TRABAJO DE GRADO
Opción Seminario.

Informe técnico caso de la empresa FOODEXPRESS COLOMBIA S.A.S.

Corporación Universitaria Remington.
Facultad de Ingenierías
Ingeniería de Sistemas

Steven Urrego Cano

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Dedicatoria

A mi esposa, por su apoyo incondicional en esta etapa de mi vida. Este logro también es tuyo.

Tabla de Contenidos

Resumen

El presente documento constituye un análisis técnico de ciberseguridad elaborado para la empresa FOODEXPRESS COLOMBIA S.A.S., compañía del sector de restaurantes de comida rápida con 18 años de trayectoria en el mercado nacional. La organización administra una red de 12 puntos de venta bajo esquema de franquicia en tres ciudades colombianas y cuenta con una planta de personal de aproximadamente 280 colaboradores.

El diagnóstico de partida puso en evidencia distintas situaciones que debilitan la protección de la información corporativa: administradores de puntos de venta que comparten credenciales de acceso al sistema POS, carencia de normativas internas de seguridad, infraestructura de red sin separación entre el segmento corporativo y el segmento de clientes, ausencia de un inventario actualizado de activos tecnológicos, y una percepción generalizada en la que la responsabilidad por la seguridad informática recae únicamente en el departamento de TI.

Este informe desarrolla los componentes esenciales de la gestión de ciberseguridad en el ámbito organizacional: clasificación de activos de información, identificación de amenazas y vulnerabilidades, construcción de una matriz de riesgos fundamentada en criterios de impacto y probabilidad, diseño de políticas y controles de protección, planificación de la respuesta ante incidentes, lineamientos de continuidad operativa y diagnóstico de la cultura interna frente a la seguridad.

Los resultados evidencian que la empresa presenta exposiciones de nivel crítico y alto en áreas como la salvaguarda de datos personales de clientes, la seguridad del sistema de punto de venta, la integridad de la red corporativa y el nivel de preparación del personal frente a técnicas de ingeniería social. Las propuestas de mejora buscan sentar las bases de una gestión segura de la información, alineada con referentes internacionales como ISO/IEC 27001 e ISO/IEC 27005, así como con el ordenamiento jurídico colombiano vigente, particularmente la Ley 1581 de 2012 y la Ley 1273 de 2009.

Palabras clave

ciberseguridad organizacional, activos de información, gestión de riesgos, vulnerabilidades, políticas de seguridad.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

En la actualidad, la ciberseguridad ocupa un lugar central dentro de la agenda estratégica de las organizaciones. Tal como lo define la Organización Internacional de Normalización, esta disciplina engloba el conjunto de actividades orientadas a proteger el ciberespacio, los sistemas de información y los datos que circulan en ellos (ISO/IEC 27032, 2012). Su alcance no se limita a la dimensión tecnológica, sino que involucra procesos, personas y estructuras de gobierno que aseguran la protección integral de la información.

Un concepto estrechamente vinculado con la ciberseguridad es la seguridad de la información, definida como el mantenimiento de la confidencialidad, la integridad y la disponibilidad de la información, principios conocidos colectivamente como la tríada CIA (Whitman & Mattord, 2021). Estos tres atributos constituyen el eje sobre el cual se articulan todos los marcos de gestión de la seguridad a escala global.

La confidencialidad alude a la garantía de que únicamente las personas o entidades autorizadas tienen acceso a determinada información. Para FOODEXPRESS COLOMBIA S.A.S., este principio reviste especial importancia considerando que la organización custodia datos personales de más de 75.000 clientes registrados en su programa de fidelización, entre ellos nombres, correos electrónicos, números de teléfono e historial de consumo. Una divulgación no controlada de esta información podría traducirse en consecuencias jurídicas y un daño reputacional de magnitud considerable.

La integridad hace referencia a la exactitud y completitud de la información, y a su protección frente a alteraciones no autorizadas (NIST, 2020). En el caso de FoodExpress, este principio cobra especial relevancia en los sistemas POS y ERP, donde cualquier modificación indebida de registros financieros o de inventario puede distorsionar la toma de decisiones operativas y afectar los resultados de la empresa.

La disponibilidad implica que la información y los recursos asociados estén al alcance de los usuarios autorizados cuando los necesiten (ISO/IEC 27001, 2022). Los eventos registrados en la organización ilustran con claridad las consecuencias que tiene la pérdida de disponibilidad sobre la continuidad del negocio.

Se denominan activos de información a todos aquellos elementos que poseen valor para la organización y que contribuyen al logro de sus objetivos (ISO/IEC 27005, 2022). Estos pueden ser físicos (equipos, infraestructura), digitales (bases de datos, sistemas, aplicaciones) o humanos (colaboradores con conocimiento crítico). Su correcta identificación y valoración es el punto de partida para cualquier ejercicio de análisis de riesgos.

Las amenazas son eventos, situaciones o acciones con capacidad de afectar negativamente un activo de información y comprometer la operación, los datos o los servicios de la organización (ENISA, 2023). Pueden tener origen, tecnológico, natural, físico u operativo. En FoodExpress, amenazas como el phishing, el acceso indebido mediante credenciales compartidas y la pérdida de dispositivos han quedado documentadas en incidentes concretos de los últimos tres años.

Las vulnerabilidades, en contraste con las amenazas, son condiciones o debilidades internas que pueden ser aprovechadas por una amenaza para dañar un activo (ISO/IEC 27005, 2022). No generan daño por sí solas, pero crean las condiciones para que las amenazas se materialicen. La inexistencia de políticas de contraseñas, la falta de capacitación del personal y la ausencia de procedimientos formales para la gestión de incidentes son ejemplos concretos de vulnerabilidades identificadas en la organización.

El riesgo, en el ámbito de la seguridad de la información, representa la combinación de la probabilidad de que una amenaza explote una vulnerabilidad determinada y el impacto que dicho evento tendría sobre los activos organizacionales (NIST, 2020). La gestión del riesgo no persigue su eliminación total, sino su reducción a niveles tolerables mediante la implementación de controles apropiados.

Los controles de seguridad son las medidas o salvaguardas implementadas para reducir la probabilidad de ocurrencia de un riesgo o para limitar su impacto en caso de materializarse (ISO/IEC 27001, 2022). Pueden ser de naturaleza preventiva, detectiva o correctiva, y abarcan tanto elementos técnicos como procedimentales y organizacionales.

Marco normativo

El análisis de ciberseguridad de FOODEXPRESS COLOMBIA S.A.S. se inscribe en un conjunto de normas, leyes y estándares nacionales e internacionales que orientan las buenas prácticas en la gestión de la seguridad de la información. A continuación, se presentan las principales referencias aplicables al caso objeto de estudio:

Tabla 1. Normatividad aplicable.

