TRABAJO DE GRADO
Opción Seminario.

Informe Técnico de la empresa Supermercados Mercavida S.A.S.

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.
Jonathan Javier Sánchez Daza
Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen

El siguiente informe técnico se centró en el análisis de seguridad de la información para la empresa Supermercados Mercavida S.A.S., una cadena de supermercados regional dedicada a la venta de productos de consumo masivo, la cual durante los últimos años ha fortalecido sus operaciones mediante el uso de plataformas digitales. A partir del caso de estudio propuesto, se desarrolló la evaluación de la situación actual de la organización, con el fin de identificar los principales riesgos, vulnerabilidades y amenazas que puedan llegar a comprometer la confidencialidad, integridad y disponibilidad de la información.

Al llevar a cabo el análisis del caso, se hacen evidentes ciertas situaciones que fueron halladas tras una revisión inicial, la cual nos arroja varias novedades relacionadas con la ciberseguridad, entre ellas el uso de credenciales compartidas, la ausencia de políticas de clasificación de la información, retrasos en el despliegue de actualizaciones de seguridad y una limitada cultura organizacional en materia de seguridad de la información. Dichas situaciones reflejan que la protección de los activos de información no depende únicamente de la infraestructura tecnológica; esta también hace parte de procesos, políticas institucionales y el comportamiento de los colaboradores.

Partiendo de dicho diagnóstico, el informe presenta la identificación de los activos de información más relevantes, el análisis de amenazas y vulnerabilidades, la valoración de riesgos y la correspondiente formulación de políticas, controles y estrategias que están orientadas a fortalecer la postura de seguridad de la información en la organización. Como parte final, se plantean recomendaciones para la mejora de atención de incidentes, la continuidad del negocio y la cultura de ciberseguridad, lo cual contribuirá al fortalecimiento de la seguridad de la información y al cumplimiento de las buenas prácticas aplicadas al contexto organizacional.

Palabras clave

Seguridad de la información, Ciberseguridad, Gestión de riesgos, Activos de información, Controles de seguridad.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

Para entender los conceptos de ciberseguridad y seguridad de la información, debemos remontarnos a 5 décadas atrás, momento en el que nos hemos ido introduciendo en la era de la información y el conocimiento, lo cual ha sido impulsado por el uso masivo de sistemas de información, redes y computadores, la velocidad con la que esta era se ha ido extendiendo y el tipo de cambios que ha estado provocando en la sociedad y en la vida de las personas. Hace que dependamos crucialmente de dichos sistemas, de modo que una falla o una caída, ya sea de manera accidental o deliberada, genere graves consecuencias para un público específico o general, afectando una cadena de servicios. En este sentido, Cisco (2026) afirma que:

La ciberseguridad es la práctica de proteger sistemas, redes y programas contra ataques digitales. Estos ciberataques suelen tener como objetivo acceder, modificar o destruir información confidencial; extorsionar a los usuarios mediante ransomware; o interrumpir los procesos comerciales normales.(párr. 1).

Esta afirmación resulta pertinente para organizaciones, tales como una cadena de supermercados, con canales de venta presenciales y digitales como Supermercados MercaVida S.A.S. El cual combina procesos manuales con infraestructura tecnológica de alta exposición. En este contexto, la seguridad de la información adquiere un papel fundamental, ya que comprende el conjunto de medidas destinadas a proteger la información frente al acceso, uso, divulgación, modificación o interrupción no autorizados, garantizando su confidencialidad, integridad y disponibilidad para los usuarios autorizados (IBM, s. f.).

Dichos conceptos tienen como base central la tríada CID, que establece que un sistema de gestión adecuado debe garantizar la confidencialidad, la integridad y la disponibilidad de la información que procesa una organización. A continuación, se detallan estos tres atributos: La confidencialidad implica que solo las personas autorizadas puedan acceder a la información; la integridad garantiza que los datos no sean alterados de forma indebida; y la disponibilidad asegura que la información esté accesible cuando se requiera para la operación (Whitman & Mattord, 2021). Cuando cualquiera de estos atributos se ve comprometido, como por ejemplo el acceso no autorizado, o se presenta una interrupción en el servicio, se produce lo que se conoce como un incidente de seguridad.

Teniendo en cuenta lo anteriormente indicado, se tiene la base para la construcción de tres conceptos, los cuales están estrechamente relacionados entre sí: la amenaza, la vulnerabilidad y el riesgo. Una amenaza es cualquier acción o evento que se pueda aprovechar o explotar para causar daño a una empresa o individuo; la vulnerabilidad es una debilidad presente en la infraestructura, los sistemas o los procesos que puede ser

Explotada por terceros no autorizados. Por su parte, el riesgo representa la posibilidad de que una amenaza aproveche una vulnerabilidad y genere pérdidas o impactos negativos para la organización (Pathlock, 2025). Dicha relación explica por qué una buena gestión de riesgos no solo debe limitarse a la adquisición e instalación de tecnología de protección, sino que también nos exige aplicar correcciones a debilidades organizativas que permitan la materialización de amenazas.

Por último, los controles de seguridad son los parámetros usados para proteger los datos e información importante de una organización. Es cualquier medida que se pueda tomar para evitar o minimizar los riesgos de un ataque (IBM, s. f.). En el caso de la cadena de Supermercados MercaVida S.A.S., los controles de seguridad representan un elemento fundamental, debido al proceso de transformación y fortalecimiento digital que la organización ha experimentado durante los últimos años.

Marco normativo

En cuanto a la normatividad aplicable, se resalta la norma ISO/IEC 27001, dicha norma es la más usada a nivel internacional para sistemas de gestión de la seguridad de la información (SGSI). Esta norma proporciona un estándar de seguridad de la información aplicable a cualquier tipo de empresa (ISO, 2022). Dicha norma no impone controles obligatorios y rígidos; por el contrario, ayuda a las organizaciones a identificar y ser conscientes de los riesgos y sus debilidades, promoviendo buenas prácticas y el uso de SGI, acorde a cada organización.

