Reporte técnico del desarrollo del SGSI de la Marina

Reporte técnico

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. - Introducción al reporte técnico:

El presente **reporte técnico** documenta el desarrollo e implementación del **Sistema de Gestión de Seguridad de la Información (SGSI)** en la empresa **La Marina**, siguiendo los principios, requisitos y buenas prácticas establecidos en la norma internacional **ISO/IEC 27001:2022**.

Este SGSI se diseñó con el propósito de **proteger los activos de información, reducir los riesgos tecnológicos y operativos, fortalecer la continuidad del negocio y garantizar la protección de los datos sensibles**, tanto internos como de clientes, proveedores y colaboradores.

El sistema se centra en asegurar la correcta protección y funcionamiento de los **procesos digitales estratégicos de la organización**, los cuales representan el núcleo de su operación comercial, logística y financiera. Entre estos procesos críticos se identificaron:

- **E-commerce y Marketplace (Plataforma VTEX):** motor principal de ventas, integración de inventarios, pagos, historial de clientes y órdenes en tiempo real.
- **Omnicanalidad:** interoperabilidad entre sucursales físicas, plataforma digital, aplicaciones móviles y sistemas logísticos.
- **Servicios Financieros:** administración de solicitudes de crédito, datos bancarios, validación de identidad y protección de información confidencial.
- **Logística y Cadena de Suministro:** trazabilidad de productos, control de inventarios, distribución y entrega al cliente final.

La construcción del SGSI incluyó diferentes componentes fundamentales:

- **Modelo de gobernanza**, donde se definieron roles, responsabilidades y estructura organizacional para la gestión de seguridad.
- **Documentación institucional**, incluyendo políticas, procedimientos, líneas base, registros y evidencia de cumplimiento, conforme a los requisitos del Anexo A de ISO 27001.
- **Implementación de controles técnicos y administrativos**, tales como cifrado, gestión de accesos, autenticación multifactor, firewall, SIEM, monitoreo de logs, matrices RACI y controles operativos.
- **Análisis, evaluación y tratamiento de riesgos**, siguiendo metodologías alineadas a ISO 27005 e ISO 31000, con clasificación de impacto, probabilidad y nivel de riesgo residual.

- **Integración de indicadores y mecanismos de seguimiento**, permitiendo medir disponibilidad, incidentes, cumplimiento de controles, trazabilidad y madurez del SGSI.

Como resultado, la empresa cuenta con un sistema estructurado, documentado y alineado con estándares internacionales, capaz de **responder a amenazas tecnológicas, garantizar la continuidad operativa, proteger la información crítica y evolucionar hacia la auditoría y certificación** bajo ISO 27001.

2. - Marco Normativo y Estándares Aplicados

El SGSI fue diseñado alineado con normas y estándares internacionales:

Norma / Estándar	Aplicación
ISO/IEC 27001:2022	Implementación del SGSI, políticas, análisis de riesgos, SoA.
ISO/IEC 27002:2022	Control técnico y administrativo: cifrado, respaldo, control de acceso.
ISO 31000	Enfoque de gestión y evaluación de riesgos.
ISO 22301	Continuidad del negocio (indisponibilidad de VTEX, servicios web).
Ley Federal de Protección de Datos	Protección de datos financieros y personales de clientes.

3. - Activos Tecnológicos y Arquitectura

Activos digitales protegidos por el SGSI:

Activo	Tipo	Relevancia
Plataforma VTEX	SaaS - Marketplace	Core comercial, ventas en línea. Informe Ejecutivo
Portal e-commerce	Web / App	Canal principal de ventas digitales.
Base de datos de clientes	Datos críticos	Datos personales, tarjetas, historial.
Sistema de logística	ERP / API	Inventarios, tracking, picking/packing.
Infraestructura TI	Servidores, redes, backups	Disponibilidad, continuidad operativ

4. - Procesos Clave con Componentes Técnicos

Los 4 procesos críticos identificados en el informe ejecutivo se documentaron técnicamente, definiendo entradas, salidas, controles de seguridad y niveles de criticidad.

Gestión Omnicanal

Integra tienda física, web, marketplace, WhatsApp y redes sociales:

Elemento	Detalle Técnico
Herramientas	**VTEX API, CRM, Integraciones web**
Riesgos	**Desincronización, inventarios falsos**
Controles sugeridos	**Control AC-12 (Acceso), API-SEC (validación real-time), LOG-02**

Gestión de E-commerce y Marketplace:

Elemento	Detalle Técnico
Herramienta principal	**Plataforma VTEX (Marketplace)**
Integraciones	**Gateway de pagos, websockets, API Inventarios**

Amenazas detectadas	**Fallo plataforma VTEX, fraude, ataques DDoS**

Gestión de Logística y Cadena de Suministro:

Elemento	Detalle Técnico
Sistemas	**ERP interno + VTEX OMS**
Riesgos	**Retrasos, pérdida de productos, fallos de inventario**
Controles	**SOP, ERP Tracking, Backup logístico**

Gestión de Servicios Financieros

Elemento	Detalle Técnico
Datos protegidos	**Información crediticia, ingresos, estados de pago** **Informe Ejecutivo**
Sistema	**Procesador interno, clearing bancario**
Riesgos	**Fraude, fuga de datos, morosidad**
Controles	**Cifrado AES-256, autenticación 2FA, auditorías trimestrales**

