TRABAJO DE GRADO

Opción Seminario.

Caso 7 Empresa de Comercio Electrónico (E-Commerce)

Compraya online S.A.S.

Corporación Universitaria Remington

Facultad de Ingenierías

Ingeniería de Sistemas

Adizam Domicó Bailarín

Adrián Alberto Mejía Bañol

Jhon Cristian Mejia Bañol

Jorge Leonardo Ramírez Restrepo – docente del seminario

Seminario

2026

Contenido

Dedicatoria

A nuestros padres, quienes siempre creyeron en nosotros y son partícipes de este gran logro.

A nuestros hijos, por quienes luchamos cada día y son nuestra inspiración para cada día ser mejores y logren seguir nuestras huellas.

Agradecimientos

A todos los que de una u otra manera nos apoyaron en este camino de la construcción de nuestros sueños, porque su apoyo también fue fundamental.

Resumen

CompraYa Online S.A.S. es una empresa colombiana de comercio electrónico que comercializa productos de tecnología, hogar, moda, deportes y accesorios a través de canales exclusivamente digitales, y que administra una base de datos superior a 180.000 clientes registrados. Su operación depende de una infraestructura tecnológica robusta —plataforma web, aplicación móvil, sistemas CRM y ERP, pasarela de pagos e infraestructura en la nube pública—, lo que la convierte en un objetivo relevante frente a amenazas de ciberseguridad.

El presente informe técnico analiza la situación de seguridad de la información de la organización a partir de los hallazgos de un diagnóstico inicial realizado por una firma consultora especializada, el cual evidenció debilidades en la clasificación de la información, la gestión de accesos, la respuesta a incidentes y la evaluación de terceros. A partir de este diagnóstico se desarrolla un marco conceptual fundamentado en la tríada de confidencialidad, integridad y disponibilidad, y un marco normativo colombiano e internacional (Ley 1581 de 2012, Ley 1273 de 2009, ISO/IEC 27001:2022 y PCI DSS v4.0).

Se identifican y valoran los activos de información más críticos de CompraYa Online y se desarrolla un análisis de riesgos bajo los lineamientos de las normas ISO 31000 e ISO/IEC 27005, mediante el cual se formalizan cinco

escenarios de riesgo inherente, tres de ellos clasificados en nivel alto: la indisponibilidad crítica de la plataforma, el compromiso de identidades por phishing y la fuga interna de información por prácticas de shadow IT. A partir de estos resultados se plantean estrategias de tratamiento, políticas y controles de seguridad, así como lineamientos de gestión de incidentes, continuidad del negocio y fortalecimiento de la cultura organizacional en ciberseguridad, orientados a mejorar la postura de seguridad de la organización en un contexto de crecimiento acelerado y expansión regional.

Palabras claves

Ciberseguridad, comercio electrónico, gestión de riesgos, seguridad de la información, activos de información, protección de datos personales.

Marco conceptual

Para analizar la situación de CompraYa Online S.A.S. es necesario partir de los conceptos fundamentales que sustentan la gestión de la seguridad de la información. La ciberseguridad puede entenderse como el conjunto de prácticas, procesos y tecnologías orientadas a proteger sistemas, redes, programas y datos frente a ataques digitales, mientras que la seguridad de la información constituye un concepto más amplio que abarca la protección de la información

independientemente del medio en que se encuentre, incluyendo aspectos organizacionales, físicos y humanos (ISO/IEC, 2018).

Un principio central en este campo es la denominada tríada CIA, que hace referencia a la confidencialidad, la integridad y la disponibilidad de la información. La confidencialidad garantiza que la información solo sea accesible para quienes están autorizados a conocerla; la integridad asegura que los datos no sean alterados de forma no autorizada o accidental; y la disponibilidad garantiza que la información y los sistemas estén accesibles cuando los usuarios legítimos los requieran (Whitman & Mattord, 2021). En el caso de CompraYa Online, estos tres principios resultan críticos: la confidencialidad protege los datos personales y financieros de más de 180.000 clientes, la integridad es indispensable en los procesos de pago y gestión de inventarios, y la disponibilidad es determinante para una organización cuya operación depende por completo de plataformas digitales.

Un activo de información se define como cualquier recurso —dato, sistema, aplicación, infraestructura o incluso persona— que tiene valor para la organización y que, por tanto, requiere protección (ISO/IEC, 2022). Frente a estos activos existen amenazas, entendidas como eventos o circunstancias con el potencial de causar daño, ya sea de origen humano, tecnológico o natural, y vulnerabilidades, que corresponden a las debilidades presentes en un activo que

pueden ser aprovechadas por una amenaza para materializar un daño (NIST, 2012). La combinación de una amenaza con una vulnerabilidad determina la existencia de un riesgo, entendido como la probabilidad de que ocurra un evento no deseado y el impacto que dicho evento tendría sobre los objetivos de la organización.

Finalmente, los controles de seguridad constituyen las medidas —técnicas, administrativas o físicas— implementadas para reducir la probabilidad de ocurrencia de una amenaza o para mitigar su impacto en caso de materializarse (ISO/IEC, 2022). En el contexto de CompraYa Online, la ausencia de controles como la autenticación multifactor generalizada, la clasificación de la información o un procedimiento formal de gestión de incidentes evidencia brechas relevantes frente a los estándares internacionalmente reconocidos en la materia, lo que refuerza la necesidad de un análisis estructurado de riesgos como el que se desarrolla en este informe (MinTIC, 2020).

