TRABAJO DE GRADO
Opción Seminario-Diplomado.

Informe tecnico Seminario Ciberseguridad a la Empresa Distrifresh S.A.S

Corporación Universitaria Remington.
Facultad de sistemas
Ingeniería de sistemas

Michael chavez zapata
Jorge Leonardo Ramírez Restrepo

Seminario de Ciberseguridad Organizacional

2026

Tabla de Contenidos

Resumen

El presente informe técnico analiza la situación de seguridad de la información en DistriFresh S.A.S., una empresa hipotética de distribución de alimentos con sede en Pereira, Colombia. La organización gestiona información sensible de clientes, proveedores y finanzas a través de canales digitales informales como WhatsApp y correo electrónico, sin contar con políticas, controles ni procedimientos formales de ciberseguridad.

El propósito del informe es aplicar los conocimientos adquiridos en el Seminario de Ciberseguridad Organizacional para identificar los activos de información de la empresa, analizar las amenazas y vulnerabilidades presentes, evaluar los riesgos asociados mediante una matriz de riesgos, y proponer controles de seguridad alineados con el estándar ISO 27001, el marco NIST y la normativa colombiana vigente (Ley 1581 de 2012).

Durante el desarrollo del trabajo se identificaron activos críticos como la base de datos de clientes, la información financiera y los procesos de ventas y entrega. Se detectaron vulnerabilidades relacionadas con la falta de autenticación segura, ausencia de copias de seguridad, acceso no controlado por roles y el manejo desprotegido de información confidencial. Frente a estas vulnerabilidades, se identificaron amenazas reales como el robo de información, fraude interno, pérdida de datos y suplantación de identidad. Como resultado del ciclo completo de análisis (identificar, evaluar, proponer), se presenta una matriz de riesgos y un conjunto de controles preventivos y correctivos orientados a reducir los riesgos más críticos y mejorar la postura de seguridad de la organización.

Palabras clave

ciberseguridad organizacional, activos de información, amenazas, vulnerabilidades, gestión de riesgos, ISO 27001, matriz de riesgos.

Marco Conceptual y Contextual

Marco Conceptual

La ciberseguridad organizacional comprende el conjunto de prácticas, políticas y tecnologías mediante las cuales una organización protege sus sistemas, redes y datos frente a amenazas digitales (Ramírez Restrepo, 2026). En el contexto de las pequeñas y medianas empresas (PYME) colombianas, esta disciplina cobra especial relevancia porque la informalidad en el manejo de información sensible puede derivar en consecuencias legales, financieras y reputacionales que comprometan la viabilidad del negocio. Tres conceptos articulan el análisis de este informe: activos, amenazas y riesgos.

Los activos de información son los elementos de valor que una organización necesita proteger: datos (bases de clientes, registros financieros), personas (empleados que acceden a información crítica) y procesos (procedimientos operativos que generan o transmiten información). Una amenaza es cualquier evento con potencial de causar daño sobre estos activos; una vulnerabilidad es la debilidad interna que permite que esa amenaza se materialice. El riesgo resulta de la combinación de ambas variables y se cuantifica mediante la fórmula Riesgo = Probabilidad × Impacto, lo que permite priorizar la respuesta según la criticidad de cada escenario.

En ese sentido, el riesgo no es un concepto abstracto: es el resultado medible de no haber tomado decisiones a tiempo. Entenderlo así —como consecuencia de una omisión— cambia la perspectiva con la que una organización debe abordar la seguridad de su información.

Dos marcos de referencia guían el análisis de este informe. El primero es la norma **ISO/IEC 27001:2022**, que en el contexto de DistriFresh S.A.S. se aplica principalmente a través de su Anexo A: el control A.9 orienta cómo restringir el acceso a los archivos financieros según el rol de cada empleado; el control A.10 fundamenta la necesidad de cifrar las comunicaciones con clientes; el A.12.3 justifica la política de copias de seguridad automáticas; y el A.7 respalda las acciones de capacitación del personal (ISO, 2022). El segundo es el **marco NIST**, cuyas cinco funciones se traducen operativamente así para esta empresa: Identificar (inventario de activos y evaluación de riesgos), Proteger (controles de acceso y cifrado), Detectar (logs de auditoría), Responder (protocolo de incidentes) y Recuperar (plan de copias de seguridad y restauración) (NIST, 2018). Ninguno de los dos marcos requiere infraestructura tecnológica sofisticada para ser aplicado en una PYME; su valor está en la metodología que proponen, no en la escala.

En el plano legal colombiano, la **Ley 1581 de 2012** no es una recomendación: es una obligación. Para DistriFresh S.A.S., esto significa que compartir la base de datos de clientes por WhatsApp sin ningún control no es solo una mala práctica operativa, sino una conducta que puede derivar en sanciones administrativas impuestas por la Superintendencia de Industria y Comercio. La empresa recolecta y almacena nombres, teléfonos y direcciones de entrega de sus clientes; eso la convierte en responsable del tratamiento de datos personales bajo los términos de esta ley (Congreso de la República, 2012), con independencia de su tamaño o de si su sistema es informal o no.