5. - 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

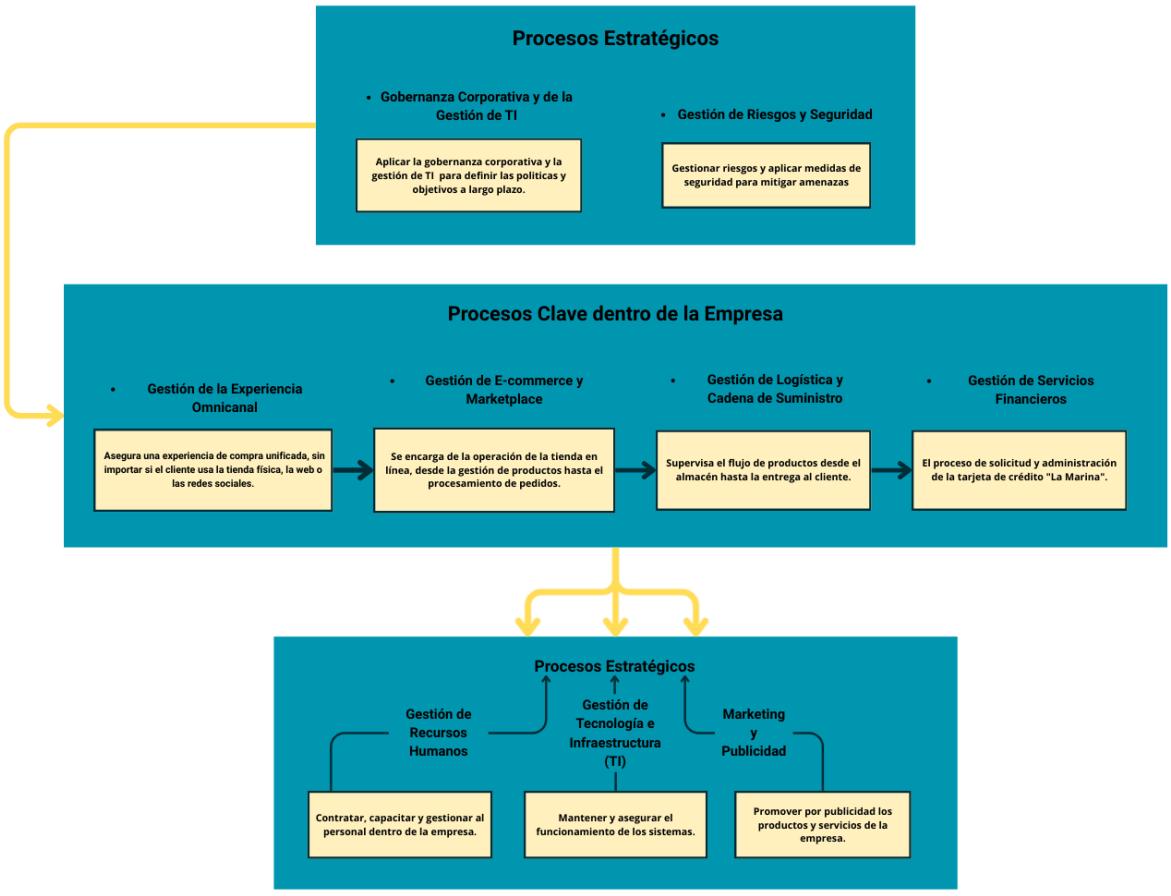
Todos los colaboradores deberán recibir formación continua en ciberseguridad, mejores prácticas en TI y protección de la información, fomentando una cultura organizacional orientada a la seguridad.

6. - 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”:



7. - 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.

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”

Valorando los riesgos anteriores, los cuales fueron plasmados en una matriz de probabilidad y consecuencia. En cambio a continuación se presenta el Análisis de Riesgos de los mismos que fueron detectados en la organización, y estos de acuerdo con la metodología 27001; los cuales requieren una atención y asignación de controles específicos para su mitigación.

La matriz cuenta con:

- Contexto del proceso.
- Identificación del riesgo.
- Evaluación del riesgo
- Tratamiento

La matriz completa se adjunta abajo:

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 - Área de eCommerce - Ventas - 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 - Comunicación con VTEX cuando hay fallas - Revisión periódica del SLA - Reporte mensual de disponibilidad	5	2
Alta exposición a datos sensibles (clientes, tarjetas y transacciones) que requieren medidas estrictas de protección.	Interna	- Cliente final - Área de TI de La Marina - Departamento financiero - eCommerce - 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. - Monitoreo limitado. - Proveedor de pagos con PCI-DSS. - 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 - Comunicación con VTEX cuando hay fallas - Revisión periódica del SLA - Reporte mensual de disponibilidad	5	2	10	- Implementar monitoreo activo 24/7 con alertas - Crear un procedimiento de contingencia para caídas de VTEX - Establecer canales alternos de venta en emergencias - Proporcionar reportes de rendimiento a La Marina	**Opción elegida: "Mitigar el riesgo".** 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. **Acciones del plan de tratamiento:** 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. **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. - Monitoreo limitado. - Proveedor de pagos con PCI-DSS. - Políticas iniciales de privacidad.	3	3	9	A.5.14 – Protección de la información A.5.15 – Control de acceso basado en privilegios A.5.23 – Seguridad en servicios de la nube A.8.7 – Protección contra malware A.8.8 – Gestión de vulnerabilidades técnicas A.8.9 – Registro de actividades (logs) A.8.10 – Monitoreo A.8.11 – Detección de incidentes A.8.12 – Respuesta a incidentes A.8.13 – Copias de seguridad A.8.16 – Cifrado A.5.36 – Obligaciones de privacidad y protección de datos/informacion	**Opción elegida: "Mitigar el riesgo".** 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. **Acciones del plan de tratamiento:** 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. **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 - Área de ventas - Logística - eCommerce - TI - 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. - Monitoreo básico - Revisión manual de inventarios - Validación diaria en tiendas.	4	3
Transacciones financieras y solicitudes de tarjeta expuestas a intentos de fraude electrónico.	Externa	- Clientes - Área financiera - eCommerce - TI - Proveedor de pagos - 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 - Verificación manual de transacciones. - 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. - Comité Directivo - Seguridad de la Información - Todas las áreas operativas - 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 - Políticas básicas no estandarizadas - Procesos definidos de manera informal - 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. - Monitoreo básico - Revisión manual de inventarios - Validación diaria en tiendas.	4	3	12	A.5.12 —Clasificación de la informaciónn A.8.16 — Seguimiento de actividades A.5.23 — Seguridad en servicios en la nube (si los sistemas se integran por API) A.8.8 — Gestión de vulnerabilidades (si la falla es técnica) A.8.32 — Gestión de cambios A.5.32 — Relaciones con proveedores (si inventarios dependen de terceros) A.5.20 — Diseño seguro de sistemas A.8.12 — Respuesta a incidentes (para errores masivos de inventario)	**Opción elegida: "Modificar la probabilidad y el impacto del riesgo".** Este riesgo no puede evitarse porque forma parte natural de la operación omnicanal, pero sí puede reducirse mediante controles automáticos de integridad y sincronización. **Acciones del plan de tratamiento:** 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. **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 - Verificación manual de transacciones. - Autenticación estándar.	5	2	10	A.5.14 — Transferencia de la información A.5.15 — Control de acceso A.8.7 — Protección contra código malicioso A.8.8 — Gestión de vulnerabilidades A.8.11 — Identificación de incidentes A.5.24 — Planificación y preparación de la gestión de incidentes de seguridad de información. A.5.34 — Privacidad y protección de datos de carácter personal (DCP) A.5.23 — Seguridad en servicios en la nube (pasarela, API)	**Opción elegida: "Mitigar el riesgo".** El fraude financiero tiene impacto extremo legal, económico y reputacional, por lo que debe mitigarse aplicando controles antifraude y seguridad reforzada. **Acciones del plan de tratamiento:** 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. **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 - Políticas básicas no estandarizadas - Procesos definidos de manera informal - Comunicación interna mínima.	5	3	15	A.5.1 — Políticas de seguridad de la información A.5.2 — Roles y responsabilidades en seguridad A.5.3 — Segregación de tareas A.5.4 — Responsabilidades de la dirección A.5.35 — Revisión independiente de la seguridad de la información A.6.3 — Concienciación, educación y formación en seguridad de la información A.6.4 — Proceso disciplinario A.8.15 — Registros de eventos	**Opción elegida: "Modificar probabilidad e impacto".** La gobernanza no puede eliminarse ni compartirse, pero sí puede fortalecerse mediante procesos formales, roles claros y supervisión estructurada. **Acciones del plan de tratamiento:** 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. **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 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 - Área financiera - Atención al cliente - eCommerce - TI - 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; - Validaciones manuales - Revisión por analistas - Sistema de captura estándar - 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 - Sucursales físicas - eCommerce - Atención al cliente - BoostTI - 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 - Operaciones define políticas y supervisión - eCommerce depende de la disponibilidad intersucursal - BoostTI asegura integraciones, sincronizaciones y procesos	- Traslados manuales bajo solicitud - Comunicación entre sucursales -Validación manual de disponibilidad - 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 - eCommerce - TI - Seguridad de la Información - Dirección - BoostTI - 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 - TI gestiona servidores, redes e infraestructura - Proveedor cloud (ej. AWS, Azure) debe mantener medidas antiddos y seguridad - BoostTI colabora en integraciones, monitoreo y respuesta	- Firewall - Antivirus básico - Proveedor cloud con mitigación DDoS - Respaldos - 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; - Validaciones manuales - Revisión por analistas - Sistema de captura estándar - Pasos tradicionales antes de aprobación.	4	4	16	A.5.19 — Seguridad de la información en las relaciones con los proveedores A.8.15 — Registros de actividades A.5.26 — Respuesta a incidentes de seguridad de la información A.5.24 — Planificación y preparación de la gestión de incidentes de seguridad de información A.5.8 — Seguridad de la información en la gestión de proyectos	**Opción elegida: "Modificar probabilidad e impacto".** El proceso de tarjeta no puede eliminarse ni evitarse, pero puede rediseñarse para reducir fricción y mejorar tiempos. **Acciones del plan de tratamiento:** 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. **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 - Operaciones define políticas y supervisión - eCommerce depende de la disponibilidad intersucursal - BoostTI asegura integraciones, sincronizaciones y procesos	- Traslados manuales bajo solicitud - Comunicación entre sucursales -Validación manual de disponibilidad - Procesos no estandarizados.	4	4	16	A.5.8 — Seguridad de la información en la gestión de proyectos A.8.15 — Registros de eventos A.8.32 — Gestión de cambios A.5.19 — Seguridad de la información en las relaciones con los proveedores A.5.24 — Planificación y preparación de la gestión de incidentes de seguridad de información. A.6.4 — Seguridad en proyectos (si se moderniza la logística)	**Opción elegida: "Modificar probabilidad e impacto".** La operación logística es necesaria, pero se puede mejorar mediante procesos estandarizados y automatización. **Acciones del plan de tratamiento:** 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. **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 - TI gestiona servidores, redes e infraestructura - Proveedor cloud (ej. AWS, Azure) debe mantener medidas antiddos y seguridad - BoostTI colabora en integraciones, monitoreo y respuesta	- Firewall - Antivirus básico - Proveedor cloud con mitigación DDoS - Respaldos - Supervisión en horario laboral.	5	2	10	A.8.7 — Controles contra el código malicioso A.8.8 — Gestión de vulnerabilidades tecnicas A.5.23 — Seguridad de la información para el uso de servicios en la nube A7.4 — Monitorización de la seguridad física A.5.26 — Respuesta a incidentes de seguridad de la información A.7.13 — Mantenimiento de los equipos A.8.7 – Protección contra malware. A.8.11 – Enmascaramiento de datos A.8.13 – Copias de seguridad de la información. A.8.5 – Autenticación segura A.8.12 – Prevención de fugas de datos	**Opción elegida: "Mitigar el riesgo".** 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. **Acciones del plan de tratamiento:** BoostTI implementará defensa avanzada contra DDoS, EDR, monitoreo 24/7, gestión de vulnerabilidades, segmentación de red, copias inmutables y plan de respuesta a incidentes. **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 - Sucursales - eCommerce - Atención al cliente - TI - 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 - Operaciones coordina canales - eCommerce depende de la sincronización - BoostTI asegura integraciones y conectividad técnica	- Procesos actuales de comunicación entre áreas. - Sincronizaciones parciales - 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 - Área de Compras - Logística - Comercial - eCommerce - 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 - Logística - Comercial - BoostTI (en integración tecnológica)	- Gestión de stock manual - Reportes de inventario - Compras periódicas - 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 - Área de eCommerce - TI - BoostTI - 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 -eCommerce -BoostTI	- Monitoreo básico del sitio - Soporte técnico reactivo - Hosting estándar - 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 - Dirección -TI -Operaciones -BoostTI -Clientes	Disponibilidad de personal capacitado, continuidad operativa, estabilidad en procesos, transferencia efectiva de conocimiento crítico.	R	**Rotación de personal clave**		x	x	-Recursos Humanos - Dirección General -TI -BoostTI	-Capacitación informal -Documentación parcial -Procesos de onboarding -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 - Operaciones coordina canales - eCommerce depende de la sincronización - BoostTI asegura integraciones y conectividad técnica	- Procesos actuales de comunicación entre áreas. - Sincronizaciones parciales - Revisión manual de información entre canales.	3	3	9	A.8.15 — Registros de eventos A.8.32 — Gestión de cambios A.5.19 — Seguridad de la información en las relaciones con los proveedores A.5.22 — Seguimiento, revisión y gestión del cambio de los servicios de proveedores A.7.4 — Monitorización de la seguridad física	**Opción elegida: "Modificar probabilidad e impacto".** 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. **Acciones del plan de tratamiento:** 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. **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 - Logística - Comercial - BoostTI (en integración tecnológica)	- Gestión de stock manual - Reportes de inventario - Compras periódicas - Revisión visual y comunicación entre áreas.	3	1	3	A.8.1 — Planificación y control operacional A.5.11 — Seguridad en procesos de negocio A.5.19 — Seguridad de la información en las relaciones con los proveedores A.6.3 — Seguridad en la planificación A.5.32 — Gestión de proveedores A.8.32 — Gestión de cambios A.7.4 — Monitorización de la seguridad física	**Opción elegida: "Aceptar el riesgo".** El riesgo presenta baja probabilidad y bajo impacto; existen controles operativos suficientes para monitorearlo y no requiere inversión o cambio estructural. **Acciones del plan de tratamiento:** 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. **Evidencias esperadas:** Reportes de abastecimiento, dashboards de disponibilidad, registros de stock, informes semestrales.
Deficiencia en aplicación web		x	x	-TI -eCommerce -BoostTI	- Monitoreo básico del sitio - Soporte técnico reactivo - Hosting estándar - Revisiones ocasionales de desempeño	2	5	10	A.8.17 — Seguridad en pruebas A.8.19 — Monitoreo de performance A.5.28 — Gestión de cambios A.5.20 — Diseño seguro A.5.25 — Seguridad en la adquisición/desarrollo A.8.10 — Monitoreo continuo	**Opción elegida: "Reducir el riesgo".** La probabilidad es muy alta y afecta directamente las ventas y experiencia del cliente; requiere acciones de mejora en la operación del sitio web. **Acciones del plan de tratamiento:** 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. **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 - Dirección General -TI -BoostTI	-Capacitación informal -Documentación parcial -Procesos de onboarding -Supervisión básica del desempeño	4	5	20	A.7.2 — Toma de conciencia, educación y capacitación A.5.30 — Revisión independiente del SGSI A.5.11 — Seguridad en procesos de negocio A.8.5 — Eliminación segura de activos (cuando personal sale) A.5.28 — Gestión de cambios A.6.3 — Seguridad en la planificación A.6.4 — Seguridad en proyectos	**Opción elegida: "Modificar probabilidad e impacto".** La rotación no se puede evitar, pero sí reducir su impacto mediante documentación, capacitación, continuidad operativa y gestión del conocimiento. **Acciones del plan de tratamiento:** 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 - Dirección - eCommerce - Finanzas - Operaciones - BoostTI - 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 - BoostTI -Dirección	-Respaldo ocasional -Almacenamiento parcial en equipos locales -Prácticas informales de guardado -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 -Logística -Ventas -eCommerce -Atención al cliente -BoostTI	Entregas puntuales, trazabilidad de paquetes, comunicación clara sobre tiempos y cumplimiento del servicio.	E	**Retraso en envíos**			x	-Logística -Ventas -eCommerce -Atención al cliente -BoostTI	-Uso de paqueterías externas -Seguimiento manual de envíos -Comunicación con clientes cuando se detectan retrasos.	3	1