Como norma complementaria, se destaca la 27032:2023, la cual es una guía de alto nivel que nos proporciona directrices específicas, centradas en la protección de amenazas de tipo web, al igual que nos brinda una visión general de seguridad en la red (ISO, s. f.). Este enfoque resulta especialmente útil para la cadena de supermercados, dado que su operación integra infraestructura tecnológica local y servicios basados en la web.

Por otra parte, la norma ISO 31000:2018 es un estándar internacional que establece principios, un marco de referencia y directrices para la gestión del riesgo en organizaciones de cualquier tipo y tamaño. Su enfoque permite identificar, analizar, evaluar y tratar los riesgos de manera sistemática, contribuyendo a una mejor toma de decisiones y al cumplimiento de los objetivos organizacionales (ISO, 2018). Esta norma es aplicable en el contexto de la cadena de supermercados para la gestión de los riesgos previamente identificados, facilitando la definición de estrategias y controles que permitan reducir su impacto y probabilidad de ocurrencia.

Partiendo del hecho de que la cadena de supermercados opera bajo el marco legal colombiano, se debe tener en cuenta la ley 1273 de 2009, la cual modificó el Código Penal para tipificar los delitos informáticos, entre ellos el acceso abusivo a sistemas, la interceptación de datos y el uso de software malicioso, estableciendo así responsabilidad penal frente a este tipo de conductas (Congreso de Colombia, 2009). De igual manera,

Resulta aplicable la Ley 1581 de 2012, la cual establece el régimen general de protección de datos personales y reconoce el derecho de los titulares a conocer, actualizar, rectificar y controlar el tratamiento de su información personal (Congreso de Colombia, 2012). Asimismo, el Decreto 1377 de 2013 reglamenta parcialmente esta ley, definiendo las condiciones para la obtención de la autorización de los titulares y las obligaciones de los responsables y encargados del tratamiento de los datos personales (Presidencia de la República de Colombia, 2013).

Tabla 1. Normatividad aplicable.

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***
ISO/IEC 27001:2022	Establecer los requisitos para implementar y mantener un SGSI basado en riesgos	Orienta la formalización de políticas y controles de seguridad, hoy ausentes o inconsistentes entre tiendas
ISO/IEC 27032:2023	Brindar directrices para la gestión de la ciberseguridad y la coordinación entre dominios de seguridad	Aplica a la protección de la plataforma de comercio electrónico, la infraestructura híbrida y las redes WiFi corporativa y de clientes
ISO 31000:2018	Proporciona principios y un proceso estructurado para la gestión de riesgos en cualquier tipo de organización.	Orienta la metodología de análisis y valoración de riesgos utilizada en el presente informe.
Ley 1581 de 2012	Regular la protección de datos personales y los derechos de los titulares de la información	Rige directamente el manejo de la base de más de 250.000 clientes registrados en el programa de fidelización

Decreto 1377 de 2013	Reglamentar los mecanismos de autorización y tratamiento de datos personales	Exige procedimientos claros para la recolección y uso de datos en canales digitales y de fidelización
Ley 1273 de 2009	Tipificar los delitos informáticos y sancionar el acceso abusivo a sistemas de información	Da fundamento legal para actuar frente a los accesos no autorizados detectados en la organización

La importancia de este marco normativo aplicado a los Supermercados MercaVida S.A.S. radica en que la cadena de supermercados trata información personal de clientes, información financiera y activos tecnológicos críticos para su operación diaria. El cumplimiento de leyes como la 1581 de 2012 es fundamental, ya que resulta relevante debido a que la compañía administra una base de datos superior a 250.000 registros, lo que obliga a contar con autorizaciones y políticas de tratamiento de datos, así como los mecanismos para poder atender los derechos de los titulares. Por otra parte, la ley 1273 de 2009 cobra importancia respecto a los hallazgos previos relacionados con el uso de credenciales compartidas y los intentos de acceso no autorizados. Como parte final, la implementación de estándares como la ISO 27001 o la ISO 27032 no constituye una obligación legal, pero dichos estándares ofrecen un marco de buenas prácticas, el cual facilita estructurar sistemas de gestión de riesgos y de seguridad de la información, lo cual permite la continuidad operativa de la cadena de supermercados.

Marco contextual

Descripción de la organización

Supermercados Mercavida S.A.S. es una cadena de supermercados establecida a nivel regional, con más de dos décadas de trayectoria dedicada a la comercialización de productos de consumo masivo. Su operación se encuentra distribuida en 15 establecimientos físicos, pero también soporta procesos digitales mediante el uso de plataformas de comercio electrónico, sistemas ERP, CRM, aplicaciones móviles y una infraestructura híbrida que integra recursos locales y servicios en la nube. El uso de esta infraestructura tecnológica permite a la compañía gestionar operaciones comerciales, logísticas y administrativas, lo cual convierte a la seguridad de la información en componente estratégico para la continuidad del negocio.

Problemática identificada

Tras el análisis realizado, se evidencia que la empresa Supermercados MercaVida S.A.S. presenta diversas debilidades en la gestión de seguridad de la información, las cuales representan un riesgo para la operación y continuidad del negocio. Entre estos hallazgos se tienen eventos como el uso compartido de credenciales administrativas, la ausencia de una política formal para la clasificación de la información, retrasos en la aplicación de actualizaciones de seguridad, la asignación de privilegios excesivos a algunos usuarios que no los requieren y la inexistencia de un doble factor de autenticación para todos los accesos administrativos.

También se identificó el uso de dispositivos personales para almacenar información corporativa, la ausencia de un procedimiento formal para la gestión de incidentes, la falta de pruebas documentadas de recuperación de respaldos, cuentas activas pertenecientes a excolaboradores y un inventario desactualizado de activos de información. Otro de los hallazgos evidencia el uso de dispositivos USB para el intercambio de información entre sedes, además de una arquitectura de red donde la infraestructura usada para conexión a red WIFI para clientes comparte componentes físicos con la red corporativa.

A todas estas vulnerabilidades se suman los incidentes ocurridos en años recientes, como intentos de acceso no autorizado mediante campañas de phishing, indisponibilidad de la plataforma de comercio electrónico durante jornadas de alta demanda, el acceso indebido ocasionado por uso de credenciales compartidas, la pérdida de equipos portátiles con información sensible e inconsistencias en inventarios ocasionadas por errores humanos.