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***
Ley 1581 de 2012 (Protección de Datos Personales)	Regular la recolección, almacenamiento, uso, circulación y supresión de datos personales de ciudadanos colombianos.	FoodExpress almacena datos personales de más de 75.000 clientes en su plataforma de fidelización. La empresa está obligada a obtener consentimiento, garantizar los derechos de los titulares e implementar medidas de seguridad adecuadas.
Ley 1273 de 2009 (Delitos Informáticos)	Incorporar al Código Penal Colombiano los delitos relacionados con la protección de la información y los datos.	Los eventos de acceso no autorizado, phishing y uso indebido de credenciales identificados en FoodExpress podrían configurar conductas tipificadas como delitos informáticos bajo esta ley.
ISO/IEC 27001:2022	Establecer los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).	Suministra el marco metodológico para que FoodExpress establezca políticas, controles y procesos de seguridad alineados con las mejores prácticas internacionales.
ISO/IEC 27005:2022	Proporcionar directrices para la gestión de riesgos de seguridad de la información, incluyendo identificación, análisis, evaluación y tratamiento.	Orienta el proceso de análisis de riesgos desarrollado en el presente informe, facilitando la priorización de los riesgos más críticos para FoodExpress y la definición de controles proporcionales.
ENISA Threat Landscape	Publicar anualmente el panorama de amenazas más relevantes a nivel global, con recomendaciones de mitigación.	Permite a FoodExpress conocer las tendencias actuales de amenazas, especialmente en el sector de servicios digitales, pagos en línea y protección de datos de consumidores.

El cumplimiento del marco normativo descrito no es para FOODEXPRESS COLOMBIA S.A.S. solo una obligación legal, sino también una condición indispensable para preservar la confianza de sus clientes, proteger el prestigio de la marca y asegurar la continuidad del negocio. La Ley 1581 de 2012 resulta especialmente relevante dado el volumen de datos personales que la empresa gestiona a través de su programa de fidelización y su aplicación móvil; su inobservancia puede derivar en sanciones administrativas impuestas por la Superintendencia de Industria y Comercio (SIC) de hasta 2.000 salarios mínimos legales mensuales vigentes (Congreso de la República de Colombia, 2012).

Por su parte, la adopción de ISO/IEC 27001 le brinda a la organización una estructura sistemática para administrar la seguridad de la información, mientras que ISO/IEC 27005 complementa ese marco con una metodología rigurosa para identificar y tratar los riesgos. La articulación de estos estándares internacionales con el cumplimiento normativo colombiano constituye la base sobre la cual se fundamentan las recomendaciones de este informe.

Marco contextual

Descripción de la organización

FOODEXPRESS COLOMBIA S.A.S. es una compañía del sector gastronómico dedicada a la operación de restaurantes de comida rápida bajo un modelo de franquicia, comparable al esquema empleado por grandes cadenas del sector a nivel internacional. Con 18 años de presencia en el mercado colombiano, la empresa se ha posicionado como un referente relevante en el segmento de comida rápida, con 12 restaurantes en funcionamiento distribuidos en tres ciudades del país.

La organización cuenta con una planta aproximada de 280 colaboradores en distintos niveles: administradores de punto de venta, supervisores de turno, cajeros, auxiliares de cocina y de aseo, domiciliarios, personal logístico, administrativo y directivo. Esta diversidad de perfiles implica diferentes grados de acceso a la información y distintas exposiciones al riesgo desde la perspectiva de la seguridad.

En el ámbito operativo, FoodExpress atiende en promedio 4.500 clientes por día y gestiona cerca de 120.000 transacciones mensuales, distribuidas entre ventas presenciales en los puntos de venta, pedidos a domicilio y transacciones realizadas mediante plataformas digitales. Este volumen confiere a los sistemas de información de la empresa una criticidad operativa muy elevada.

La estructura organizacional comprende las áreas de Gerencia General, Dirección de Operaciones, Dirección Comercial, Talento Humano, Tecnología y Sistemas, Compras e Inventarios, Logística y Distribución, Marketing Digital, Servicio al Cliente, y Contabilidad y Finanzas. La gestión tecnológica recae sobre un coordinador de TI respaldado por tres analistas de soporte, una capacidad que resulta limitada frente al volumen y la complejidad de la infraestructura que deben administrar.

La infraestructura tecnológica incluye 65 computadores de escritorio, 40 tabletas para la toma de pedidos, 12 servidores virtuales, un sistema POS centralizado, un ERP para inventarios y finanzas, una plataforma de gestión de domicilios, una aplicación móvil para clientes, un sitio web corporativo, una plataforma CRM, correo electrónico institucional, sistema de videovigilancia, control biométrico de acceso, redes WiFi corporativa y para clientes, almacenamiento en la nube y plataforma de copias de seguridad.

El programa de fidelización de clientes es uno de los activos de mayor valor informativo para la organización, pues almacena datos personales de más de 75.000 clientes registrados, incluyendo nombres, correos electrónicos, teléfonos, historial de compras y preferencias de consumo. Adicionalmente, la compañía proyecta ampliar su presencia con cinco nuevas sedes en los próximos dos años e integrar pagos mediante billeteras digitales, lo que incrementará de forma significativa la complejidad de su infraestructura y sus necesidades de seguridad.

Problemática identificada

El diagnóstico inicial realizado en FOODEXPRESS COLOMBIA S.A.S. permitió establecer que la problemática central de la organización en materia de ciberseguridad no radica en la ausencia de tecnología, sino en la falta de gobernanza sobre su uso: la empresa opera sistemas críticos como el POS, el ERP y la plataforma CRM sin políticas formales de seguridad de la información, sin un inventario actualizado de activos tecnológicos y sin procedimientos documentados para la gestión de incidentes. Esta carencia estructural se refleja en un conjunto de prácticas inseguras y de eventos ya materializados durante los últimos tres años, que se describen a continuación.

El uso de credenciales compartidas entre los administradores de punto de venta para acceder al sistema POS, práctica que impide atribuir cada transacción a un responsable individual y que anula la trazabilidad de las operaciones. Esta debilidad, agravada por la inexistencia de una política de contraseñas, ya tuvo consecuencias concretas: en uno de los eventos registrados, un tercero no autorizado logró ingresar a la red utilizando credenciales compartidas entre empleados.

La infraestructura de red presenta una debilidad de diseño significativa, pues la red WiFi corporativa y la red destinada a los clientes operan sobre la misma infraestructura física, sin segmentación alguna. Esta condición implica que cualquier dispositivo conectado a la red pública de los restaurantes podría, en teoría, alcanzar los sistemas internos de la organización, incluyendo los servidores que alojan el POS, el ERP y la base de datos de clientes.