EVALUACIÓN DEL RIESGO									TRATAMIENTO
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)
	x	x	-TI - BoostTI -Dirección	-Respaldo ocasional -Almacenamiento parcial en equipos locales -Prácticas informales de guardado -Algunos respaldos manuales.	3	2	6	A.8.13 — Copias de seguridad A.8.12 — Registro y monitoreo A.5.11 — Seguridad en procesos de negocio A.8.16 — Gestión de la configuración A.5.23 — Gestión de la información A.5.28 — Gestión de cambios	**Opción elegida: "Reducir el riesgo".** Aunque la probabilidad es baja, el impacto afecta directamente integridad y disponibilidad. Se requiere implementar un proceso formal y automatizado de respaldo. **Acciones del plan de tratamiento:** Establecer políticas de backup diario, respaldo automático en la nube, verificación periódica de recuperación, bitácoras de respaldo, pruebas de restauración y definición de tiempos de retención. BoostTI apoyará en el diseño del proceso y automatización. **Evidencias esperadas:** Bitácoras de backup, reportes de restauración exitosa, configuraciones del sistema de respaldo, políticas
		x	-Logística -Ventas -eCommerce -Atención al cliente -BoostTI	-Uso de paqueterías externas -Seguimiento manual de envíos -Comunicación con clientes cuando se detectan retrasos.	3	1	3	A.5.11 — Seguridad en procesos de negocio A.5.32 — Gestión de proveedores A.8.10 — Monitoreo continuo A.8.21 — Seguimiento y revisión A.5.23 — Gestión de la información	**Opción elegida: "Aceptar el riesgo".** La probabilidad es muy baja y los retrasos ocasionales dependen mayormente de proveedores externos; mantener controles básicos es suficiente para este nivel. **Acciones del plan de tratamiento:** Mantener monitoreo de envíos, comunicación proactiva con clientes, análisis mensual de desempeño de paqueterías y retroalimentación a proveedores cuando existan atrasos significativos. BoostTI apoyará en métricas y automatización de notificaciones. **Evidencias esperadas:** Registros de seguimiento de envíos, KPIs de entrega, reportes de desempeño de paqueterías, evidencia de comunicación con clientes.