Marco Contextual

DistriFresh S.A.S. es una empresa hipotética de distribución de alimentos y productos perecederos ubicada en la ciudad de Pereira, Risaralda. La empresa opera con aproximadamente 15 empleados distribuidos en áreas de ventas, logística, contabilidad y administración. Su modelo de negocio se basa en la recepción de pedidos de clientes minoristas a través de canales informales como WhatsApp, llamadas telefónicas y correo electrónico, para luego coordinar la entrega con proveedores locales.

La información de clientes, pedidos y facturación se gestiona principalmente en hojas de cálculo de Excel que se comparten entre los empleados a través de grupos de WhatsApp y correos electrónicos sin cifrar. La empresa no cuenta con un sistema de información centralizado, ni con políticas formales de seguridad, contraseñas seguras, control de acceso por roles o mecanismos de respaldo de la información.

Esta situación genera un entorno de alta exposición al riesgo, donde la confidencialidad, integridad y disponibilidad de la información crítica del negocio pueden verse comprometidas fácilmente por errores humanos, accesos no autorizados o pérdida de dispositivos, lo que justifica plenamente el desarrollo del presente análisis de ciberseguridad.

Desarrollo e Implementación del Aprendizaje

Definición del Problema

DistriFresh S.A.S. presenta una problemática clara en la gestión de su información: los datos de clientes, proveedores y transacciones financieras se manejan sin ningún control de seguridad formal. Los empleados comparten archivos con información sensible a través de aplicaciones de mensajería sin cifrado, no existen copias de seguridad automatizadas, y cualquier integrante del equipo puede acceder a información que no corresponde a su rol. Desde el análisis realizado, el mayor riesgo no es un ataque externo, sino la falta de control interno sobre la información.

Esta situación expone a la empresa a riesgos concretos: pérdida de información ante falla de un dispositivo, fuga de datos de clientes a la competencia, fraude interno por acceso indiscriminado a registros financieros, y posibles sanciones por incumplimiento de la Ley 1581 de 2012 en materia de protección de datos personales.

Identificación de Activos de Información

De acuerdo con el estándar ISO 27001 (2022), el primer paso en la gestión de riesgos consiste en identificar y clasificar los activos de información que requieren protección. A continuación se presenta la tabla de activos identificados en DistriFresh S.A.S., clasificados por tipo, nivel de criticidad y justificación de su importancia para la operación del negocio:

Tabla 1. Activos de información de DistriFresh S.A.S.

Tipo	Activo	Descripción	Ubicación	Responsable	Criticidad	Justificación
Datos	Base de datos de clientes	Información personal y compras de clientes	Hojas de cálculo, WhatsApp	Ventas	**Alta**	Clave para ventas y relación con clientes
Datos	Información financiera	Registros de pagos y facturación	Correos, archivos contables	Contador	**Alta**	Impacta ingresos y control financiero
Datos	Conversaciones con clientes	Mensajes en WhatsApp y redes	Dispositivos móviles	Ventas / Redes	**Media**	Contiene acuerdos comerciales
Datos	Información de proveedores	Datos de contacto y pedidos	Correos electrónicos	Gerencia / Logística	**Media**	Permite abastecimiento del negocio
Personas	Vendedores	Gestionan pedidos y datos de clientes	Área comercial	Ventas	**Alta**	Manejan información crítica directamente
Personas	Contador	Manejo de información financiera	Área contable	Contabilidad	**Alta**	Accede a datos financieros sensibles
Procesos	Proceso de ventas	Registro y gestión de pedidos	General	Ventas	**Alta**	Fallas afectan directamente la operación
Procesos	Validación de pagos	Confirmación de transacciones	Contabilidad	Contador	**Alta**	Impacta ingresos y control financiero
Procesos	Gestión de información	Manejo y almacenamiento de datos	General	Todos	**Alta**	No está estructurado, genera riesgo elevado
Procesos	Proceso de entrega	Coordinación de envíos	Logística	Logística	**Media**	Afecta satisfacción del cliente

Justificación de criticidad: impacto en la continuidad operacional

La clasificación de criticidad de los activos no es un ejercicio teórico: cada nivel de criticidad representa un escenario concreto de interrupción del negocio. Para DistriFresh S.A.S., los activos marcados como de criticidad alta son aquellos cuya pérdida, alteración o exposición podría detener o comprometer de forma irreversible la operación del negocio. Los de criticidad media generan problemas operativos relevantes pero recuperables en el corto plazo.