El personal operativo no recibe formación en seguridad de la información y desconoce amenazas comunes como el phishing y el malware, lo que quedó en evidencia cuando un

colaborador ingresó sus credenciales institucionales en un sitio fraudulento que suplantaba a un área interna (Evento 1) y cuando un error operativo en la actualización de inventarios afectó la información del sistema (Evento 5). A esta falta de preparación se suma una percepción generalizada de que la seguridad es responsabilidad exclusiva del área de Tecnología y Sistemas, equipo conformado por apenas cuatro personas frente a una planta de 280 colaboradores.

Se identificaron debilidades en la gestión de la información y de los dispositivos: la pérdida del computador portátil de un supervisor regional, que contenía bases de datos exportadas sin cifrar, expuso información sensible sin que la organización pudiera determinar el alcance real del compromiso; asimismo, aunque las copias de seguridad se ejecutan diariamente, no se realizan pruebas periódicas de restauración, por lo que no existe certeza de que la información crítica pueda recuperarse ante un incidente. La falla de sincronización entre servidores que obligó a uno de los restaurantes a registrar ventas de forma manual durante varias horas (Evento 2) evidenció, además, la fragilidad de la continuidad operativa.

El conjunto de situaciones descritas adquiere una dimensión especialmente crítica si se considera que la organización custodia datos personales de más de 75.000 clientes protegidos por la Ley 1581 de 2012, y que proyecta abrir cinco nuevas sedes e incorporar pagos mediante billeteras digitales en los próximos dos años. Esta problemática constituye el punto de partida del análisis de activos, amenazas, vulnerabilidades y riesgos que se desarrolla en los capítulos siguientes.

Identificación y análisis de activos

Inventario de activos

Con base en la información del caso de estudio, se identificaron y clasificaron los activos de información más relevantes para FOODEXPRESS COLOMBIA S.A.S., considerando su importancia para la operación, el nivel de sensibilidad de la información que contienen y las consecuencias que tendría su compromiso, pérdida o indisponibilidad.

Tabla 2. Inventario de activos

Activo	***Tipo***	***Descripción***	***Criticidad***
Sistema POS centralizado	Digital	Plataforma de punto de venta que procesa la totalidad de transacciones presenciales en los 12 restaurantes. Gestiona cerca de 120.000 transacciones por mes.	Alta

Base de datos del programa de fidelización (CRM)	Digital	Almacena datos personales de más de 75.000 clientes: nombres, correos, contactos, historial de compras y preferencias de consumo.	Alta
Sistema ERP (inventarios y finanzas)	Digital	Plataforma integrada para la gestión de inventarios, compras, contabilidad y finanzas corporativas. Consolida la información financiera de toda la organización.	Alta
Servidores virtuales (12)	Digital	Infraestructura que aloja los sistemas críticos: POS, ERP, correo institucional y plataformas digitales.	Alta
Aplicación móvil para clientes	Digital	Canal de pedidos en línea con acceso a datos personales de los clientes. Funciona como canal de ventas y captación de datos.	Alta
Red corporativa WiFi	Físico/Digital	Infraestructura inalámbrica que conecta los equipos de los restaurantes con los sistemas centrales. Actualmente comparte infraestructura con la red de clientes.	Alta
Coordinador de TI y analistas de soporte	Humano	Equipo de 4 personas con conocimiento crítico sobre la infraestructura, configuraciones y accesos privilegiados de la organización.	Alta
Computadores de escritorio (65)	Físico	Equipos distribuidos en restaurantes y sede administrativa. Algunos operan con sistemas operativos sin actualizar.	Media
Tabletas para toma de pedidos (40)	Físico	Dispositivos móviles utilizados en los restaurantes para recibir pedidos. Tienen acceso al sistema POS.	Media
Plataforma de copias de seguridad	Digital	Sistema que realiza respaldos diarios de la información crítica. No se ejecutan pruebas periódicas de recuperación.	Media

Correo electrónico institucional	Digital	Canal oficial de comunicación organizacional. Algunos colaboradores utilizan correo personal para compartir documentos laborales.	Media
Sistema de videovigilancia	Físico/Digital	Cámaras de seguridad instaladas en los puntos de venta. Genera registros relevantes para la investigación de incidentes.	Media
Plataforma de domicilios	Digital	Sistema de gestión de pedidos a domicilio integrado con plataformas aliadas. Administra información de clientes y rutas de entrega.	Media
Personal operativo (cajeros, auxiliares, domiciliarios)	Humano	Colaboradores con acceso a sistemas POS y manejo de datos de clientes. Representan un vector de riesgo por ingeniería social ante su bajo nivel de capacitación en seguridad.	Media
Página web corporativa	Digital	Presencia web de la empresa. Canal de pedidos y representación de la marca.	Baja

El análisis del inventario permite determinar que los activos de criticidad alta están directamente vinculados con la operación comercial, la protección de datos personales y la continuidad del negocio. El sistema POS y el CRM resultan los más críticos desde la perspectiva de seguridad de la información, pues su compromiso afectaría simultáneamente los ingresos de la empresa y los derechos de más de 75.000 titulares de datos personales.

Los servidores virtuales constituyen el sustento tecnológico de todos los demás activos digitales, convirtiéndose en objetivos de alto valor para potenciales atacantes. Su indisponibilidad generaría un efecto en cascada sobre el resto de sistemas. El equipo de TI, como activo humano crítico, concentra el conocimiento sobre la arquitectura de la infraestructura y los accesos privilegiados; su pérdida o compromiso podría paralizar la capacidad de respuesta de la organización ante incidentes.

Análisis de amenazas y vulnerabilidades

El análisis que sigue se construye a partir del diagnóstico inicial, los eventos registrados en los últimos tres años y el inventario de activos previamente identificado. Su propósito es establecer cómo los factores de riesgo externos e internos se relacionan con los activos más críticos de la organización.

Tabla 3. Amenazas y vulnerabilidades

Activo	***Amenaza***	***Vulnerabilidad***
Sistema POS centralizado	Acceso no autorizado / interrupción del servicio	Credenciales compartidas entre administradores; equipos con sistemas operativos desactualizados en los puntos de venta.
Base de datos CRM (75.000+ clientes)	Fuga o robo de datos personales	Carencia de política de control de accesos; datos no clasificados formalmente; ausencia de cifrado documentado en reposo.
Sistema ERP (inventarios y finanzas)	Alteración o acceso indebido a información financiera	Sin perfiles de acceso diferenciados; uso no controlado de dispositivos USB; ausencia de procedimientos de renovación de contraseñas.
Servidores virtuales (12)	Ransomware / indisponibilidad del servicio	Equipos sin actualizaciones de seguridad recientes; red sin segmentación entre sistemas críticos; copias de seguridad no verificadas periódicamente.
Red corporativa WiFi	Interceptación de tráfico / acceso no autorizado desde red de clientes	Red corporativa y de clientes sobre la misma infraestructura física; credenciales compartidas entre empleados utilizadas por terceros no autorizados.
Correo electrónico institucional	Phishing / robo de credenciales	Falta de capacitación en detección de correos fraudulentos; uso de cuentas personales para documentos laborales, evadiendo controles.