10. Desarrollo del SGSI / Sistema o Herramienta Implementada

Se desarrolló un **Módulo Web centralizado** que funciona como plataforma de gestión del Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema permite **organizar, supervisar y mantener el control documental, los indicadores, los hallazgos, los riesgos y el cumplimiento de políticas de seguridad**.

A continuación, se explican de forma explícita cada una de sus funciones principales:

1. Gestión de Documentación SGSI

Permite almacenar, organizar y consultar todos los documentos generados durante la implementación del SGSI, como:

- Políticas (de acceso, backup, seguridad, tratamiento de datos, uso de sistemas)
- Procedimientos (gestión de incidentes, continuidad, clasificación de activos)
- Matriz de Riesgos, Matriz RACI, Declaración de Aplicabilidad (SoA)
- Actas del Comité SGSI y evidencias de cumplimiento

Ventaja técnica: evita versiones incorrectas, mantiene trazabilidad documental y cumple con ISO 27001 (control A.7 y A.12).

2. Registro y Seguimiento de Hallazgos

Este apartado permite registrar **no conformidades, incidentes, fallas operativas o debilidades de seguridad**, y asignarles:

- Responsable
- Fecha de detección
- Impacto y criticidad
- Estado (pendiente, en revisión, resuelto)

- Evidencia de corrección

3. Indicadores del SGSI (KPIs y Métricas Técnicas)

El sistema incluye un panel de indicadores que permite visualizar el estado de salud del SGSI y del ecosistema digital, por ejemplo:

- Disponibilidad del sitio (uptime)
- Número de incidentes de seguridad detectados
- Tiempo promedio de recuperación ante fallos (MTTR)
- Errores de inventario y cancelaciones por stock
- Cumplimiento de políticas y controles

Apoya la toma de decisiones técnicas y permite medir eficacia del SGSI (ISO 27004).

4. Gestión de Políticas y Controles

Este módulo almacena y organiza las **políticas internas y los controles de seguridad implementados**, estableciendo:

- Qué control se aplicó (ej. cifrado, acceso, respaldo)
- A qué riesgo responde
- En qué proceso se aplica (inventarios, plataforma VTEX, logística digital, pagos)
- Responsable del control
- Evidencia de cumplimiento

Permite relacionar cada control con su riesgo correspondiente, como lo exige ISO 27001 en la **Declaración de Aplicabilidad (SoA).**

5. Monitoreo y Seguimiento del SGSI

Funciona como tablero de control donde se visualiza el estado general del SGSI:

Elemento Monitoreado	Qué muestra
Estado de políticas	Aplicadas, en revisión, vencidas
Riesgos críticos	Nivel de riesgo alto/medio/bajo según impacto
Incidentes activos	Problemas abiertos en plataforma, fraudes, exposiciones
Documentos pendientes	Políticas o procedimientos no actualizados
Nivel de cumplimiento ISO 27001	Avances del SGSI por cláusula o control

Brinda visibilidad en tiempo real de la madurez del SGSI.

6. Soporte para Auditoría Interna

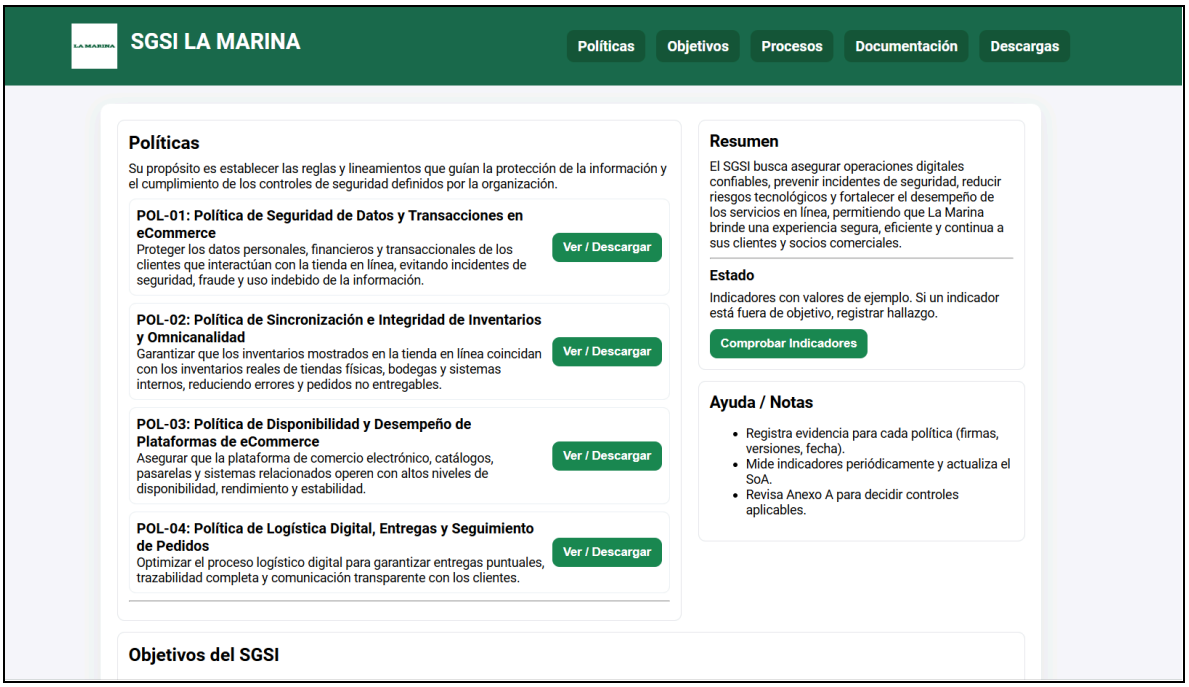
El sistema permite generar evidencias, informes, documentos y registros de cumplimiento del SGSI, lo cual facilita auditorías internas y futuras auditorías de certificación ISO 27001.