Marco normativo

El análisis de la situación de CompraYa Online S.A.S. debe considerar el marco normativo colombiano e internacional aplicable a la protección de datos personales y a la ciberseguridad. En Colombia, la Ley 1581 de 2012 establece el régimen general de protección de datos personales, definiendo principios como

la finalidad, la libertad y la seguridad en el tratamiento de la información, mientras que el Decreto 1377 de 2013 reglamenta aspectos operativos de dicha ley, incluyendo la exigencia de contar con políticas de tratamiento de datos y mecanismos de autorización (Congreso de la República de Colombia, 2012).

Adicionalmente, la Ley 1273 de 2009 incorporó al Código Penal colombiano el bien jurídico de la protección de la información y de los datos, tipificando conductas como el acceso abusivo a sistemas informáticos y la interceptación de datos, disposiciones directamente relacionadas con los intentos de acceso no autorizado detectados tras el incidente de phishing reportado por la organización (Congreso de la República de Colombia, 2009).

En el ámbito internacional, la norma ISO/IEC 27001:2022 constituye el estándar de referencia para la implementación de un sistema de gestión de seguridad de la información, proporcionando un marco de controles aplicable a la gestión de activos, accesos, criptografía y continuidad del negocio (ISO/IEC, 2022). Dado que CompraYa Online procesa pagos electrónicos mediante una pasarela externa, resulta igualmente aplicable el estándar PCI DSS, orientado específicamente a la protección de los datos de tarjetahabientes en organizaciones que almacenan, procesan o transmiten información de tarjetas de pago (PCI Security Standards Council, 2022).

Tabla 1.

Normatividad aplicable

Norma o estándar	Propósito	Aplicabilidad en la organización
Ley 1581 de 2012	Establece el régimen general de protección de datos personales en Colombia.	Aplica directamente a la administración de la base de datos de más de 180.000 clientes registrados por CompraYa Online.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012, definiendo autorización, políticas de tratamiento y transferencia de datos.	Exige a la organización contar con políticas formales de tratamiento de datos, actualmente inexistentes.
Ley 1273 de 2009	Tipifica los delitos informáticos en Colombia, incluyendo el acceso abusivo a sistemas y la interceptación de datos.	Relevante frente a los intentos de acceso no autorizado a cuentas corporativas identificados en la organización.
ISO/IEC 27001:2022	Estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI).	Sirve como referencia para estructurar la gestión de activos, riesgos y controles ante la ausencia de un SGSI formal.
PCI DSS v4.0	Estándar de seguridad de datos para la industria de tarjetas de pago.	Aplica al procesamiento de pagos electrónicos a través de la pasarela utilizada por CompraYa Online.

La revisión de estas normas y estándares resulta particularmente importante para CompraYa Online porque evidencia brechas de cumplimiento

actuales: la ausencia de una política formal de clasificación de la información contraviene las buenas prácticas exigidas por la ISO/IEC 27001, mientras que la falta de autenticación multifactor en accesos administrativos y de evaluaciones periódicas a las integraciones con terceros representa un riesgo frente a los requisitos de PCI DSS. En conjunto, este marco normativo constituye el referente que debe orientar la construcción de políticas y controles en etapas posteriores del presente trabajo.

Descripción de la Organización

CompraYa Online S.A.S. es una empresa colombiana de comercio electrónico que opera exclusivamente a través de canales digitales, comercializando productos de tecnología, hogar, moda, deportes y accesorios para clientes en todo el territorio nacional. Fundada hace ocho años, la organización cuenta actualmente con aproximadamente 240 colaboradores, distribuidos en las áreas comercial, tecnológica, administrativa, logística y de atención al cliente.

La empresa procesa en promedio 6.500 pedidos semanales y administra una base de datos que supera los 180.000 clientes registrados, cifras que evidencian el volumen operativo y la relevancia de la información personal y transaccional que gestiona. Su crecimiento ha estado impulsado por el

incremento de las compras digitales en el país y por el fortalecimiento continuo de sus plataformas tecnológicas.

En términos de estructura organizacional, CompraYa Online cuenta con una Gerencia General y direcciones especializadas en las áreas Comercial, de Tecnología, Marketing Digital, Servicio al Cliente, Gestión Logística, Compras y Proveedores, Talento Humano, Contabilidad y Finanzas, y Analítica de Datos. El área de tecnología, responsable de la operación y seguridad de las plataformas digitales, está conformada por un director, cuatro desarrolladores, dos administradores de infraestructura, dos analistas de soporte y un analista de bases de datos.

La infraestructura tecnológica de la organización incluye 120 computadores de escritorio y 95 portátiles, una plataforma web de comercio electrónico, una aplicación móvil para clientes, plataformas CRM y ERP, un sistema de gestión de inventarios, una pasarela de pagos electrónicos, un sistema de gestión logística, infraestructura alojada en la nube pública, una base de datos centralizada de clientes, una plataforma de marketing digital, correo electrónico corporativo, un sistema de respaldo de información, redes WiFi corporativas y un sistema de monitoreo de infraestructura.