Personal operativo	Ingeniería social / error humano	Ausencia de formación en seguridad; cultura que privilegia la velocidad sobre los protocolos de seguridad; desconocimiento de amenazas como phishing y malware.
Aplicación móvil para clientes	Exposición de datos personales / vulnerabilidades de la aplicación	Usuarios sin claridad sobre cómo se protege su información; política de privacidad no comunicada efectivamente; posible almacenamiento inseguro en dispositivos.
Plataforma de copias de seguridad	Pérdida permanente de información ante incidentes	Respaldos diarios sin pruebas periódicas de restauración; procedimiento de recuperación no documentado formalmente.
Computadores y tabletas	Pérdida o robo de dispositivos	Dispositivos portátiles sin cifrado de almacenamiento; laptop extraviada de supervisor regional contenía bases de datos exportadas sin cifrar.

Del análisis anterior se desprende que las amenazas de mayor impacto potencial para FOODEXPRESS COLOMBIA S.A.S. son aquellas que afectan de forma simultánea la confidencialidad de los datos de clientes y la disponibilidad de los sistemas operativos críticos. Tres situaciones concentran el mayor nivel de riesgo para la organización.

En primer término, la combinación de credenciales compartidas en el POS con la ausencia de políticas de contraseñas genera una vulnerabilidad estructural que facilita tanto el acceso no autorizado como la imposibilidad de rastrear la autoría de acciones fraudulentas en el sistema. Esta situación quedó en evidencia en el Evento 4, donde un tercero accedió a la red usando credenciales compartidas entre empleados.

En segundo término, la base de datos CRM con más de 75.000 registros representa el activo con mayor potencial de daño legal y reputacional en caso de fuga de información. La ausencia de clasificación formal y de controles de acceso diferenciados incrementa la probabilidad de que esta información sea comprometida, ya sea por un ataque externo o por una acción interna.

En tercer término, la vulnerabilidad humana evidenciada en el phishing (Evento 1) y el error operativo en la actualización de inventarios (Evento 5) demuestra que el personal representa el eslabón más débil de la cadena de seguridad, situación que se agrava por la cultura organizacional que delega exclusivamente en TI la responsabilidad por la seguridad.

Análisis y gestión de riesgos

Metodología de análisis

La valoración de los riesgos identificados se realizó siguiendo un enfoque cualitativo de tres niveles (alto, medio y bajo), coherente con los lineamientos de la norma ISO/IEC 27005:2022 para la gestión de riesgos de seguridad de la información (ISO/IEC 27005, 2022) y con las buenas prácticas descritas en la publicación NIST SP 800-53 Rev. 5 (NIST, 2020). El impacto de cada riesgo se determinó evaluando cinco criterios: la afectación a la operación de los restaurantes y de los canales digitales, las posibles pérdidas económicas, el efecto sobre los clientes y sus datos personales, las consecuencias legales derivadas de la Ley 1581 de 2012 y la Ley 1273 de 2009, y el daño reputacional para la marca. Un riesgo se calificó como alto cuando comprometía procesos críticos como el sistema POS, el ERP o la continuidad del negocio; como medio cuando afectaba parcialmente algunos procesos; y como bajo cuando las consecuencias eran menores y fácilmente recuperables.

La probabilidad, por su parte, se estableció considerando la frecuencia con la que cada situación podría presentarse, la existencia de controles preventivos, los antecedentes documentados en los últimos tres años (el evento de phishing, la pérdida de un equipo portátil, el acceso no autorizado a la red, entre otros) y el nivel de exposición actual de la organización, en línea con el enfoque metodológico propuesto por ENISA en su informe anual de panorama de amenazas (ENISA, 2023). Los riesgos que ya se habían materializado al menos una vez, como el acceso indebido mediante credenciales compartidas o el phishing dirigido al personal, se valoraron con una probabilidad alta, mientras que aquellos sin antecedentes directos pero con vulnerabilidades identificadas se calificaron como de probabilidad media. Finalmente, el nivel de riesgo resultó de cruzar el impacto y la probabilidad mediante una matriz de doble entrada, de manera que un riesgo de impacto alto combinado con una probabilidad alta o media se clasifica como riesgo alto, siguiendo el mismo principio de combinación aplicado por Whitman y Mattord (2021)en su definición del riesgo como producto de la probabilidad de ocurrencia y la magnitud de sus consecuencias.

Matriz de riesgos

Tabla 4. Matriz de riesgos

Riesgo	***Impacto***	***Probabilidad***	***Nivel***
Acceso no autorizado al sistema POS mediante el uso de credenciales compartidas entre administradores de punto de venta.	Alto	Alta	Alto
Fuga o robo de los datos personales de los más de 75.000 clientes almacenados en la plataforma CRM.	Alto	Media	Alto

Indisponibilidad de los servidores virtuales por ransomware, fallas de sincronización o ausencia de actualizaciones de seguridad.	Alto	Media	Alto
Acceso no autorizado a la red corporativa debido a la falta de segmentación con la red WiFi destinada a los clientes.	Alto	Alta	Alto
Robo de credenciales institucionales mediante ataques de phishing dirigidos al correo electrónico corporativo.	Medio	Alta	Alto
Errores humanos y comportamientos inseguros del personal operativo por ausencia de capacitación en seguridad de la información.	Medio	Alta	Alto
Alteración o acceso indebido a la información financiera y de inventarios registrada en el sistema ERP.	Alto	Baja	Medio
Pérdida permanente de información crítica ante la ausencia de pruebas periódicas de restauración de las copias de seguridad.	Alto	Media	Alto
Pérdida o robo de computadores portátiles y tabletas que almacenan información institucional sin cifrado.	Medio	Media	Medio
Exposición de datos personales de clientes por vulnerabilidades o falta de comunicación sobre la protección de datos en la aplicación móvil.	Medio	Baja	Bajo

La matriz elaborada evidencia que FOODEXPRESS COLOMBIA S.A.S. enfrenta un panorama de riesgo predominantemente alto, con siete de los diez riesgos identificados clasificados en ese nivel. Esta situación confirma el diagnóstico inicial y exige que la organización priorice su atención en cuatro frentes concretos.