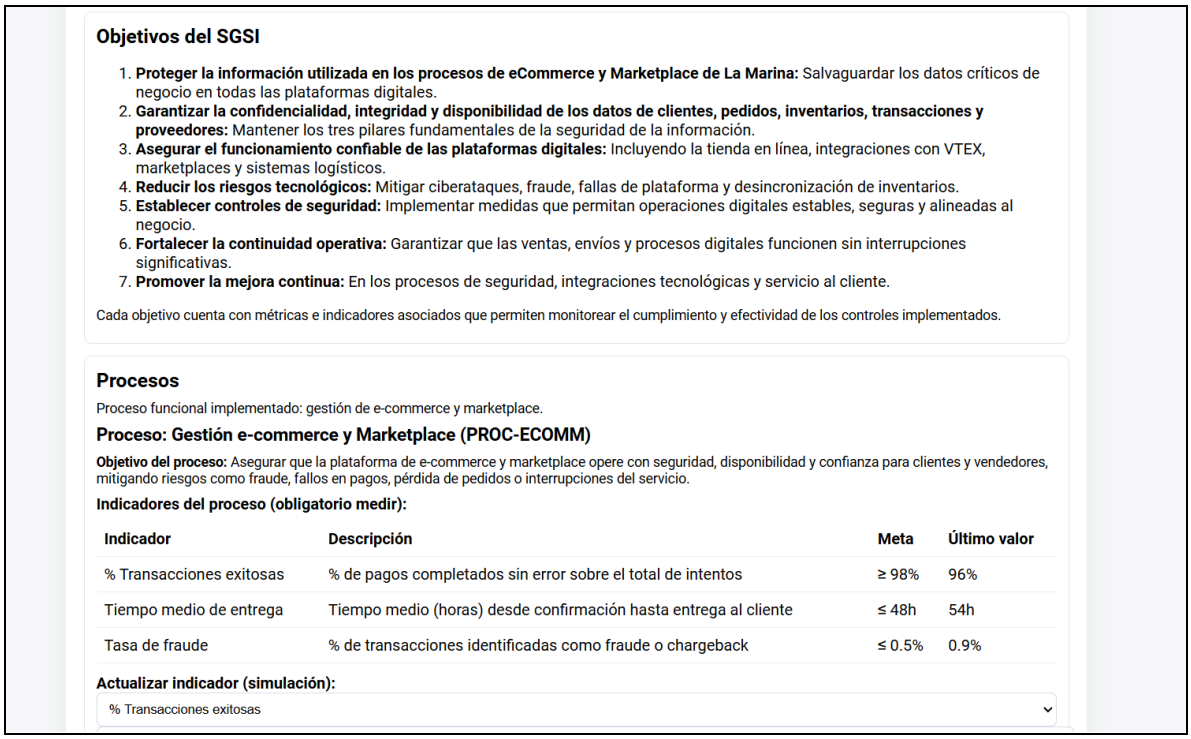
- Generación de reportes PDF o Word
- Registro histórico de acciones, decisiones y cambios
- Evidencia de cumplimiento y trazabilidad

Cumple con las fases de auditoría de ISO/IEC 19011 y mantiene la trazabilidad documental.

11. - SGSI LA MARINA

Pantallas del SGSI de “La Marina”:





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%

Actualizar indicador (simulación):

% Transacciones exitosas

Nuevo valor (ej. 98% o 36h o 0.3%)

Actualizar

Hallazgos (incidencias detectadas)

Registra aquí los hallazgos relacionados con el proceso. Deben incluir: descripción, impacto, recomendación y responsable.

Descripción del hallazgo:

Ej: Fallos en sincronización de inventario

Impacto:

Ej: Sobreventa o pérdida de ventas

Recomendación:

Ej: Implementar validaciones en tiempo real

Responsable:

Ej: Equipo de Operaciones TI

Recomendación:

Ej: Implementar validaciones en tiempo real

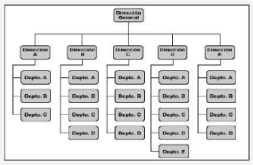
Responsable:

Ej: Equipo de Operaciones TI

Registrar Hallazgo

Documentación del SGSI

A continuación se presentan los componentes clave de la documentación del Sistema de Gestión de Seguridad de la Información:

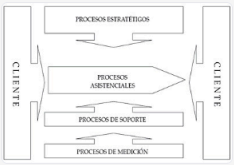


Organigrama

¿Qué es? Estructura jerárquica que define los roles, responsabilidades y líneas de autoridad dentro de la organización para la gestión de seguridad de la información.

Componentes: Dirección General, Responsable SGSI, Equipo de Seguridad TI, Responsables de Procesos, y todas las áreas involucradas.

Propósito: Establecer quién es responsable de qué en materia de seguridad y cómo fluye la comunicación en la organización.