Entre sus procesos principales se encuentran la gestión de ventas en línea, la gestión de clientes, el procesamiento de pagos mediante pasarelas

externas, la gestión logística de almacenamiento y despacho de pedidos, el marketing digital y la analítica de datos orientada al análisis del comportamiento de consumo. La misión de la organización es ofrecer una experiencia de compra digital segura, eficiente y confiable, mientras que su visión apunta a consolidarse como una de las principales plataformas de comercio electrónico del país, garantizando disponibilidad, confianza y protección de la información.

Problemática identificada

El diagnóstico inicial realizado por la firma consultora especializada evidenció múltiples debilidades en la gestión de la seguridad de la información de CompraYa Online S.A.S., las cuales, analizadas en conjunto, configuran un escenario de riesgo significativo para una organización cuya operación depende por completo de canales digitales. Entre los hallazgos más relevantes se encuentra la ausencia de una política formal de clasificación de la información y de un inventario actualizado de activos, lo que impide a la organización priorizar adecuadamente sus esfuerzos de protección.

Se identificó además que algunos colaboradores utilizan dispositivos personales para acceder a sistemas corporativos y herramientas externas para compartir información laboral, prácticas que amplían la superficie de exposición fuera del perímetro controlado por la organización. A esto se suma que algunos

usuarios mantienen privilegios de acceso superiores a los requeridos por sus funciones, que las contraseñas de ciertos sistemas críticos no cumplen requisitos mínimos de complejidad, y que no todos los accesos administrativos cuentan con autenticación multifactor, lo cual incrementa la probabilidad de accesos no autorizados.

La organización tampoco cuenta con un procedimiento formal para la gestión de incidentes de ciberseguridad, y aunque los respaldos de información

se realizan diariamente, no se efectúan pruebas periódicas de restauración, situación que compromete la capacidad real de recuperación ante un evento adverso. De igual forma, las integraciones con terceros no han sido evaluadas recientemente desde la perspectiva de seguridad, lo que resulta especialmente relevante considerando que la operación de la empresa depende de pasarelas de pago y servicios en la nube prestados por proveedores externos.

Esta problemática se ha materializado en eventos concretos durante los últimos tres años: una interrupción prolongada de la plataforma web por sobrecarga de solicitudes durante una campaña promocional, un intento de fraude mediante correo electrónico que derivó en intentos de acceso no autorizado a cuentas corporativas, fallas en la aplicación móvil originadas en una actualización incorrecta, la exposición accidental de información de clientes por

una configuración indebida en un servicio en la nube, y vulnerabilidades en una integración con un proveedor externo que afectaron procesos operativos. Estos eventos, sumados a una cultura organizacional en la que la seguridad es percibida como responsabilidad exclusiva del área tecnológica y en la que las capacitaciones son esporádicas, justifican el desarrollo de un análisis técnico que permita a la organización identificar sus activos críticos, comprender las amenazas y vulnerabilidades que los afectan, y avanzar hacia una gestión de riesgos más estructurada, en un contexto además de expansión regional y crecimiento acelerado proyectado por la alta dirección.

Identificación y valoración de activos

La identificación y valoración de activos constituye una etapa fundamental para la gestión de la seguridad de la información, ya que permite reconocer los recursos que sustentan la operación de la organización y priorizar los esfuerzos de protección sobre aquellos de mayor valor o criticidad (ISO/IEC, 2022a). Para el caso de CompraYa Online S.A.S., los activos se clasificaron en las categorías de información, software, servicios, infraestructura y personas, considerando su rol dentro de los procesos de ventas en línea, gestión de clientes, procesamiento de pagos, gestión logística y analítica de datos.

La valoración de criticidad se realizó de manera cualitativa, considerando el impacto que tendría sobre la organización la pérdida de confidencialidad, integridad o disponibilidad de cada activo, así como su relación directa con la operación comercial y con la información de los clientes.

Tabla 2.

Inventario de activos

Activo	Tipo	Descripción	Criticidad
Base de datos centralizada de clientes	Digital	Almacena datos personales, de contacto e historial de compras de más de 180.000 clientes.	Alta
Plataforma web de comercio electrónico	Digital	Canal principal de ventas en línea; soporta el procesamiento de pedidos.	Alta
Aplicación móvil para clientes	Digital	Canal alterno de venta y atención utilizado por los clientes desde dispositivos móviles.	Alta
Pasarela de pagos electrónicos	Digital	Gestiona las transacciones financieras de los clientes mediante un proveedor externo.	Alta
Plataforma ERP	Digital	Administra procesos administrativos, financieros y de inventarios de la organización.	Media
Plataforma CRM	Digital	Gestiona la relación e interacción con los clientes y sus preferencias.	Media

Activo	Tipo	Descripción	Criticidad
Infraestructura en la nube pública	Digital	Aloja aplicaciones, servicios y bases de datos de la organización.	Alta
Sistema de gestión logística	Digital	Coordina el almacenamiento, despacho y seguimiento de pedidos.	Media
Correo electrónico corporativo	Digital	Canal de comunicación interna y externa, utilizado también en procesos administrativos.	Media
Personal del área de Tecnología	Humano	Equipo responsable del desarrollo, soporte e infraestructura tecnológica de la organización.	Alta