En primer lugar, el riesgo de acceso no autorizado al sistema POS mediante credenciales compartidas debe considerarse la prioridad más urgente, pues combina un impacto alto con una probabilidad alta, ya materializada en el Evento 4 descrito en el diagnóstico. La ausencia de una política formal de contraseñas agrava esta condición al impedir identificar con certeza al responsable de cada transacción.

En segundo lugar, la fuga o el robo de los datos personales almacenados en el CRM representa el riesgo con mayor potencial de consecuencias legales y reputacionales, dado que involucra información de más de 75.000 titulares protegidos por la Ley 1581 de 2012. Aunque no se ha registrado un incidente confirmado de fuga, la ausencia de clasificación formal de la información y de controles de acceso diferenciados sostiene una probabilidad media que, combinada con el alto impacto, ubica este riesgo en el nivel más crítico de la matriz.

En tercer lugar, la falta de segmentación entre la red WiFi corporativa y la red destinada a los clientes constituye un riesgo estructural, pues cualquier persona conectada a la red pública podría, en teoría, alcanzar los sistemas internos de la organización; esta condición ya facilitó el acceso no autorizado documentado en el Evento 4.

Finalmente, los riesgos asociados al factor humano concentran una probabilidad alta debido a la ausencia de formación formal en seguridad, la cultura organizacional que privilegia la velocidad de atención sobre el cumplimiento de procedimientos, y la percepción generalizada de que la ciberseguridad es responsabilidad exclusiva del área de TI.

En un nivel intermedio se ubican los riesgos relacionados con la alteración de información financiera en el ERP y la pérdida o el robo de dispositivos portátiles sin cifrado, cuyo impacto es considerable pero cuya probabilidad se reduce por la menor frecuencia de exposición directa. El riesgo de menor prioridad corresponde a la exposición de datos personales a través de la aplicación móvil, dado que, si bien el impacto legal sería significativo, no existen antecedentes que sugieran una probabilidad alta de ocurrencia en el corto plazo. Esta priorización constituye la base para el diseño de las políticas y los controles de seguridad que se desarrollan en el siguiente capítulo, los cuales deben orientarse principalmente a mitigar los cuatro riesgos calificados como más críticos.

Políticas y controles de seguridad

Con base en la priorización de riesgos ya establecida, en esta sección se formulan las políticas de seguridad y los controles de protección que FOODEXPRESS COLOMBIA S.A.S. debería adoptar para reducir su exposición. Las políticas definen los lineamientos generales de comportamiento esperado dentro de la organización, mientras que los controles constituyen las medidas concretas mediante las cuales dichas políticas se materializan en la operación diaria de los 12 restaurantes y de la sede administrativa. Esta distinción resulta especialmente relevante para FoodExpress, pues su diagnóstico inicial reveló la ausencia casi total de lineamientos formales, lo que exige construir la estrategia de seguridad prácticamente desde sus fundamentos.

Los controles propuestos se clasifican en tres categorías complementarias. Los controles administrativos corresponden a medidas organizacionales, como la capacitación del personal o la definición de procedimientos, orientadas a reducir errores humanos y fortalecer el cumplimiento de las políticas. Los controles técnicos son mecanismos tecnológicos, como la autenticación multifactor, el cifrado o la segmentación de redes, que protegen directamente los sistemas de información frente a accesos indebidos o fallas. Los controles físicos, por su parte, protegen la infraestructura y los equipos, por ejemplo, mediante el control de acceso a las salas de servidores o el cifrado de los dispositivos portátiles utilizados por el personal directivo. Esta clasificación, coherente con el enfoque de la norma ISO/IEC 27001:2022 (ISO/IEC 27001, 2022), garantiza que las medidas propuestas para FoodExpress no dependan exclusivamente de la tecnología, sino que combinen procesos, personas e infraestructura física.

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***
Política de Gestión de Usuarios y Contraseñas	Establecer la asignación de credenciales individuales e intransferibles, así como reglas de complejidad y renovación periódica de contraseñas para todos los sistemas críticos (POS, ERP, CRM).	Acceso no autorizado al sistema POS mediante credenciales compartidas.
Política de Clasificación y Manejo de la Información	Definir niveles de sensibilidad (pública, interna, confidencial, restringida) para la información institucional y de clientes, estableciendo reglas de acceso y manejo según cada nivel.	Fuga o robo de los datos personales almacenados en el CRM.

Política de Segmentación y Uso de Redes	Separar la infraestructura de red corporativa de la red destinada a los clientes y regular el acceso remoto a los sistemas internos.	Acceso no autorizado a la red corporativa por falta de segmentación.
Política de Uso Seguro del Correo Electrónico	Regular el uso del correo institucional, prohibir el envío de información laboral a cuentas personales y establecer pautas para identificar correos fraudulentos.	Robo de credenciales institucionales mediante phishing.
Política de Copias de Seguridad y Recuperación	Garantizar la ejecución de respaldos periódicos de la información crítica y su verificación mediante pruebas formales de restauración.	Pérdida permanente de información ante fallas o incidentes.
Política de Uso de Dispositivos Móviles y Medios Removibles	Establecer condiciones de cifrado, autorización y control para el uso de computadores portátiles, tabletas y dispositivos USB.	Pérdida o robo de dispositivos con información institucional sin cifrar.
Política de Capacitación y Sensibilización en Seguridad de la Información	Garantizar que todo el personal, desde su ingreso, reciba formación periódica sobre riesgos de ciberseguridad, phishing e ingeniería social.	Errores humanos y baja preparación del personal frente a ataques de ingeniería social.

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***
Acceso no autorizado al sistema POS	Autenticación multifactor (MFA) y asignación de usuarios individuales con bloqueo automático tras intentos fallidos (control técnico).	Elimina la posibilidad de que varias personas operen bajo una misma identidad y permite trazar cada transacción a un responsable específico.

Fuga de datos personales del CRM	Cifrado de la base de datos en reposo y en tránsito, y control de accesos basado en roles (control técnico).	Reduce la probabilidad de exposición de la información y favorece el cumplimiento de la Ley 1581 de 2012.
Indisponibilidad de los servidores virtuales	Actualización periódica de sistemas operativos, protección antimalware y copias de seguridad verificadas mediante pruebas de restauración (control técnico).	Corrige las vulnerabilidades explotables y garantiza la recuperación oportuna de la información ante un incidente.
Acceso no autorizado a la red corporativa	Segmentación de la red mediante VLAN independientes para clientes y para sistemas internos, junto con firewall perimetral (control técnico).	Impide que un dispositivo conectado a la red de clientes alcance los sistemas críticos de la organización.
Phishing sobre el correo institucional	Filtros antispam, autenticación SPF/DKIM/DMARC y simulaciones periódicas de phishing (control técnico y administrativo).	Disminuye la probabilidad de que los correos fraudulentos lleguen a los colaboradores y mide su nivel de preparación real.
Errores humanos e ingeniería social	Programa permanente de capacitación y campañas de sensibilización en seguridad de la información (control administrativo).	Fortalece el conocimiento del personal y reduce la dependencia exclusiva de controles tecnológicos.
Pérdida o robo de dispositivos	Cifrado de disco en equipos portátiles, inventario actualizado de activos y procedimientos de bloqueo remoto (control físico y técnico).	Protege la información aun cuando el dispositivo físico se extravíe o sea sustraído.