Al observar todas estas novedades, relacionadas con seguridad de la información y desde la perspectiva organizacional, se hace evidente la falta de cultura de seguridad de la información, lo cual está caracterizado por una baja percepción del riesgo, una escasa capacitación en ciberseguridad y resistencia frente a controles adicionales de autenticación. Estas condiciones justifican la realización del presente informe técnico y la formulación

de medidas que permitan fortalecer la gestión de la seguridad de la información en la organización.

Identificación y análisis de activos

Inventario de activos

La identificación y el análisis de los activos de los Supermercados MercaVida S.A.S. Se da a partir de la información brindada en el caso, considerando los recursos tecnológicos que se implementan para soportar la operación diaria, los recursos humanos encargados de administrar y proteger dichos recursos. Para llevar a cabo esta identificación, se agruparon los activos en los 3 tipos de categorías: Activos digitales, tales como Bases de datos, sistemas y plataformas, Activos físicos, como infraestructura y equipos, por último Activos Humanos, es el personal y los respectivos roles clave con acceso privilegiado o responsabilidad directa sobre la seguridad de la información, al realizar la clasificación nos permite identificar que la protección de los datos y la organización no depende únicamente de la tecnología instalada, sino que también involucra a las personas que la operan y los procesos que dependen de ella.

Para poder determinar la criticidad de cada uno de los activos de la tabla, se tuvo en cuenta su relación con la tríada CID, así como el impacto que tendría su perdida, alteración, o indisponibilidad sobre la continuidad del negocio y el impacto sobre los clientes finales, los activos clasificados con criticidad alta son todos aquellos que su afectación comprometa directamente la operación comercial, los datos de clientes o la toma de decisiones de la organización, la criticidad media orientada cuando la afectación no detiene la operación, pero sí reduce su capacidad de respuesta.

Tabla 2. Inventario de activos

Activo	***Tipo***	***Descripción***	***Criticidad***
Base de datos de clientes	Digital	Contiene la información personal, historial de compras y datos de más de 250.000 clientes registrados.	Alta
ERP Empresarial	Digital	Sistema que integra los procesos administrativos, financieros, comerciales y operativos de la empresa.	Alta

Sistema de Gestión de Inventarios	Digital	Permite controlar el ingreso, almacenamiento, rotación y salida de productos.	Alta
Plataforma de Comercio Electrónico	Digital	Canal de ventas en línea utilizado por los clientes para realizar compras.	Alta
CRM y Plataforma de Fidelización	Digital	Gestiona la información de clientes, campañas comerciales y programas de fidelización.	Alta
Plataforma de Respaldo de Información	Digital	Realiza copias de seguridad y facilita la recuperación de la información ante incidentes.	Alta
Infraestructura híbrida (local y nube)	Físico	Infraestructura tecnológica que soporta el funcionamiento de los sistemas corporativos y servicios digitales.	Alta
Red WiFi Corporativa	Físico	Permite la conectividad entre usuarios, equipos y sistemas internos de la organización.	Alta

Sistema de Monitoreo de Operaciones	Digital	Supervisa el estado y disponibilidad de la infraestructura tecnológica y los servicios.	Alta
Sistema de Video vigilancia	Físico	Sistema de cámaras utilizado para la protección de las instalaciones y apoyo en investigaciones de incidentes.	Media
Equipos portátiles	Físico	60 computadores portátiles asignados a personal administrativo y supervisores regionales, algunos utilizados fuera de las instalaciones.	Media
Terminales POS	Físico	180 terminales de punto de venta distribuidas en las 15 tiendas para el procesamiento de transacciones.	Alta
Correo electrónico corporativo	Digital	Plataforma de comunicación institucional utilizada por los colaboradores para la gestión de proveedores y procesos internos.	Media
Información corporativa transportada entre sedes USB	Digital	Reportes, inventarios y documentos comerciales trasladados entre tiendas mediante dispositivos removibles.	Media

De los catorce activos identificados, el foco de mayor exposición se centra en tres activos que merecen una atención prioritaria, el primero de ellos es la base de datos, la cual contiene información de clientes, con un total de más 250.000 registros, la perdida o alteración no solo comprometería la operación comercial, sino que expondría a la organización a responsabilidades legales, frente a la normativa de protección de datos, llevando también a un daño reputacional frente a sus clientes y aliados comerciales.

El segundo activo es el ERP empresarial, al tratarse de un sistema que integra los procesos administrativos, financieros, comerciales y de orden operativo de las 15 tiendas a nivel regional. En caso de presentar una falla o que el sistema se vea comprometido, paralizaría simultáneamente varias funciones críticas del negocio, generando novedades en la facturación y el control financiero, lo que lo convierte en un activo cuya indisponibilidad tendría un efecto cascada en la operación.

El tercer activo es la plataforma de comercio electrónico, la cual se ha evidenciado vulnerable, con un evento de indisponibilidad ocurrido durante una jornada de promociones, al ser uno de los canales de crecimiento estratégico para los Supermercados MercaVida S.A.S. Y teniendo en cuenta los planes de la organización para llevar a cabo una ampliación significativa en las ventas digitales, su disponibilidad e integridad son determinantes tanto para los ingresos actuales, como para los planes de expansión.

Sumado a estos activos, se resalta la importancia de la gestión adecuada de los responsables, tales como el administrador de base de datos y el analista de seguridad informática, ya que son quienes garantizan de forma directa la integridad y la disponibilidad de los activos críticos. Ante un error, una ausencia o un compromiso de estos roles, puede generarse una afectación transversal en toda la infraestructura; incluso si la tecnología no presenta fallas, el foco se debe centrar en estos activos en conjunto.