De acuerdo con la valoración realizada, los activos más críticos de CompraYa Online son la base de datos centralizada de clientes, la plataforma web de comercio electrónico, la aplicación móvil, la pasarela de pagos electrónicos, la infraestructura alojada en la nube pública y el personal del área de tecnología. Estos activos concentran la mayor criticidad porque de ellos depende directamente la capacidad de la organización para operar, generar ingresos y proteger la información personal y financiera de sus clientes; su afectación, como lo evidencian los eventos ocurridos durante los últimos tres años, tiene un impacto directo sobre la continuidad del negocio, la confianza de los clientes y el cumplimiento normativo de la organización.

Análisis de amenazas y vulnerabilidades

A partir del inventario de activos y de los hallazgos del diagnóstico inicial, se identificaron las principales amenazas y vulnerabilidades que afectan a CompraYa Online S.A.S. Una amenaza representa un evento con potencial de causar daño a un activo, mientras que la vulnerabilidad corresponde a la debilidad específica que permitiría que dicha amenaza se materialice (NIST, 2012); su análisis conjunto resulta indispensable para orientar la posterior valoración de riesgos de la organización.

Tabla 3.

Amenazas y vulnerabilidades

Activo	Amenaza	Vulnerabilidad
Base de datos centralizada de clientes	Exposición o filtración no autorizada de información de clientes.	Ausencia de una política formal de clasificación de la información y de criterios homogéneos de protección entre áreas.
Plataforma web de comercio electrónico	Interrupción del servicio por sobrecarga de solicitudes (denegación de servicio).	Capacidad de la plataforma insuficiente para picos de demanda durante campañas promocionales de alto impacto.
Aplicación móvil para clientes	Fallas funcionales que impiden la operación normal de la aplicación.	Ausencia de procedimientos rigurosos de prueba y control de

Activo	Amenaza	Vulnerabilidad
		calidad previos al despliegue de actualizaciones.
Correo electrónico corporativo / cuentas de usuario	Suplantación de identidad (phishing) y acceso no autorizado a cuentas corporativas.	Contraseñas sin requisitos mínimos de complejidad y ausencia de autenticación multifactor en todos los accesos administrativos.
Infraestructura en la nube pública	Exposición accidental de información por configuración indebida de servicios.	Falta de revisión periódica de las configuraciones de seguridad de los servicios en la nube.
Integraciones con proveedores externos	Compromiso de procesos operativos a través de vulnerabilidades en servicios de terceros.	Integraciones con terceros que no han sido evaluadas recientemente desde la perspectiva de seguridad.
Accesos de usuarios internos	Uso indebido o abuso de privilegios de acceso a la información.	Usuarios con privilegios superiores a los requeridos por sus funciones actuales.
Información corporativa compartida	Fuga de información a través de canales no controlados por la organización.	Uso de dispositivos personales y herramientas externas para acceder o compartir información laboral.
Sistema de respaldo de información	Pérdida definitiva de información ante un incidente, por fallas en la recuperación.	Ausencia de pruebas periódicas de restauración de los respaldos realizados diariamente.

Del análisis anterior se observa que las situaciones de mayor riesgo para CompraYa Online se concentran en tres frentes. En primer lugar, la protección de la información de clientes, dado que tanto la ausencia de clasificación de la

información como las debilidades en la configuración de servicios en la nube ya derivaron en un evento real de exposición de datos. En segundo lugar, la gestión de accesos, pues la combinación de privilegios excesivos, contraseñas débiles y autenticación multifactor incompleta incrementa significativamente la probabilidad de que un ataque de phishing, como el ya ocurrido, derive en un compromiso mayor de las cuentas corporativas. En tercer lugar, la disponibilidad de las plataformas digitales, considerando que tanto la sobrecarga de la plataforma web como las fallas de la aplicación móvil han afectado directamente la capacidad de la organización para generar ventas, un riesgo especialmente relevante dado el crecimiento acelerado y la expansión regional proyectados por la alta dirección.

Análisis y gestión de riesgos

Análisis.

A partir de la problemática descrita y del inventario de activos, amenazas y vulnerabilidades presentado en la sección anterior, se desarrolla a continuación una metodología sistemática de análisis y gestión de riesgos para CompraYa Online S.A.S., orientada a estructurar planes de tratamiento robustos y alineados con los estándares internacionales y el marco legal vigente.

Metodología de Análisis de Riesgos

La presente evaluación de riesgos se estructura de manera rigurosa bajo los lineamientos metodológicos internacionales de la norma de gestión de riesgos ISO 31000 y el estándar sectorial de seguridad de la información ISO/IEC 27005. El enfoque adoptado es de carácter cuali-cuantitativo, fundamentando la estimación de la severidad del riesgo mediante el cálculo del riesgo inherente, el cual se define formalmente como el producto directo de dos variables esenciales: la probabilidad de ocurrencia del escenario y el impacto potencial que este ejercería sobre los activos informáticos y objetivos del negocio.