Alteración de información financiera en el ERP	Perfiles de acceso diferenciados según el cargo, registro de auditoría (logs) y restricción del uso de dispositivos USB no autorizados (control técnico).	Dificulta la manipulación no autorizada de la información financiera y permite identificar el origen de cualquier cambio.

Las políticas y los controles propuestos se diseñaron a partir de una relación directa con los riesgos priorizados en la matriz de riesgos, de manera que cada medida responde a una causa concreta identificada durante el diagnóstico. La política de gestión de usuarios y contraseñas, junto con el control de autenticación multifactor, ataca directamente la vulnerabilidad estructural de las credenciales compartidas en el sistema POS, que constituye el riesgo de mayor prioridad para la organización; al exigir identidades individuales, se elimina la posibilidad de acceso indebido no trazable y se refuerza la responsabilidad individual de cada colaborador.

De forma similar, la política de clasificación de la información y el control de cifrado de la base de datos CRM abordan el segundo riesgo más crítico, relacionado con la protección de los datos personales de más de 75.000 clientes; estas medidas no solo reducen la probabilidad de una fuga de información, sino que constituyen una condición indispensable para el cumplimiento de la Ley 1581 de 2012, evitando la exposición a sanciones de la Superintendencia de Industria y Comercio.

La política de segmentación de redes y su respectivo control técnico atienden la debilidad de infraestructura identificada como uno de los riesgos de mayor probabilidad, al eliminar la conexión directa entre la red de clientes y los sistemas internos, condición que en el pasado permitió el acceso no autorizado documentado en el diagnóstico. Por su parte, la política de uso seguro del correo electrónico y los controles técnicos asociados (filtros antispam y protocolos de autenticación de dominio) buscan reducir la efectividad de los ataques de phishing, un vector que ya afectó a la organización y que se agrava por la falta de capacitación del personal.

Los controles de tipo administrativo, en particular el programa de capacitación y sensibilización, resultan fundamentales porque atienden el riesgo transversal del factor humano, presente en la mayoría de los eventos registrados en los últimos tres años. Ningún control técnico, por robusto que sea, puede compensar por completo una cultura organizacional en la que la seguridad se percibe como responsabilidad exclusiva del área de TI.

En conjunto, las políticas y los controles propuestos abordan de manera proporcional los riesgos de nivel alto identificados en la matriz, sin descuidar los riesgos de nivel medio relacionados con la integridad de la información financiera y la protección de los

dispositivos móviles. Esta proporcionalidad es consistente con el principio de gestión de riesgos establecido en la norma ISO/IEC 27001:2022, según el cual los controles deben ser adecuados al nivel de riesgo que pretenden mitigar, evitando tanto la sobreprotección de activos de baja criticidad como la desatención de los riesgos más significativos para la continuidad del negocio (ISO/IEC 27001, 2022).

Gestión de incidentes y continuidad del negocio

La gestión de incidentes y la continuidad del negocio son componentes complementarios de la estrategia de ciberseguridad de FOODEXPRESS COLOMBIA S.A.S.: mientras la primera define cómo la organización detecta, contiene y recupera su operación ante un evento que compromete la información o los sistemas, la segunda garantiza que los procesos críticos puedan mantenerse o restablecerse dentro de un tiempo aceptable. A continuación, se identifican los incidentes con mayor probabilidad de ocurrencia y se plantea un plan básico de respuesta alineado con las fases reconocidas internacionalmente para la gestión de incidentes de seguridad.

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***
Cifrado de información por ransomware en los servidores virtuales	Un archivo malicioso ejecutado en un equipo conectado a la red compromete uno o varios servidores, cifrando las bases de datos del POS o del ERP y exigiendo un pago para su liberación.	Interrupción total o parcial de la operación en los puntos de venta, imposibilidad de procesar transacciones y pérdida temporal de acceso a la información financiera y de inventarios.
Acceso no autorizado al sistema POS mediante credenciales compartidas	Un tercero o un colaborador sin autorización utiliza credenciales compartidas entre administradores para ingresar al sistema de ventas y alterar o consultar registros.	Pérdida de trazabilidad financiera, posible fraude interno y dificultad para identificar al responsable de las acciones realizadas.

Ataque de phishing exitoso sobre el correo institucional	Un colaborador ingresa sus credenciales institucionales en un sitio fraudulento que suplanta a un área interna, permitiendo que un atacante intente acceder a los sistemas de la organización.	Compromiso de cuentas institucionales, posible acceso a información confidencial y afectación de la confianza interna en las comunicaciones oficiales.
Fuga de los datos personales del programa de fidelización	Exposición no autorizada de la base de datos CRM, que contiene información de más de 75.000 clientes, por un ataque externo o una filtración interna.	Sanciones bajo la Ley 1581 de 2012, pérdida de confianza de los clientes y daño reputacional significativo para la marca.
Pérdida o robo de un equipo portátil con información sensible	Un dispositivo asignado a personal directivo o de supervisión se extravía o es sustraído, conteniendo reportes operativos y bases de datos exportadas sin cifrar.	Exposición de información estratégica y de clientes, con dificultad para determinar el alcance real del compromiso.
Falla del sistema POS por errores de sincronización entre servidores	Indisponibilidad del sistema centralizado de ventas que obliga a registrar las transacciones de forma manual durante varias horas, como ocurrió previamente en uno de los restaurantes.	Retrasos operativos, riesgo de inconsistencias en los registros de ventas y afectación de la experiencia del cliente.

Una vez identificados los incidentes con mayor probabilidad de materializarse, es necesario definir un plan de respuesta estructurado que permita a la organización actuar de manera oportuna y ordenada. La siguiente tabla presenta las fases básicas de respuesta que FOODEXPRESS COLOMBIA S.A.S. debería adoptar, inspiradas en el modelo de gestión de incidentes reconocido internacionalmente en el campo de la ciberseguridad.