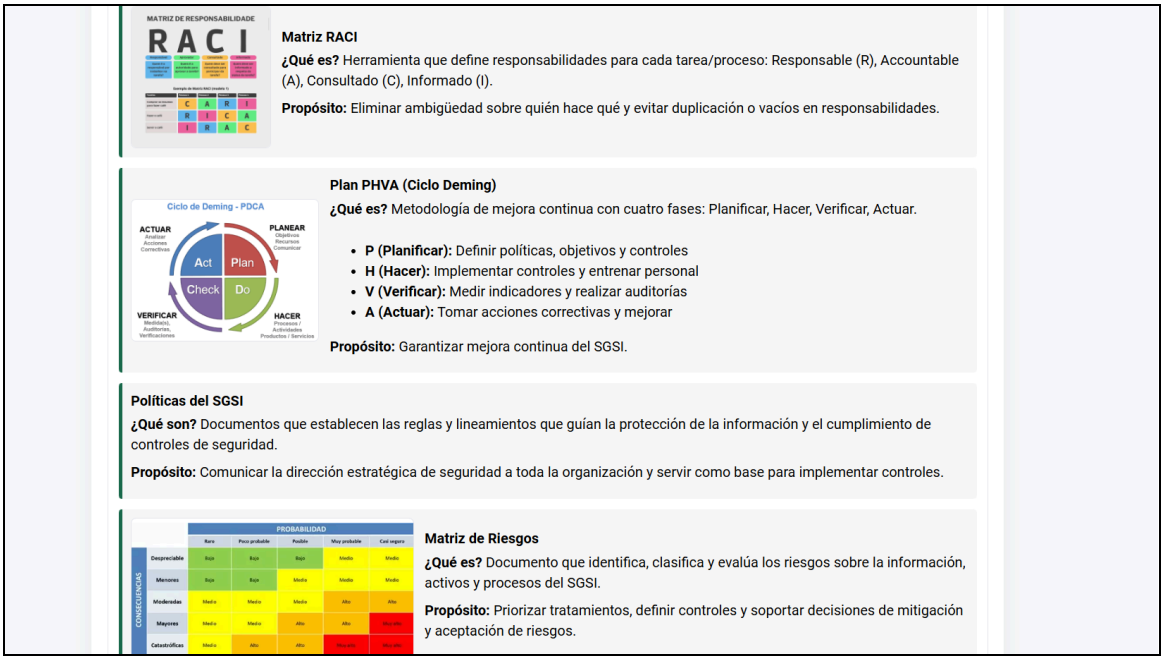


Cédula de Procesos

¿Qué es? Documento que describe detalladamente cada proceso, incluyendo su objetivo, alcance, partes interesadas, entradas, actividades y salidas.

Propósito: Documentar cómo se ejecutan los procesos y qué controles de seguridad deben aplicarse en cada uno.

Matriz RACI



Matriz RACI

¿Qué es? Herramienta que define responsabilidades para cada tarea/proceso: Responsable (R), Accountable (A), Consultado (C), Informado (I).

Propósito: Eliminar ambigüedad sobre quién hace qué y evitar duplicación o vacíos en responsabilidades.

Plan PHVA (Ciclo Deming)

¿Qué es? Metodología de mejora continua con cuatro fases: Planificar, Hacer, Verificar, Actuar.

- **P (Planificar):** Definir políticas, objetivos y controles
- **H (Hacer):** Implementar controles y entrenar personal
- **V (Verificar):** Medir indicadores y realizar auditorías
- **A (Actuar):** Tomar acciones correctivas y mejorar

Propósito: Garantizar mejora continua del SGSI.

Políticas del SGSI

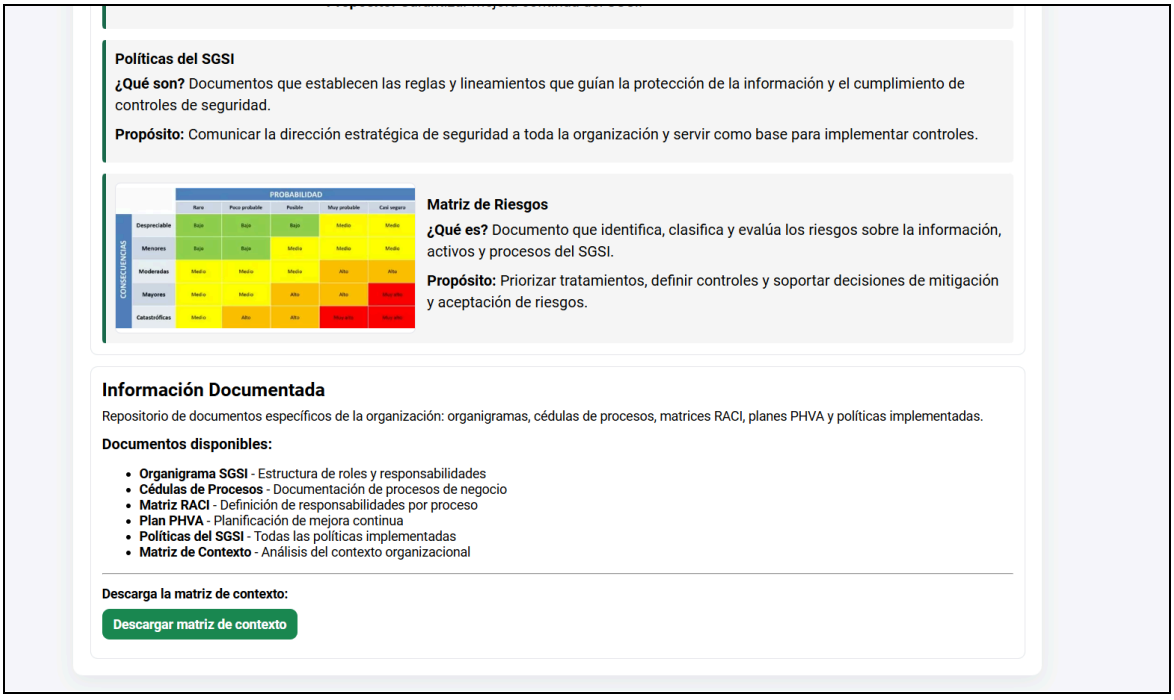
¿Qué son? Documentos que establecen las reglas y lineamientos que guían la protección de la información y el cumplimiento de controles de seguridad.