Valoración de la Probabilidad: Se determinó utilizando una escala cualitativa de tres niveles: 1 (Baja), 2 (Media) y 3 (Alta). Para la asignación de este factor se tomaron como criterios de referencia la frecuencia histórica documentada de incidentes en la organización, el nivel de exposición de vulnerabilidades específicas (tales como accesos de administración sin autenticación multifactor o ausencia de políticas de contraseñas) y el grado de resistencia o madurez cultural de los colaboradores frente a controles de seguridad.

Valoración del Impacto: Se categorizó bajo la misma escala de tres niveles: 1 (Bajo), 2 (Medio) y 3 (Alto). Esta variable mide la degradación potencial sobre la tríada fundamental de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad (CIDA). De forma complementaria, el impacto evalúa las consecuencias financieras directas por pérdidas transaccionales, las implicaciones reputacionales derivadas de la pérdida de confianza de los clientes, y la exposición a severas sanciones legales bajo el marco de la Ley 1581 de 2012 en Colombia ante vulneraciones a la privacidad de datos personales.

El producto resultante de la multiplicación de ambas variables (Probabilidad × Impacto) consolida una matriz de criticidad donde el nivel de riesgo se clasifica finalmente en: Bajo (valores de 1-2), Medio (valores de 3-4) y Alto (valores de 6-9).

Identificación, Evaluación y Matriz de Criticidad

A partir del cruce entre el diagnóstico situacional y los eventos históricos, se formalizan y evalúan cinco grandes escenarios de riesgo inherente dentro de la operación transaccional de la empresa:

R1: Indisponibilidad Crítica de Plataforma

Descripción: Interrupciones operativas prolongadas causadas por sobrecarga de solicitudes en campañas comerciales y actualizaciones erróneas en entornos productivos de la app móvil (Eventos históricos 1 y 3).

Evaluación: Probabilidad Alta (3) × Impacto Alto (3) = **Riesgo Inherente Alto (9)**

R2: Brecha y Fuga de Datos Personales

Descripción: Exposición pública accidental de registros de clientes en la nube (Evento histórico 4), agravada por la total ausencia de políticas formales para la clasificación de información sensible.

Evaluación: Probabilidad Media (2) × Impacto Alto (3) = **Riesgo Inherente Alto (6)**

R3: Compromiso de Identidades por Ingeniería Social (Phishing)

Descripción: Suplantación de pasarelas de pago externas dirigida a colaboradores (Evento histórico 2). Vulnerabilidad crítica debido a la falta de autenticación multifactor (MFA) administrativa y contraseñas débiles.

Evaluación: Probabilidad Alta (3) × Impacto Alto (3) = **Riesgo Inherente Alto (9)**

R4: Fallas por Dependencia de Proveedores Tecnológicos

Descripción: Vulnerabilidades técnicas explotadas en integraciones con terceros que impactan procesos operativos de comercio (Evento histórico 5). Confianza desmedida en software externo sin evaluaciones recientes.

Evaluación: Probabilidad Media (2) × Impacto Medio (2) = **Riesgo Inherente Medio (4)**

R5: Fuga Interna de Información por Prácticas de Shadow IT

Descripción: Uso generalizado de dispositivos personales (BYOD) sin supervisión técnica y transferencia de datos corporativos a través de herramientas públicas no autorizadas.

Evaluación: Probabilidad Alta (3) × Impacto Medio (2) = **Riesgo Inherente Alto (6)**

Estrategias de Gestión y Planes de Mitigación

Para contrarrestar y reducir los niveles de los riesgos críticos identificados, la alta dirección debe adoptar una estrategia de tratamiento activa enfocada en mitigar la probabilidad y contener el impacto de los incidentes.

Tratamiento de R1 y R3 (Seguridad Tecnológica): Es de carácter urgente revocar los privilegios administrativos excesivos de los usuarios implementando el principio de mínimo privilegio y desplegar de forma obligatoria soluciones de Autenticación Multifactor (MFA) en todos los accesos a la nube,

CRM, ERP y consolas corporativas. Se deben configurar directrices estrictas de complejidad para las contraseñas. Respecto a la estabilidad de la plataforma de ventas, se requiere el aprovisionamiento de arquitectura elástica con escalado automático (Auto-scaling) en la nube y la adopción de pipelines de integración y despliegue continuo (CI/CD) con pruebas automatizadas que bloqueen compilaciones defectuosas antes de llegar a producción.

Tratamiento de R2, R4 y R5 (Gobernanza y Cumplimiento): Se debe estructurar un programa formal de Gobierno de Datos que inicie con un inventario de activos de información y una Política de Clasificación de la Información. La infraestructura en la nube debe auditarse continuamente mediante herramientas de gestión de postura de seguridad (CSPM) para prevenir malas configuraciones. Para neutralizar el Shadow IT, se debe regular el modelo BYOD mediante la obligatoriedad de soluciones de Gestión de Dispositivos Móviles (MDM), aislando los datos corporativos de los personales. Asimismo, el proceso de respaldo de datos diarios debe reforzarse mediante la ejecución trimestral de simulacros formales de restauración en entornos de prueba. Finalmente, toda integración con API de terceros debe condicionarse a evaluaciones anuales de seguridad y acuerdos de niveles de servicio (SLA) con penalidades por brechas cibernéticas.