Análisis de amenazas y vulnerabilidades

Tabla 3. Amenazas y vulnerabilidades

Activo	***Amenaza***	***Vulnerabilidad***
Base de datos de clientes CRM y fidelización	Fuga o acceso indebido a información de clientes	Ausencia de una política formal de clasificación de la información

ERP empresarial sistemas administrativos	Acceso no autorizado a información comercial	Uso de credenciales compartidas entre administradores de tienda
Red WiFi corporativa	Intrusión a la red interna desde la red de clientes	La red WiFi de clientes comparte infraestructura física con la red corporativa
Plataforma de respaldo de información	Pérdida permanente de información ante un incidente	Ausencia de pruebas documentadas recientes de restauración de los respaldos
Equipos portátiles asignados a personal rotativo	Pérdida o hurto del equipo fuera de las instalaciones	Falta de controles de cifrado y bloqueo en dispositivos que salen de la organización
Plataforma de comercio electrónico	Indisponibilidad del servicio por sobrecarga operativa	Falta de capacidad de escalamiento ante picos de demanda (ej. jornadas de promoción)
Correo electrónico corporativo	Ataques de phishing simulando proveedores estratégicos	Ausencia de campañas periódicas de sensibilización en ciberseguridad

Terminales POS	Explotación de vulnerabilidades técnicas conocidas	Retrasos en la instalación de actualizaciones de seguridad
ERP empresarial, sistemas administrativos	Uso indebido de accesos por personas no autorizadas	Cuentas activas pertenecientes a excolaboradores
Sistema de gestión de inventarios	Alteración o inconsistencia en los registros de inventario	Procedimientos inconsistentes entre tiendas para el manejo de información
Información transportada entre sedes mediante dispositivos USB	Fuga o pérdida de información durante el traslado	Uso de dispositivos USB sin control ni cifrado para transportar información

Se realizó el análisis y revisión del conjunto de amenazas y vulnerabilidades identificadas; se encontraron tres situaciones que concentran el mayor nivel de riesgo para los Supermercados MercaVida S.A.S. Esto con relación a la probabilidad de ocurrencia evidenciada en eventos reales ocurridos durante los últimos tres años y el impacto que estos tendrían en la operación y los clientes.

La primera situación es el acceso no autorizado al ERP mediante el uso de credenciales compartidas, este un riesgo que ya se materializó en un evento documentado, uno de los colaboradores accedió a información comercial haciendo uso de las credenciales de otro usuario, este tipo de vulnerabilidad es especialmente critica ya que facilita accesos indebidos, lo que impide que se tenga una debida trazabilidad de quien realizo una acción específica en el sistema, lo que complica realizar una investigación si se presenta un evento o incidente.

En segundo lugar, tenemos la posible fuga de información de la base de datos de clientes, dado que dicho activo concentra más de 250.000 registros, y aunque no se ha reportado ningún evento de fuga masiva, la ausencia de una política de clasificación de

información, sumada a la falta de segmentación en la red usada por los clientes y el personal de la organización, crea una ruta de exposición que, de llegar a materializarse, tendría consecuencias legales y reputacionales para la organización.

La tercera situación de alto riesgo es la indisponibilidad de los respaldos ante un incidente real, esto debido a que dichos respaldos nunca han sido probados, y se desconoce su verdadera capacidad de restauración, este tipo de vulnerabilidad por lo general suele pasar desapercibida hasta que se presenta una emergencia, si se presenta un ataque de ransomware o una falla en los servidores, es allí en el peor momento donde la organización podría descubrir que sus copias de seguridad no son recuperables, lo que pasaría de un incidente técnico manejable a un evento de indisponibilidad prolongada.

En cuanto a un nivel de riesgo intermedio, se ubican la indisponibilidad de la plataforma de comercio electrónico, la cual ya colapsó una vez durante una jornada de promociones, lo cual afectó directamente los ingresos de la cadena de supermercados; por otro lado, tenemos el phishing dirigido a los colaboradores, cuya principal debilidad no es de ámbito tecnológico, sino de cultura organizacional, la falta de sensibilización constante frente a correos fraudulentos; por último, riesgos como el uso de dispositivos de almacenamiento extraíbles sin control, las cuentas activas de colaboradores retirados, y la falta de actualización de sistemas POS, si bien dichos eventos tienen poca probabilidad de generar un indecente masivo, sin son una puerta a situaciones que combinadas entre sí puedan llegar a generar una afectación mayor en la operación.

Análisis y gestión de riesgos

Metodología de análisis

Para valorar los riesgos de Supermercados MercaVida S.A.S. se utilizó un enfoque cualitativo, coherente con los principios de gestión del riesgo establecidos en la norma ISO 31000:2018. La aplicación de esta metodología resulta apropiada cuando la organización no cuenta con series históricas de datos cuantificables sobre incidentes de seguridad. En el caso de la cadena de supermercados, la información disponible corresponde principalmente a un registro narrativo de los eventos ocurridos durante los últimos tres años, por lo que la valoración de los riesgos se fundamenta en el análisis de la evidencia disponible y en el juicio de expertos, permitiendo priorizar aquellos riesgos que requieren una atención más inmediata (ISO, 2018).

Esta valoración se realizó a partir de dos variables: la probabilidad, entendida como la posibilidad de que una amenaza se materialice al aprovechar una vulnerabilidad existente, y el impacto, definido como la magnitud de las consecuencias que dicha materialización podría generar sobre la operación, la información o los clientes de la organización (ISO,

2022). Ambas variables se calificaron mediante una escala cualitativa de tres niveles: baja, media y alta para la probabilidad, y bajo, medio y alto para el impacto. La adopción de este enfoque resulta apropiada debido a la dificultad de cuantificar con precisión las consecuencias de muchos riesgos de seguridad de la información; por ello, las organizaciones suelen apoyarse en información cualitativa, como la experiencia, el contexto y las tendencias históricas disponibles, para estimar el nivel de riesgo (IBM, 2025; ISO, 2022).

Para asignar la probabilidad de cada uno de los riesgos, se tomó como criterio principal la evidencia previamente registrada en el diagnóstico realizado para los Supermercados MercaVida S.A.S. Dichos riesgos están asociados a situaciones que ya se materializaron en algunos de los eventos que se han documentado durante los últimos tres años, los cuales se calificaron con probabilidad alta, mientras que aquellos vinculados a vulnerabilidades identificadas, pero sin un evento reciente se calificaron con probabilidad media o baja, esto en relación con la frecuencia en la que se presente dicha condición en la operación diaria. Para el impacto, se tuvo en consideración el efecto que tendría cada riesgo sobre tres dimensiones: la continuidad del negocio, la confidencialidad de la información y la exposición legal o reputacional de la organización.