Tabla 8. Plan básico de respuesta

Fase	***Acción***
Detección	Identificar el incidente mediante el monitoreo de los sistemas, los reportes del personal o las alertas generadas por las herramientas de seguridad, confirmando que efectivamente se trata de un evento que compromete la confidencialidad, la integridad o la disponibilidad de la información.
Contención	Aislar de forma inmediata los equipos, cuentas o segmentos de red comprometidos —por ejemplo, desconectar el servidor afectado o suspender las credenciales involucradas— para evitar que el incidente se propague al resto de la infraestructura.
Erradicación	Eliminar la causa raíz del incidente, ya sea el software malicioso, el acceso indebido o la vulnerabilidad explotada, y corregir las configuraciones o credenciales comprometidas antes de restablecer el servicio.
Recuperación	Restaurar los sistemas y la información afectada a partir de las copias de seguridad verificadas, validando su correcto funcionamiento antes de reincorporarlos a la operación de los restaurantes.
Lecciones aprendidas	Documentar el incidente, analizar sus causas y fortalecer las políticas, los controles y los programas de capacitación de la organización para reducir la probabilidad de que se repita.

La respuesta ante un incidente de seguridad en FOODEXPRESS COLOMBIA S.A.S. debe iniciar con la activación de un procedimiento claro que involucre al coordinador de TI, a los analistas de soporte y, cuando el incidente afecte datos personales o la operación comercial, a la Dirección de Operaciones y a la Gerencia General. La organización actualmente no cuenta con un procedimiento formal para la gestión de incidentes, situación que debe corregirse mediante la adopción de las cinco fases descritas anteriormente, las cuales permiten reducir el tiempo de exposición y minimizar el impacto sobre los clientes y la operación diaria de los 12 restaurantes.

Durante la respuesta a un incidente, la comunicación interna cumple un papel determinante. La experiencia registrada en el Evento 1, en el que un colaborador reportó oportunamente el ingreso de sus credenciales en un sitio fraudulento, permitió a la organización detectar los intentos de acceso no autorizado antes de que se agravaran; esta reacción debe convertirse en la norma y no en la excepción, mediante un canal claro y conocido por todo el personal para reportar situaciones sospechosas sin temor a

represalias. De igual manera, se recomienda designar un responsable de comunicación durante la crisis, encargado de informar a los clientes, a las franquicias y, cuando corresponda, a la Superintendencia de Industria y Comercio, evitando que la información se divulgue de manera desorganizada o que se agrave el daño reputacional de la marca.

En cuanto a la continuidad del negocio, la organización debe priorizar la protección de sus procesos críticos: la venta presencial a través del sistema POS, la gestión de pedidos digitales y de domicilios, y la disponibilidad de la información financiera consolidada en el ERP. El Evento 2 documentado en el diagnóstico, en el que uno de los restaurantes debió registrar las ventas de forma manual durante varias horas por una falla de sincronización entre servidores, evidencia que la organización ya cuenta, de manera informal, con una capacidad básica de continuidad operativa; sin embargo, esta capacidad debe formalizarse mediante procedimientos documentados de contingencia, de manera que cualquier punto de venta pueda operar manualmente por un periodo definido sin comprometer la trazabilidad de las transacciones ni la experiencia del cliente.

Adicionalmente, la continuidad del negocio depende directamente de la confiabilidad de las copias de seguridad. Dado que actualmente los respaldos se ejecutan diariamente pero no se someten a pruebas periódicas de restauración, la organización no tiene certeza de que la información pueda recuperarse en un escenario real de pérdida, como un ataque de ransomware sobre los servidores virtuales. Por ello, se recomienda establecer objetivos concretos de tiempo de recuperación (RTO) y de punto de recuperación (RPO) para los sistemas críticos, de modo que el sistema POS y el ERP puedan restablecerse en un plazo máximo definido por la organización, y que la pérdida de información en caso de incidente no supere el respaldo más reciente verificado.

Este enfoque de gestión de incidentes y continuidad operativa es coherente con las funciones de "responder" y "recuperar" descritas en el Marco de Ciberseguridad del NIST (NIST, 2018), el cual complementa el ciclo de identificación, protección y detección desarrollado en los capítulos anteriores del presente informe. La adopción formal de este enfoque permitiría a FOODEXPRESS COLOMBIA S.A.S. reducir de manera significativa el tiempo de interrupción ante incidentes futuros, proteger la confianza de sus más de 75.000 clientes registrados y sostener el crecimiento proyectado hacia nuevas sedes y nuevos medios de pago digital.

Cultura organizacional en ciberseguridad

La cultura organizacional constituye uno de los factores más determinantes en la efectividad de cualquier estrategia de ciberseguridad, pues las políticas y los controles técnicos más robustos pierden buena parte de su eficacia si las personas que interactúan a diario con los sistemas no comprenden su importancia o no los aplican de manera consistente. En el caso de FOODEXPRESS COLOMBIA S.A.S., las entrevistas realizadas durante el diagnóstico inicial revelaron un conjunto de comportamientos y percepciones que, si bien no constituyen amenazas técnicas en sí mismas, actúan como vulnerabilidades organizacionales que incrementan la probabilidad de que los riesgos identificados en los capítulos anteriores lleguen a materializarse.

Cuando una organización cuenta con una cultura sólida de ciberseguridad, sus colaboradores reportan oportunamente los incidentes, cumplen las políticas de manera natural y perciben la protección de la información como parte de su labor diaria; por el contrario, la ausencia de esta cultura favorece el incumplimiento de procedimientos, retrasa la detección de incidentes y traslada de manera desproporcionada la responsabilidad de la seguridad a un equipo de tecnología que, con apenas cuatro integrantes, no tiene la capacidad de vigilar por sí solo el comportamiento de 280 colaboradores distribuidos en 12 restaurantes.

Tabla 9. Hallazgos organizacionales

Situación observada	***Riesgo asociado***
Los colaboradores priorizan la rapidez en la atención al cliente sobre el cumplimiento de los procedimientos de seguridad.	Incumplimiento sistemático de políticas y adopción de atajos inseguros, como el uso de credenciales compartidas en el sistema POS.
Algunos administradores de punto de venta consideran que los controles de seguridad retrasan la operación diaria.	Resistencia a la adopción de nuevos controles técnicos y administrativos, incluso cuando reducen riesgos críticos.
Existe poca comunicación entre el área de Tecnología y Sistemas y las áreas operativas de los restaurantes.	Detección y reporte tardío de incidentes, y desalineación entre las necesidades operativas y las medidas de seguridad implementadas.
Los nuevos colaboradores reciben capacitación operativa, pero no siempre formación en seguridad de la información desde su ingreso.	Personal desprevenido frente a amenazas comunes, como el phishing, desde el inicio de su vinculación laboral.