Transformación de la Cultura de Riesgo: La organización debe erradicar la falsa premisa de que la seguridad concierne únicamente a TI. Se implementará un plan periódico de concienciación y sensibilización en técnicas de ingeniería social e higiene digital para el 100% de los colaboradores, promoviendo reportes oportunos ante anomalías.

Matriz de riesgos

Tabla 4

Matriz de riesgos

Riesgo	Impacto	Probabilidad	Nivel
R1: Indisponibilidad Crítica de Plataforma	3	3	9
R2: Brecha y Fuga de Datos Personales	3	2	6
R3: Compromiso de Identidades (Phishing)	3	3	9
R4: Fallas por Dependencia de Terceros	2	2	4
R5: Fuga Interna (Shadow IT)	2	3	6

La escala de valoración utilizada corresponde a una calificación cualitativa de probabilidad e impacto en un rango de 1 a 3, cuyo producto determina el nivel

de riesgo en una escala de 1 a 9, clasificada en tres zonas: riesgo bajo (1-2), riesgo medio (3-4) y riesgo alto (6-9).

De acuerdo con esta clasificación, los riesgos R1 (Indisponibilidad Crítica de Plataforma) y R3 (Compromiso de Identidades por Phishing) presentan el nivel más alto (9), al combinar una probabilidad alta con un impacto alto, por lo que constituyen la primera prioridad de tratamiento para CompraYa Online. Los riesgos R2 (Brecha y Fuga de Datos Personales) y R5 (Fuga Interna por Shadow IT) se ubican en un nivel alto (6) y representan la segunda prioridad de atención: el primero por el impacto máximo asociado a posibles sanciones y pérdida de confianza de los clientes, y el segundo por su alta frecuencia asociada al uso extendido de dispositivos personales. Finalmente, el riesgo R4 (Fallas por Dependencia de Terceros) se clasifica en un nivel medio (4), por lo que puede gestionarse mediante controles contractuales y evaluaciones periódicas a mediano plazo.

Este ordenamiento permite a CompraYa Online dirigir sus recursos de mitigación hacia los escenarios de mayor severidad —la indisponibilidad de la plataforma y el compromiso de identidades por phishing—, sin descuidar el tratamiento de los riesgos de nivel medio, en el marco de un plan de gestión de riesgos estructurado y priorizado.

Políticas y controles de seguridad propuestas

Políticas:

Las políticas son las reglas que la organización debe exigir a sus colaboradores y proveedores para reducir los riesgos identificados en CompraYa Online:

Política de Control de Accesos: Define que ningún usuario debe tener más permisos de los estrictamente necesarios para su cargo (principio de mínimo privilegio). Obliga a no compartir cuentas y a revocar accesos inmediatamente cuando alguien cambia de rol o sale del equipo.

Política de Tratamiento y Privacidad de Datos: Establece cómo se debe capturar, almacenar y proteger la información personal de los clientes y empleados, asegurando el cumplimiento de la Ley 1581 de 2012.

Política de Uso Aceptable de Activos y BYOD: Regula qué se puede y qué no se puede hacer con los equipos de la empresa, y establece reglas estrictas para el uso de dispositivos personales en el acceso a sistemas corporativos.

Política de Gestión de Incidentes: Define quién hace qué, a quién se debe llamar y cómo se debe contener el daño en el momento exacto en que ocurre un ciberataque o una falla crítica en las plataformas de CompraYa Online.

Controles:

Los controles son los mecanismos técnicos o físicos que hacen que las políticas se cumplan en la operación real de la organización. Se dividen en preventivos, detectivos y correctivos:

Controles de autenticación (preventivos): implementación obligatoria de autenticación multifactor (MFA/2FA) para todos los sistemas críticos, y configuración de contraseñas robustas con caducidad programada.

Controles de infraestructura y red (preventivos y detectivos): uso de firewalls de aplicaciones web (WAF) para bloquear tráfico malicioso hacia la plataforma de comercio electrónico, y sistemas de prevención de intrusos (IPS) y monitoreo de la nube para detectar configuraciones inseguras.

Controles de protección de datos (preventivos): cifrado (encriptación) de la base de datos de clientes tanto en reposo como en tránsito.

Controles de resiliencia (correctivos): sistemas de copias de seguridad (backups) automatizados, inmutables y aislados de la red principal.

Controles de talento humano: capacitación constante al personal para identificar correos fraudulentos (phishing) y técnicas de ingeniería social.

Gestión de incidentes y continuidad del negocio

La gestión de incidentes y la continuidad del negocio son dos disciplinas complementarias, pero con enfoques distintos: la gestión de incidentes es la respuesta táctica para contener un evento en el momento en que ocurre, mientras que la continuidad del negocio es la estrategia que asegura que la operación de CompraYa Online no se detenga por completo mientras dura la crisis.

A continuación, se detalla cómo se estructuran ambas prácticas para la organización, con base en los marcos de referencia internacionales ISO/IEC 27035 e ISO 22301.