El nivel de riesgo se obtuvo a partir del cruce entre las variables de probabilidad e impacto. De esta manera, una combinación de probabilidad alta e impacto alto, así como una probabilidad alta con impacto medio o una probabilidad media con impacto alto, se clasificó como riesgo alto; las combinaciones intermedias se categorizaron como riesgo medio; y aquellas en las que tanto la probabilidad como el impacto fueron bajos se clasificaron como riesgo bajo. Esta metodología facilita la construcción de la matriz de riesgos y la priorización de los eventos que requieren una atención inmediata, siguiendo un enfoque de gestión del riesgo alineado con los principios de la norma ISO 31000 y con metodologías de evaluación cualitativa ampliamente utilizadas (ISO Tools, 2021). Una vez elaborada la matriz, el análisis se centra en aquellos riesgos que presentan el mayor nivel de criticidad para definir las acciones de tratamiento correspondientes.

Matriz de riesgos

Tabla 4. Matriz de riesgos

Riesgo	***Impacto***	***Probabilidad***	***Nivel***
Acceso no autorizado al ERP mediante credenciales compartidas	Alto	Alta	Alto

Fuga o acceso indebido a la base de datos de clientes	Alto	Media	Alto
Pérdida de información ante fallas no detectadas en la restauración de respaldos	Alto	Media	Alto
Indisponibilidad de la plataforma de comercio electrónico por sobrecarga	Medio	Alta	Alto
Phishing dirigido a colaboradores simulando proveedores	Medio	Alta	Alto
Intrusión a la red corporativa a través de la red WiFi de clientes	Alto	Baja	Medio
Pérdida o hurto de equipos portátiles con información comercial	Medio	Media	Medio

Uso de accesos indebidos por cuentas activas de excolaboradores	Medio	Media	Medio
Fuga de información mediante dispositivos USB sin control	Medio	Baja	Bajo
Explotación de vulnerabilidades técnicas en terminales POS des actualizados	Bajo	Media	Bajo

El mayor riesgo para la cadena de Supermercados MercaVida S.A.S. Es el acceso no autorizado al sistema ERP mediante el uso de credenciales compartidas, este riesgo es clasificado con un impacto critico, dicha clasificación se otorga debido a un evento ya documentado, el cual hace parte de otros 4 eventos registrados, este corresponde a un acceso indebido a información comercial utilizando credenciales compartidas entre colaboradores, al tratarse de un riesgo cuya probabilidad es alta y comprobada el impacto es alto sobre la integridad de la información administrativa y financiera, dicho riesgo debe ser el primero en atenderse mediante controles de autenticación individual y logs de accesos.

En el nivel alto se agrupan cuatro riesgos que aunque no comparten el mismo origen si comparten la característica de tener la probabilidad considerable de ocurrencia, dado el contexto actual de la organización, estos riesgos son: la fuga de información de la base de datos de los clientes, la posible falla en la restauración de respaldos representan un impacto potencial, este dado al volumen de información gestionado y la dependencia total de respaldos ante cualquier incidente mayor, aun cuando su probabilidad se calificó como media al no existir todavía un evento de esta naturaleza. Por otra parte, la indisponibilidad de la plataforma de comercio electrónico y el phishing a colaboradores presentan una probabilidad alta, dichos riesgos ya se materializaron como eventos reales con un impacto medio, centrado principalmente en perdidas de origen comercial. Y en primera medida una posible cadena de acceso no autorizado.

Los riesgos de nivel medio como la intrusión a través de la red WiFi compartida, la pérdida de equipos portátiles y las cuentas activas de excolaboradores, no deben perder seguimiento, aunque su atención sé de después de gestionar los riesgos críticos y altos, no se deben dejar de lado, ya que estos actúan como puertas de entrada adicionales que podrían escalar su probabilidad si no se corrigen a tiempo. Por último tenemos los riesgos de nivel bajo como lo son el uso de USB sin control y el retraso en actualizaciones de terminales POS, estos riesgos representan la base sobre la cual deben construirse controles preventivos generales, incluso si su atención no es prioritaria como en los demás riesgos.

Políticas y controles de seguridad

Con base en la matriz de riesgos desarrollada en la sección anterior, a continuación se proponen las políticas y los controles de seguridad orientados a mitigar los riesgos priorizados en la cadena de Supermercados MercaVida S.A.S. Las políticas se plantean como directrices de carácter organizacional que orienten el comportamiento y los procedimientos de la empresa, mientras que los controles constituyen las medidas técnicas y operativas que servirán para materializar dichas políticas frente a cada riesgo específico.

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***
Política de gestión de identidades y accesos	Garantizar que cada colaborador cuente con credenciales individuales, con privilegios acordes a su rol y con revocación inmediata al finalizar su vínculo laboral	Acceso no autorizado al ERP mediante credenciales compartidas; accesos indebidos por cuentas activas de excolaboradores
Política de clasificación y protección de la información	Establecer niveles de confidencialidad para la información de clientes, comercial y financiera, definiendo quién puede acceder, modificar o compartir cada tipo de dato	Fuga o acceso indebido a la base de datos de clientes
Política de copias de seguridad y continuidad operativa	Asegurar la generación periódica de respaldos y la verificación documentada de su capacidad de restauración	Pérdida de información ante fallas no detectadas en la restauración de respaldos

Política de seguridad para dispositivos móviles y removibles	Regular el uso de portátiles fuera de las instalaciones y de dispositivos USB para el transporte de información entre sedes	Pérdida o hurto de equipos portátiles; fuga de información mediante USB
Política de sensibilización y cultura en ciberseguridad	Fortalecer de forma continua la capacidad de los colaboradores para reconocer intentos de phishing e ingeniería social	Phishing dirigido a colaboradores simulando proveedores