Muchos empleados desconocen los riesgos asociados al phishing, al malware o a la fuga de información.	Mayor probabilidad de éxito de ataques de ingeniería social, como el evidenciado en el Evento 1 del diagnóstico.
El personal considera que los incidentes tecnológicos son poco probables dentro de la organización.	Baja percepción del riesgo, lo que reduce la vigilancia y el reporte oportuno de comportamientos o correos sospechosos.
El personal operativo considera que la seguridad de la información es responsabilidad exclusiva del área de Tecnología y Sistemas.	Ausencia de corresponsabilidad frente a la protección de la información, con controles dependientes casi exclusivamente de un equipo de cuatro personas.

Tabla 10. Recomendaciones de mejora

Hallazgo	***Recomendación***
Priorización de la rapidez operativa sobre el cumplimiento de los procedimientos de seguridad.	Rediseñar los procedimientos críticos (como el inicio de sesión en el POS) para que las medidas de seguridad impliquen la menor fricción posible, y reforzar su cumplimiento mediante indicadores de gestión visibles para cada punto de venta.
Percepción de que los controles de seguridad retrasan la operación.	Involucrar a los administradores de punto de venta en el diseño e implementación de los controles, explicando claramente su propósito y los beneficios para la operación y para ellos mismos.
Poca comunicación entre el área de Tecnología y las áreas operativas.	Establecer canales formales y periódicos de comunicación, como comités de seguridad o boletines internos, que mantengan informado al personal sobre riesgos y medidas vigentes.

Falta de formación en seguridad desde el ingreso del colaborador.	Incorporar un módulo obligatorio de seguridad de la información dentro del proceso de inducción de todo el personal, independientemente de su cargo.
Desconocimiento generalizado de amenazas como el phishing y el malware.	Implementar un programa permanente de capacitación y simulaciones periódicas de phishing que permitan medir y mejorar la capacidad de detección del personal.
Baja percepción del riesgo por parte de los colaboradores.	Difundir, de manera anonimizada, los eventos reales ocurridos en la organización durante los últimos tres años, para sensibilizar sobre la probabilidad real de los incidentes.
Percepción de la seguridad como responsabilidad exclusiva del área de Tecnología.	Impulsar el liderazgo visible de la alta dirección en las iniciativas de seguridad y definir roles y responsabilidades claras en cada área de la organización.

Las recomendaciones planteadas buscan transformar la cultura organizacional de FOODEXPRESS COLOMBIA S.A.S. desde un enfoque reactivo, centrado en el cumplimiento ocasional de normas durante auditorías, hacia una cultura preventiva en la que la seguridad de la información se perciba como una responsabilidad compartida por todos los niveles de la organización. El rediseño de los procedimientos críticos y la participación de los administradores de punto de venta en el diseño de los controles atienden directamente la resistencia identificada en el diagnóstico, pues una medida percibida como impuesta desde fuera tiene menor probabilidad de sostenerse en el tiempo que una construida con la participación de quienes la aplican a diario.

El fortalecimiento de la comunicación entre el área de Tecnología y Sistemas y las áreas operativas, junto con la incorporación de la seguridad en los procesos de inducción, permitiría cerrar la brecha de conocimiento que actualmente deja al personal operativo como el eslabón más vulnerable de la organización frente a técnicas de ingeniería social. El programa permanente de capacitación y las simulaciones periódicas de phishing, en particular, ofrecen una forma medible de verificar si estas recomendaciones están generando un cambio real de comportamiento, en lugar de limitarse a una actividad formal sin seguimiento.

Finalmente, el liderazgo visible de la alta dirección resulta determinante para consolidar estas transformaciones. Cuando la Gerencia General y las direcciones de Operaciones y

de Talento Humano participan activamente en las campañas de seguridad, se envía un mensaje claro de que la protección de la información no es una función aislada del área de Tecnología, sino un compromiso institucional. Esta corresponsabilidad es especialmente relevante para FOODEXPRESS COLOMBIA S.A.S. considerando sus planes de expansión a cinco nuevas sedes y la incorporación de pagos mediante billeteras digitales, iniciativas que ampliarán tanto la superficie de exposición de la organización como la necesidad de que toda su fuerza laboral, y no solo el equipo de TI, actúe como una línea activa de defensa.

Conclusiones

El diagnóstico realizado evidencia que la mayor exposición al riesgo de FOODEXPRESS COLOMBIA S.A.S. no proviene principalmente de la ausencia de tecnología, sino de la falta de gobernanza sobre su uso: la organización dispone de una plataforma tecnológica relativamente robusta, pero opera sin políticas formales que regulen su uso, lo que confirma que la seguridad de la información depende tanto de decisiones organizacionales como de herramientas tecnológicas.

La práctica de compartir credenciales, presente tanto en el sistema POS como en el acceso a la red corporativa, se consolidó como el patrón de riesgo más transversal identificado durante el análisis, al estar directamente relacionado con varios de los eventos documentados en los últimos tres años; esto sugiere que una sola vulnerabilidad organizacional, si no se corrige, puede materializarse repetidamente bajo distintas formas de incidente.

La ausencia de segmentación entre la red WiFi corporativa y la red destinada a los clientes representa una de las decisiones de infraestructura con mayor impacto potencial sobre la totalidad de los sistemas de la organización, lo que evidencia la importancia de que las decisiones de arquitectura tecnológica se evalúen también desde una perspectiva de seguridad y no únicamente de costo u operatividad.

El factor humano se confirma como el eslabón más determinante de la cadena de seguridad de la organización: los eventos de phishing y de acceso indebido mediante credenciales compartidas no habrían tenido el mismo alcance si el personal hubiese contado con formación adecuada, lo que reafirma que ninguna inversión en controles técnicos sustituye la necesidad de una cultura organizacional de seguridad sólida y sostenida en el tiempo.

El crecimiento proyectado de FOODEXPRESS COLOMBIA S.A.S. representa una oportunidad para incorporar la seguridad de la información desde el diseño de los nuevos procesos, en lugar de tratarla como una corrección posterior, lo que resultaría considerablemente más costoso y complejo una vez la infraestructura esté en operación.

El desarrollo de este informe permitió comprender que la gestión de riesgos, las políticas de seguridad, la respuesta a incidentes y la cultura organizacional no son componentes

independientes, sino un sistema interrelacionado: una política sin un control que la respalde carece de efecto práctico, y un control sin una cultura que lo sostenga tiende a debilitarse con el tiempo, por lo que las recomendaciones formuladas deben implementarse de manera articulada y no como iniciativas aisladas.

Referencias

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"*. Diario Oficial No. 47.223.

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

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

International Organization for Standardization. (2012). *Information technology — Security techniques — Guidelines for cybersecurity* (ISO/IEC Standard No. 27032:2012).

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001:2022).

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO/IEC Standard No. 27005:2022).

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.