Tabla 5

Incidentes potenciales

Incidente	Descripción	Impacto
Ataque de phishing a cuentas corporativas	Un colaborador recibe un correo fraudulento que compromete sus credenciales de acceso a los sistemas corporativos.	Acceso no autorizado, fuga de información, afectación de la operación y posibles sanciones legales.

Indisponibilidad de la plataforma web	Caída del sitio web por sobrecarga de solicitudes o ataques de denegación de servicio durante campañas comerciales.	Interrupción de ventas, pérdidas económicas y afectación de la imagen corporativa.
Exposición de datos en la nube	Configuración incorrecta de servicios en la nube que permite el acceso no autorizado a información de clientes.	Violación de la confidencialidad, incumplimiento de la Ley 1581 de 2012 y pérdida de confianza de los clientes.
Falla de proveedores o integraciones externas	Vulnerabilidades o interrupciones en servicios de terceros como la pasarela de pagos o proveedores en la nube.	Afectación de procesos críticos, retraso en las transacciones y disminución de la disponibilidad del servicio.

Tabla 6

Plan Básico de Respuesta

Fase	**Acción**
Preparación	Definir el equipo responsable, establecer procedimientos, capacitar al personal y mantener herramientas de monitoreo y respaldo actualizadas.
Identificación	Detectar el incidente mediante alertas, monitoreo y reportes de usuarios; analizar el alcance y la criticidad del evento.
Contención	Aislar los sistemas afectados, bloquear accesos comprometidos y evitar la propagación del incidente hacia otros activos.
Erradicación y recuperación	Eliminar la causa del incidente, restaurar los servicios mediante respaldos verificados y validar el funcionamiento normal de la plataforma.

Fase	Acción
Lecciones aprendidas	Documentar el incidente, evaluar la respuesta realizada, actualizar procedimientos y fortalecer los controles de seguridad para prevenir recurrencias.

La gestión de incidentes en CompraYa Online S.A.S. se fundamenta en una respuesta organizada que permita minimizar el impacto de los eventos de seguridad sobre los activos críticos de la organización. Ante cualquier incidente, el equipo de tecnología deberá activar el procedimiento establecido, identificar rápidamente el origen del problema y aplicar medidas de contención para impedir que el incidente afecte otros sistemas o comprometa información adicional. Una vez controlada la situación, se ejecutarán las actividades de erradicación y recuperación utilizando copias de seguridad verificadas y restaurando la operación de los servicios afectados.

Para garantizar la continuidad del negocio, la organización implementará un Plan de Continuidad del Negocio (BCP) basado en la norma ISO 22301 y un Plan de Recuperación ante Desastres (DRP). Estos planes contemplan la definición de procesos críticos, tiempos máximos de recuperación (RTO), puntos objetivos de recuperación de datos (RPO), infraestructura redundante en la nube, respaldos automatizados y simulacros periódicos para validar la efectividad de los procedimientos. Asimismo, la empresa mantendrá un

monitoreo continuo de sus plataformas, revisiones periódicas de seguridad, autenticación multifactor, controles de acceso y capacitación permanente del personal, fortaleciendo así su capacidad para responder oportunamente ante incidentes y asegurar la continuidad de sus operaciones comerciales aun en situaciones de crisis.

Cultura organizacional en ciberseguridad

Tabla 7

Hallazgos organizacionales

Situación observada	Riesgo asociado
La seguridad de la información es percibida como responsabilidad exclusiva del área de Tecnología.	Baja participación del resto de la organización en la prevención y detección de incidentes de seguridad.
Las capacitaciones en ciberseguridad son esporádicas y no abarcan a todos los colaboradores.	Mayor probabilidad de éxito de ataques de phishing, ingeniería social y errores humanos.
Se utilizan dispositivos personales y herramientas no autorizadas para acceder o compartir información corporativa.	Fuga de información, pérdida de control sobre los datos y aumento del riesgo de Shadow IT.
No existe una cultura de reporte oportuno de incidentes o errores de seguridad.	Retraso en la detección y contención de incidentes, incrementando el impacto sobre la operación.

Tabla 8

Recomendaciones de mejora

Hallazgo	Recomendación
La seguridad es vista como responsabilidad exclusiva del área de TI.	Implementar una estrategia de responsabilidad compartida, involucrando a todas las áreas en la protección de la información.
Capacitaciones insuficientes en ciberseguridad.	Establecer un programa permanente de capacitación y campañas de concientización sobre phishing, ingeniería social y buenas prácticas digitales.
Uso de dispositivos personales y aplicaciones no autorizadas.	Implementar una política BYOD con herramientas MDM y restringir el uso de aplicaciones externas para el manejo de información corporativa.
Ausencia de una cultura de reporte de incidentes.	Promover una cultura de "cero culpa" que incentive el reporte inmediato de errores o incidentes sin temor a sanciones, facilitando una respuesta temprana.

Fortalecer la cultura organizacional en ciberseguridad permitirá que la protección de la información deje de depender únicamente de controles tecnológicos y se convierta en un compromiso de todos los colaboradores. La implementación de programas permanentes de capacitación incrementará la capacidad del personal para identificar amenazas como el phishing, reducir

errores humanos y aplicar buenas prácticas de seguridad en las actividades diarias.