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***
Acceso no autorizado al ERP mediante credenciales compartidas	Implementación de doble factor de autenticación y eliminación de credenciales compartidas, asignando un usuario único por colaborador	Elimina la principal causa raíz identificada en el evento ya ocurrido y restablece la trazabilidad de cada acción dentro del sistema
Fuga o acceso indebido a la base de datos de clientes	Cifrado de la información sensible y segmentación de la red WiFi de clientes respecto de la red corporativa	Reduce la exposición del activo más crítico de la organización, cerrando la ruta de acceso que hoy comparten ambas redes
Falla en la restauración de respaldos	Pruebas periódicas y documentadas de restauración de copias de seguridad, con reporte formal de resultados	Garantiza que, ante un incidente real, la información pueda recuperarse efectivamente y no solo en teoría

Indisponibilidad de la plataforma de comercio electrónico	Monitoreo proactivo de capacidad y mecanismos de escalamiento de infraestructura ante picos de demanda	Previene la repetición del evento de sobrecarga ya registrado durante una jornada de promociones, protegiendo un canal estratégico de crecimiento

Las políticas y controles propuestos responde de manera directa a los riesgos priorizados en la matriz de riesgos, estas funcionan sin introducir medidas ajenas a la cadena de Supermercados MercaVida S.A.S. La política de gestión de identidades y accesos, junto con el doble factor de autenticación ataca de raíz al riesgo identificado como critico, el cual afecta el acceso no autorizado al sistema ERP, ya que elimina la condición que permitió que este riesgo se materializara en el pasado, la ausencia de credenciales individuales, al mismo tiempo esta política ataca un segundo riesgo de nivel medio las cuentas activas de excolaboradores, mediante el procedimiento formal para el retiro de accesos y credenciales a colaboradores no activos en la compañía.

La política de clasificación de la información, junto con el cifrado y la segmentación de red, reduce directamente el riesgo de fuga de la base de datos de clientes, calificado como Alto. Este control es particularmente relevante porque no solo protege la confidencialidad de los datos frente a accesos internos indebidos, sino que también corrige la debilidad estructural detectada en el diagnóstico: la coexistencia de la red Wifi de clientes con la infraestructura corporativa.

Por otra parte, la política de copias de seguridad y continuidad operativa, se materializa en pruebas periódicas de restauración, lo que disminuye el riesgo alto asociado a la posible perdida irreversible de información, transformando respaldos que hoy solo son rutina en una capacidad de recuperación verificada, de manera similar el monitoreo proactivo de capacidad reduce la probabilidad de que se presente de nuevo la indisponibilidad de la plataforma de comercio electrónico, riesgo que se materializó causando perdidas económicas en una fecha de promociones.

Finalmente, tenemos la política de dispositivos móviles y unidades extraíbles, junto con la política de sensibilización, actúan sobre los riesgos de nivel medio y bajo, como lo son la perdida de equipos portátiles, uso de dispositivos USB sin control y phishing simulando proveedores comerciales, si bien estos riesgos no representan el mayor impacto individual si contribuyen de manera acumulativa a ampliar el rango de exposición de la organización si se dejan sin atención, este conjunto de políticas y controles cubre la totalidad de los riesgos identificados en la matriz, dando prioridad a aquellos cuyo impacto es mayor continuando con los de un impacto medio, y por último se abordan los impactos bajos, teniendo siempre en mente el enfoque de gestión de riesgos desarrollado en la sección anterior.

Gestión de incidentes y continuidad del negocio

La cadena de Supermercados MercaVida S.A.S. actualmente no cuenta con un procedimiento formal para la gestión de incidentes, por lo que se propone adoptar un ciclo de cinco fases, las cuales son: detección, contención, erradicación, recuperación y lecciones aprendidas, alineando ello con las buenas prácticas internacionales para la gestión de incidentes de seguridad de la información.

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***
Acceso no autorizado al ERP mediante credenciales compartidas	Un colaborador o tercero ingresa al sistema ERP utilizando credenciales de otro usuario, accediendo a información comercial, financiera o administrativa sin autorización.	Alto
Fuga o filtración de la base de datos de clientes	Exposición no controlada de los datos personales y de compra de los más de 250.000 clientes registrados, ya sea por acceso indebido interno o por explotación de la segmentación deficiente entre la red corporativa y la red WiFi de clientes.	Alto
Cifrado malicioso de información por ransomware	Un ataque de ransomware compromete los servidores o la infraestructura híbrida de la organización, cifrando información crítica y dejando en evidencia la falta de pruebas de restauración de los respaldos.	Alto

Indisponibilidad de la plataforma de comercio electrónico	Caída o sobrecarga del canal de ventas en línea durante una jornada de alta demanda, similar al evento ya ocurrido durante una campaña de promociones, afectando directamente los ingresos digitales.	Medio

Tabla 8. Plan básico de respuesta

Fase	***Acción***
Detección	Identificar el incidente mediante el sistema de monitoreo de operaciones, alertas del área de tecnología o reportes de colaboradores; por ejemplo, un acceso inusual al ERP con credenciales compartidas o una caída de la plataforma de comercio electrónico.
Contención	Aislar de inmediato el sistema, cuenta o segmento de red afectado para evitar que el incidente se propague; por ejemplo, revocar las credenciales comprometidas del ERP o desconectar los servidores afectados por un posible ransomware.
Erradicación	Eliminar la causa raíz del incidente y corregir la vulnerabilidad explotada; por ejemplo, cerrar el acceso indebido detectado, identificar el correo de phishing que originó el ataque y actualizar los sistemas comprometidos.

Recuperación	Restaurar la información y los servicios afectados a partir de las copias de seguridad verificadas, y validar que los sistemas críticos (ERP, base de datos de clientes, comercio electrónico) vuelvan a operar con normalidad.
Lecciones aprendidas	Documentar el incidente, evaluar la efectividad de la respuesta y actualizar las políticas, controles o procedimientos, fortaleciendo la capacitación del personal para reducir la probabilidad de que el mismo evento se repita.

La estrategia de respuesta a incidentes que deberá adoptar la cadena de Supermercados MercaVida S.A.S. es un proceso continuo y no una acción aislada que solo se activa cuando ya se ha presentado un evento grave. Esta acción resulta necesaria porque, como se evidenció en el diagnóstico, la organización no cuenta actualmente con procedimiento formal para la gestión de incidentes de seguridad de la información, lo que ha causado que eventos como el acceso con credenciales compartidas o la caída de la plataforma de comercio electrónico se hayan gestionado de manera reactiva. Como método correctivo, se propone la adopción de 5 fases, las cuales son detección, contención, erradicación, recuperación y lecciones aprendidas.

