos con responsables, impacto y acciones<br>index |
| Fortalecimiento de seguridad | Implementación de políticas sobre transacciones, inventarios, plataformas y logística digital<br>index |
| Eficiencia operativa | Reducción de errores de inventario desde API VTEX mediante controles |

## 9. Conclusión General del Sistema de Gestión de Seguridad de la Información (SGSI)

La implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en La Marina permitió establecer una estructura formal y sistemática para proteger la información crítica del negocio, garantizar la continuidad de los servicios digitales y reducir los riesgos asociados a operaciones financieras, manejo de inventarios, comercio electrónico y logística omnicanal.

El SGSI consolida un marco de gobernanza basado en ISO/IEC 27001 y otras normas internacionales, lo que permitió identificar activos, clasificar información, evaluar riesgos, implementar controles, documentar responsabilidades y establecer procedimientos para la gestión de incidentes y la mejora continua. De esta manera, la seguridad informática deja de ser un conjunto de acciones aisladas, para convertirse en un sistema organizado, medible y alineado a los objetivos estratégicos del negocio.

Los beneficios alcanzados se reflejan en cuatro pilares fundamentales:

- Mayor disponibilidad de servicios digitales y plataforma VTEX, gracias a protocolos de continuidad, monitoreo y recuperación ante fallos.
- Mejora en la confidencialidad e integridad de los datos mediante políticas, cifrado, controles de acceso y herramientas de monitoreo.
- Mayor eficiencia operativa y trazabilidad, con procesos documentados, responsables definidos y registros auditables.
- Fortalecimiento de la confianza, tanto para clientes como para socios estratégicos y entidades financieras.

Eel SGSI proporciona a La Marina una base tecnológica y organizacional sólida para enfrentar amenazas digitales, cumplir con estándares legales y prepararse para procesos de auditoría y certificación. Representa no solo una medida de protección, sino una inversión estratégica que impulsa la competitividad, innovación y sostenibilidad del negocio en el entorno digital.

**Referencias**:


- ISOTools México. (s. f.). *Identificación, definición y desarrollo del mapa de procesos*. ISOTools Excellence. Recuperado de https://mx.isotools.us/identificacion-definicion-desarrollo-mapa-procesos/
- Dragon1. (s. f.). *RACI matrix definition*. Dragon1 Enterprise Architecture Method. Recuperado de https://www.dragon1.com/terms/raci-matrix-definition
- ISO Council. (s. f.). *What is the Plan-Do-Check-Act model in ISO 14001*. ISO Council. Recuperado de https://isocouncil.com.au/plan-do-check-act-iso-14001