Propósito: Comunicar la dirección estratégica de seguridad a toda la organización y servir como base para implementar controles.

Matriz de Riesgos

¿Qué es? Documento que identifica, clasifica y evalúa los riesgos sobre la información, activos y procesos del SGSI.

Propósito: Priorizar tratamientos, definir controles y soportar decisiones de mitigación y aceptación de riesgos.



Políticas del SGSI

¿Qué son? Documentos que establecen las reglas y lineamientos que guían la protección de la información y el cumplimiento de controles de seguridad.

Propósito: Comunicar la dirección estratégica de seguridad a toda la organización y servir como base para implementar controles.

Matriz de Riesgos

¿Qué es? Documento que identifica, clasifica y evalúa los riesgos sobre la información, activos y procesos del SGSI.

Propósito: Priorizar tratamientos, definir controles y soportar decisiones de mitigación y aceptación de riesgos.

Información Documentada

Repositorio de documentos específicos de la organización: organigramas, cédulas de procesos, matrices RACI, planes PHVA y políticas implementadas.

Documentos disponibles:

- **Organigrama SGSI** - Estructura de roles y responsabilidades
- **Cédulas de Procesos** - Documentación de procesos de negocio
- **Matriz RACI** - Definición de responsabilidades por proceso
- **Plan PHVA** - Planificación de mejora continua
- **Políticas del SGSI** - Todas las políticas implementadas
- **Matriz de Contexto** - Análisis del contexto organizacional

---

Descarga la matriz de contexto:

Descargar matriz de contexto

12. Conclusión, impacto, alineamientos y componentes clave del SGSI de “La Marina”

El SGSI se alinea con los siguientes objetivos empresariales clave:

- Garantizar la confiabilidad y disponibilidad de la plataforma en línea (tienda virtual, integraciones VTEX, Marketplace, etc.).
- Salvaguardar los datos de clientes (personales, financieros, transaccionales) y los datos de negocio (inventarios, pedidos).
- Reducir los riesgos de fraude, ciberataques y desincronización de inventarios que puedan interrumpir el negocio.

Componentes Clave

EL SGSI se estructura en las siguientes secciones para lograr la seguridad integral:

1. Políticas: Se han establecido cuatro políticas clave (POL-01 a POL-04) que cubren la seguridad de datos, la integridad de inventarios (omnicanalidad), la disponibilidad de plataformas y la logística digital (entrega y seguimiento de pedidos).
2. Procesos: El sistema se enfoca en el Proceso de Gestión E-commerce y Marketplace (PROC-ECOMM), asegurando que sus indicadores críticos (transacciones exitosas, tiempo de entrega, tasa de fraude) estén bajo control y se gestione cualquier Hallazgo detectado.
3. Documentación: La gobernanza se soporta con documentos esenciales como el Organigrama, la Cédula de Procesos, la Matriz RACI, la Matriz de Riesgos y el Plan PHVA (Mejora Continua).

¿Qué problemas resuelve?

- Dispersión de información: Consolida en un solo lugar todas las políticas, objetivos, procesos e información documentada del SGSI, eliminando la necesidad de buscar documentos en múltiples archivos y carpetas.
- Opacidad en la medición: Permite una visualización rápida del estado de los indicadores clave del proceso de e-commerce y marketplace (como el % de Transacciones Exitosas y la Tasa de Fraude), facilitando a la dirección identificar rápidamente si un área está fuera de la meta.

- Trazabilidad de la Mejora: Proporciona una herramienta para registrar los hallazgos (incidencias o no conformidades) directamente asociados al proceso, asegurando que se documenten las descripciones, impactos, recomendaciones y responsables para su corrección.

¿Cómo apoya los procesos actuales de La Marina?

El módulo apoya directamente al proceso PROC-ECOMM (Gestión e-commerce y Marketplace), el cual es crítico para la estrategia omnicanal de la empresa. Al centralizar la documentación y ofrecer una vista clara de los indicadores y hallazgos, el sistema asegura la disponibilidad y confiabilidad de la tienda en línea y sus integraciones, mitigando el riesgo de fraude, fallas en los pagos y desincronización de inventarios.

13. - Resultados Esperados / Beneficios Potenciales del SGSI

La implementación exitosa del Sistema de Gestión de Seguridad de la Información (SGSI) proyectará beneficios estratégicos y medibles en la operación de La Marina, especialmente en su crucial estrategia digital:

- **Reducción Proactiva de Riesgos Tecnológicos:** Al definir la Matriz de Riesgos y aplicar controles específicos el SGSI permitirá mitigar de manera proactiva las amenazas más críticas.
- **Protección de Datos y Fortalecimiento de la Confianza del Cliente:** La Política POL-01 (Seguridad de Datos y Transacciones) garantizará la confidencialidad e integridad de la información sensible del cliente. Esto se traducirá directamente en una mayor fidelidad y confianza al utilizar los servicios en línea de La Marina, un activo intangible vital para el negocio.
- **Soporte a un Crecimiento Digital Sostenible (E-commerce):** El SGSI alineará la seguridad con el objetivo de "Asegurar el funcionamiento confiable de las plataformas digitales".
- **Mejora de la Eficiencia Operativa y Logística:** Establecerá el marco para optimizar los procesos de envío. Monitorear y gestionar activamente el Tiempo Medio de Entrega. Que la logística digital sea eficiente y cumpla consistentemente con las expectativas de servicio al cliente.

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