La fase de detección, su importancia recae sobre el sistema de monitoreo y el analista de seguridad informática, ya que son estos activos y los responsables los que permitirán identificar de manera oportuna si un incidente afecta la confidencialidad, integridad o disponibilidad de alguno de los activos críticos priorizados en la matriz de riesgos, como lo son el sistema ERP, la base de datos de clientes o la plataforma de comercio electrónico. Cuanto antes se detecte un incidente, menor será el impacto acumulado, esto en especial si es un ataque de ransomware, el cual cada minuto cuenta para mitigar su propagación.

Las fases de contención y erradicación deberán ejecutarse de forma diferenciada según el activo afectado. Ejemplo: para un acceso no autorizado al sistema ERP, la contención de este incidente es la revocación inmediata de credenciales de acceso y activar el log de auditoría. En el caso de una fuga de información de clientes, se deberá proceder aislando el segmento de red comprometido y notificar a las áreas jurídicas o legales dado el volumen de datos comprometidos. En un caso de ataque por ransomware, se deberá proceder con la desconexión de la red de todos aquellos sistemas o dispositivos afectados para luego proceder con su limpieza.

La fase de recuperación dependerá directamente de que los respaldos hayan sido previamente probados y verificados, corrigiendo de esta manera una de las vulnerabilidades más críticas identificadas en el informe, la cual es la ausencia de pruebas documentadas de restauración.

Como parte final, se tiene la fase de lecciones aprendidas, cerrando el ciclo y dando continuidad a la mejora del sistema de gestión, lo cual se traduce en que cada incidente atendido es un ajuste a las políticas y controles existentes, evitando que se presenten eventos futuros como los previamente documentados.

Para que la cadena de supermercados pueda sostener su operación durante un incidente, debe apoyarse en tres medidas mínimas. Lo primero será mantener copias de seguridad periódicas y debidamente verificadas, que permitan restaurar la información en momentos críticos. Segundo, deberán contar con una redundancia básica en los servicios de infraestructura híbrida, de tal manera que una falla en la plataforma de comercio electrónico no interrumpa la operación de manera presencial en las sucursales. Por último, establecer canales de comunicación claros entre las áreas de TI y los administradores de las tiendas que permitan una correcta gestión de ventas y atención al cliente mientras se resuelve la afectación presentada en los sistemas digitales. Dichas medidas no eliminan el impacto de un incidente, pero aseguran que la cadena de supermercados pueda seguir operando mientras se ejecuta la acción técnica.

Cultura organizacional en ciberseguridad

Tabla 9. Hallazgos organizacionales

Situación observada	***Riesgo asociado***
La seguridad de la información se percibe como responsabilidad exclusiva del área de Tecnología y Sistemas	Baja participación de los colaboradores en la prevención de incidentes, lo que facilita eventos como el acceso indebido con credenciales compartidas
Prioridad constante de la operación comercial sobre el cumplimiento de controles de seguridad	Persistencia de prácticas riesgosas, como compartir credenciales entre administradores de tienda para no interrumpir la atención al cliente

Exceso de confianza frente a correos de proveedores y contactos externos	Mayor exposición a ataques de phishing, como el evento ya documentado que simuló ser un proveedor estratégico
Resistencia del personal a mecanismos como la autenticación multifactor	Retraso en la implementación de controles clave definidos en las políticas propuestas, prolongando la vulnerabilidad del ERP y otros sistemas críticos

Tabla 10. Recomendaciones de mejora

Hallazgo	***Recomendación***
La seguridad de la información se percibe como responsabilidad exclusiva del área de Tecnología y Sistemas	Implementar un programa de sensibilización dirigido a todos los colaboradores, no solo al área tecnológica, reforzando que la seguridad es una responsabilidad compartida
Prioridad constante de la operación comercial sobre el cumplimiento de controles de seguridad	Incorporar la seguridad como criterio dentro de los procesos operativos de tienda, con lineamientos claros que no comprometan la atención al cliente
Exceso de confianza frente a correos de proveedores y contactos externos	Desarrollar campañas periódicas de simulación de phishing y capacitación práctica para el reconocimiento de correos fraudulentos

Resistencia del personal a mecanismos como la autenticación multifactor	Acompañar la implementación técnica del MFA con una estrategia de comunicación que explique su propósito y beneficios, reduciendo la percepción de incomodidad

La cultura organizacional en la cadena de Supermercados MercaVida S.A.S. Evidencia que los colaboradores participan de manera desigual en la gestión de seguridad de la información, en el día a día el personal de la tienda y las áreas comerciales asumen que la seguridad de la información es un tema ajeno a sus funciones, delegando de esta manera toda la responsabilidad al área de TI, esta percepción es comprensible para una organización que se dedica a la venta y atención al cliente, y es precisamente esto lo que ha permitido que vulnerabilidades como el uso de credenciales compartidas o la falta de sensibilización frente a correos fraudulentos se mantengan vigentes durante los últimos tres años dando como resultado los eventos documentados.

No todo lo observado en la organización es malo, la compañía cuenta con algunos elementos que favorecen una base sobre la cual construir una cultura más sólida, la existencia de un área de TI estructurada con roles definidos como los analistas de soporte, el analista de seguridad informática o el administrador de base de datos, nos ofrece un punto de partida institucional para liderar un cambio cultural, de igual manera el hecho que la organización haya optado por documentar sus propios incidentes de seguridad en lugar de ignorarlos nos indica cierto nivel de conciencia organizacional que puede aprovecharse como insumo para las campañas de sensibilización propuestas.