Asimismo, promover una cultura de responsabilidad compartida permitirá que cada área de la organización participe activamente en la protección de los activos de información, integrando la seguridad desde el diseño de los procesos y proyectos. La adopción de políticas claras sobre el uso de dispositivos personales, el manejo de la información y el control de accesos reducirá significativamente la exposición a riesgos derivados del Shadow IT y de accesos no autorizados.

Por otra parte, fomentar una cultura de reporte temprano de incidentes, basada en un enfoque de aprendizaje y mejora continua en lugar de sanciones, facilitará la detección oportuna de amenazas y permitirá responder con mayor rapidez antes de que un incidente afecte la continuidad del negocio. Finalmente, estas acciones fortalecerán el cumplimiento de estándares como ISO/IEC 27001 e ISO 22301, mejorarán la resiliencia de CompraYa Online S.A.S. frente a ciberataques y aumentarán la confianza de clientes, proveedores y demás partes interesadas en la capacidad de la organización para proteger la información y garantizar la continuidad de sus servicios.

Conclusiones

El análisis realizado permitió evidenciar que la seguridad de la información en una organización de comercio electrónico no depende únicamente de la implementación de herramientas tecnológicas, sino de una adecuada gestión integral de los riesgos. La identificación y valoración de los activos críticos demostraron que la base de datos de clientes, la plataforma de comercio electrónico, la infraestructura en la nube y la pasarela de pagos representan los recursos más importantes para la continuidad del negocio, por lo que requieren controles de seguridad acordes con su nivel de criticidad. Este hallazgo demuestra que conocer y clasificar los activos es el punto de partida para establecer estrategias de protección efectivas.

El estudio de amenazas, vulnerabilidades y riesgos permitió comprender que muchas de las afectaciones sufridas por la organización tienen su origen en debilidades de gestión más que en fallas tecnológicas. La ausencia de políticas formales, la falta de autenticación multifactor en todos los accesos, el uso de dispositivos personales sin controles y la inexistencia de un procedimiento estructurado para responder a incidentes incrementan considerablemente la probabilidad de materialización de ataques. Esto evidencia que la prevención debe convertirse en un proceso permanente y no limitarse únicamente a la reacción cuando ocurre un incidente.

Otro aprendizaje importante es que la continuidad del negocio debe ser considerada un elemento estratégico para garantizar la operación de organizaciones cuyo funcionamiento depende completamente de plataformas digitales. La definición de procedimientos para la gestión de incidentes, la implementación de planes de continuidad y recuperación ante desastres, junto con la realización periódica de simulacros y pruebas de restauración, fortalecen la capacidad de la organización para recuperarse de eventos adversos en el menor tiempo posible y minimizar las pérdidas económicas, operativas y reputacionales.

Asimismo, el desarrollo del informe permitió concluir que la cultura organizacional representa uno de los pilares fundamentales de la ciberseguridad. La tecnología por sí sola no elimina los riesgos cuando los colaboradores desconocen las buenas prácticas o consideran que la seguridad es responsabilidad exclusiva del área de tecnología. Promover una cultura basada en la capacitación continua, la responsabilidad compartida y el reporte oportuno de incidentes permitirá disminuir significativamente los riesgos asociados al factor humano, que continúa siendo uno de los principales vectores de ataque en las organizaciones modernas.

Finalmente, el análisis realizado demuestra que la adopción de estándares internacionales como ISO/IEC 27001, ISO/IEC 27005, ISO 31000, ISO 22301 e ISO/IEC 27035 proporciona un marco sólido para fortalecer la gestión de la seguridad de la información y la continuidad del negocio. La implementación progresiva de las

políticas, controles y recomendaciones propuestas permitirá a CompraYa Online S.A.S. incrementar su nivel de madurez en ciberseguridad, mejorar el cumplimiento de la normatividad colombiana sobre protección de datos personales y aumentar la confianza de clientes, proveedores y demás partes interesadas. Como oportunidad de mejora, la organización debe establecer un proceso de revisión y actualización continua de sus controles, garantizando que estos evolucionen al mismo ritmo que las amenazas y los cambios tecnológicos, consolidando así una estrategia de seguridad sostenible y alineada con sus objetivos de crecimiento.

Referencias

Congreso de la República de Colombia. (2009). Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico denominado de la protección de la información y de los datos.

Congreso de la República de Colombia. (2012). Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

International Organization for Standardization. (2018). ISO/IEC 27000:2018 – Information technology — Security techniques — Information security management systems — Overview and vocabulary.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC). (2020). Modelo de Seguridad y Privacidad de la Información.

National Institute of Standards and Technology (NIST). (2012). Special Publication 800-30 Rev. 1 – Guide for Conducting Risk Assessments.

PCI Security Standards Council. (2022). Payment Card Industry Data Security Standard (PCI DSS), versión 4.0.

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (7ª ed.). Cengage Learning.

Organización Internacional de Normalización [ISO]. (2018). *Gestión del riesgo — Directrices* (ISO Standard No. 31000:2018). https://www.iso.org

Organización Internacional de Normalización [ISO]. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la gestión de riesgos de seguridad de la información* (ISO/IEC Standard No. 27005:2022). https://www.iso.org

Congreso de la República de Colombia. (17 de octubre de 2012). Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial No. 48.587*.