Las principales oportunidades de mejora se centran en dos frentes el primero es cerrar la brecha entre el discurso corporativo y la práctica diaria, la visión de los Supermercados MercaVida S.A.S. Hace referencia a posicionarse como una cadena de supermercados reconocida haciendo énfasis explícitamente en la gestión segura de la información como parte de su identidad, pero esto no se refleja en el comportamiento diario de sus colaboradores, especialmente en el campo operativo, el segundo frente es lograr transformar la resistencia al uso de MFA en una comprensión clara y genuina del propósito de usar este método garantizando la seguridad de la información y evitando riesgos como los documentados en la matriz de riesgos relacionados con el acceso no autorizado al sistema ERP, la fuga de información o los correos de suplantación de identidad, comprender estos temas es importante para todos los colaboradores y no solo para las áreas relacionadas.

Las recomendaciones que se han propuesto buscan fortalecer la cultura organizacional específicamente en los puntos donde el análisis técnico del informe ya identificó una mayor exposición: el programa de sensibilización general busca reforzar la política de identidades y accesos; la incorporación de la seguridad en los procesos operativos de la tienda respalda la política de clasificación de la información; por otra parte, las campañas

de simulación de phishing atacan directamente la vulnerabilidad del correo fraudulento ya documentado. Esto, acompañado de la implementación del MFA, acelera la implementación del control considerado prioritario para mitigar el riesgo crítico de la organización. Todas estas recomendaciones no se plantean como acciones aisladas, sino como el complemento cultural necesario para que las políticas y controles y el plan de respuestas a incidentes sean sostenibles durante años.

Conclusiones

El desarrollo de este informe técnico permitió comprender que la seguridad de la información en la cadena de Supermercados MercaVida S.A.S. no depende de un único factor, sino que depende de la interacción entre tecnología, procesos y personas. Esto me permitió entender ciertos puntos:

La organización enfrenta una brecha significativa entre el ritmo de su crecimiento tecnológico y la madurez de su gestión de seguridad. Los Supermercados MercaVida S.A.S. han adoptado infraestructura robusta con sistemas como ERP, CRM, comercio electrónico y una infraestructura híbrida, sin que la implementación de políticas y controles formales haya avanzado al mismo ritmo, lo que explica por qué situaciones como el uso de credenciales compartidas o la ausencia de un inventario actualizado de activos pudieron persistir el tiempo suficiente como para materializarse en incidentes reales.

Los riesgos de mayor criticidad identificados durante la elaboración de este informe son el acceso no autorizado al sistema ERP, la exposición de la base de datos de clientes y la falta de pruebas de restauración de los respaldos, estos eventos no son hipotéticos, sino que ya cuentan con antecedentes documentados en la propia organización. Esto reafirma que la gestión de riesgos no debe entenderse como un ejercicio teórico, sino como una respuesta directa a patrones de vulnerabilidad que la empresa ya ha experimentado.

La construcción de este informe permitió identificar que un sistema de gestión de seguridad de la información es efectivo, pero requiere trazabilidad entre sus componentes; los activos deben estar debidamente inventariados para poder valorar las amenazas que los afectan, las amenazas deben traducirse en riesgos priorizados y, a su vez, estos riesgos deben dar origen a políticas y controles. Todo ello, más allá de ser un requisito para el informe, es una condición necesaria para que se pueda aplicar cualquier estrategia de seguridad.

El desarrollo de este informe técnico permitió aplicar los conceptos fundamentales de seguridad de la información al caso de Supermercados MercaVida S.A.S., evidenciando el proceso metodológico que conlleva estructurar un sistema de gestión de seguridad de la información: desde la identificación de activos y la valoración de amenazas, hasta la formulación de políticas, controles y un plan de respuesta a incidentes. A partir de este

análisis se identificaron oportunidades de mejora concretas para la organización, entre ellas fortalecer los controles de acceso e identidades, formalizar procesos actualmente inexistentes como la gestión de incidentes, y generar espacios que promuevan la participación activa de todos los colaboradores en temas relacionados con la seguridad de la información.

Referencias

¿Qué es la ciberseguridad? (22 de mayo de 2026). Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

Holdsworth, J. y Kosinski, M. (s.f.). ¿Qué es la seguridad de la información? IBM.com . https://www.ibm.com/mx-es/think/topics/information-security

Whitman, ME, y Mattord, HJ (s.f.). Seguridad de la información . Studentebookhub.com. Recuperado el 5 de julio de 2026 de https://studentebookhub.com/wp-content/uploads/2024/preview/9780357506554.pdf

Bowman, K. (30 de enero de 2025). Amenaza vs. Vulnerabilidad vs. Riesgo: ¿Cuáles son las diferencias? Pathlock . https://pathlock.com/learn/threat-vs-vulnerability-vs-risk-what-are-differences/

¿Qué son los controles de seguridad? (s.f.). IBM.com . https://www.ibm.com/mx-es/think/topics/security-controls

(Sin fecha). Iso.org. Recuperado el 5 de julio de 2026 de https://www.iso.org/es/norma/27001?__cf_chl_f_tk=DbeCsjkuWwl.ZEF86m2GvusLskTSMDKnBfIc2zIV3sY-1783281247-1.0.1.1-oGwHJa5eUsFcYlDhAF9YOeHBeb7FtzvOVGWUSzTuqz4

(Nd-b). Iso.org. Recuperado el 5 de julio de 2026 de https://www.iso.org/standard/76070.html

Decreto 1377 de 2013 - Gestor Normativo. Gobernador.co. Recuperado el 5 de julio de 2026 de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Ley 1273 de 2009 - Gestor Normativo. Gobernador.co. Recuperado el 5 de julio de 2026 de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley 1581 de 2012 - Gestor Normativo. Gobernador.co. Recuperado el 5 de julio de 2026 de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Norma ISO 31000:2018 . (2024). ISO. https://www.iso.org/standard/65694.html

Iso/iec 27005:2022. (2022). ISO. https://www.iso.org/standard/80585.html
¿Qué es la gestión de riesgos cibernéticos? (2025, 27 de noviembre). IBM.com . https://www.ibm.com/mx-es/think/topics/cyber-risk-management

Suscriptor. (2021, 16 de febrero). Identificación de riesgos ISO 31000: claves para aplicarla en tu organización . ISO de software; ISOHerramientas. https://isotools.org/2021/02/16/identificacion-de-riesgos-segun-la-iso-31000/