Si se pierde o compromete la base de datos de clientes, DistriFresh pierde su capacidad de contactar a sus compradores habituales, de gestionar pedidos pendientes y de mantener los acuerdos comerciales ya establecidos. El impacto no es solo operativo: también es legal bajo la Ley 1581 de 2012, y reputacional frente a clientes que depositan su confianza en la empresa. Si se compromete la información financiera, la empresa pierde trazabilidad sobre sus ingresos y pagos, lo que puede generar errores contables, pagos duplicados o no detectados, e incluso fraudes que pasen desapercibidos durante semanas. Si el proceso de validación de pagos falla o es alterado —por ejemplo, porque un empleado no autorizado modifica un registro—, la empresa puede pagar a proveedores incorrectos o dejar de cobrar a clientes, afectando directamente su flujo de caja. Y si el proceso de ventas se interrumpe porque los archivos de pedidos se pierden o se vuelven inaccesibles, la coordinación con logística colapsa y la entrega de productos a tiempo se hace imposible. En una empresa de 15 personas donde cada proceso depende de pocas personas y herramientas informales, la pérdida de un activo crítico no tiene red de protección: el daño es inmediato y visible.

Análisis de Amenazas y Vulnerabilidades

El análisis de amenazas y vulnerabilidades constituye el núcleo del diagnóstico de ciberseguridad. Tal como lo establece el marco ISO 27001 (2022), una amenaza por sí sola no representa riesgo si no existe una vulnerabilidad que pueda explotar; es la combinación de ambas lo que produce el incidente. A continuación, se presentan las principales amenazas detectadas en DistriFresh S.A.S., cada una relacionada directamente con la vulnerabilidad que la habilita y el activo que pone en peligro.

Amenaza 1: Fuga de datos de clientes por canales no seguros

DistriFresh S.A.S. gestiona la información personal y comercial de sus clientes —nombres, teléfonos, direcciones de entrega y registros de compras— a través de grupos de WhatsApp y correos electrónicos sin cifrar. Esta práctica expone permanentemente los datos a terceros no autorizados que puedan acceder a los dispositivos de los empleados o interceptar comunicaciones.

Amenaza identificada: Acceso no autorizado y robo de información personal de clientes.

Vulnerabilidad asociada: Ausencia de canales seguros y cifrados para la transmisión de información sensible.

Activo afectado: Base de datos de clientes (criticidad Alta).

Cuando esta amenaza se materializa, la empresa podría enfrentar la pérdida de clientes estratégicos, daño reputacional y sanciones legales bajo la Ley 1581 de 2012

(Congreso de la República, 2012), que exige implementar medidas técnicas y administrativas para proteger los datos personales.

Amenaza 2: Fraude interno por acceso irrestricto a información financiera

La información de pagos, facturación y transacciones de DistriFresh S.A.S. se almacena en hojas de cálculo de Excel accesibles para todos los miembros del equipo, sin distinción de rol o responsabilidad. Esto significa que un vendedor de campo tiene acceso a los mismos registros contables que el contador, lo cual abre la puerta al fraude interno.

Amenaza identificada: Manipulación fraudulenta o robo de información financiera por parte de empleados con acceso indebido.

Vulnerabilidad asociada: Inexistencia de controles de acceso basados en roles (RBAC), uno de los controles fundamentales del Anexo A de la ISO 27001 (A.9).

Activos afectados: Información financiera y proceso de validación de pagos (criticidad Alta).

Amenaza 3: Pérdida irreversible de información por falla de dispositivos

Amenaza identificada: Pérdida definitiva de información crítica del negocio por falla física o robo de dispositivos.

Vulnerabilidad asociada: Ausencia total de políticas de respaldo (backup) y de un repositorio centralizado de información, incumpliendo el control A.12.3 de ISO 27001.

Activos afectados: Conversaciones con clientes, información de proveedores, proceso de ventas y proceso de entrega.

Amenaza 4: Suplantación de identidad y engaño a clientes o proveedores

Amenaza identificada: Suplantación de identidad de empleados para desviar pagos, obtener información confidencial o dañar la reputación de la empresa.

Vulnerabilidad asociada: Uso de canales de comunicación personales e informales sin autenticación corporativa.

Activos afectados: Proceso de ventas, validación de pagos, relación con clientes y proveedores.

Tabla 2. Resumen de amenazas, vulnerabilidades e impacto en DistriFresh S.A.S.

Amenaza	Vulnerabilidad	Activo(s) afectado(s)	Impacto	Criticidad
Fuga de datos de clientes por canales no seguros	Ausencia de canales cifrados; uso de WhatsApp personal sin control	Base de datos de clientes	Legal, financiero y reputacional	**Alta**
Fraude interno por acceso irrestricto a registros financieros	Sin control de acceso por roles (RBAC); archivos sin protección	Información financiera, proceso de pagos	Financiero directo, pérdida de trazabilidad	**Alta**
Pérdida de información por falla o robo de dispositivos	Sin políticas de respaldo; información en dispositivos personales	Conversaciones, pedidos, proveedores	Operativo, interrupción del servicio	**Alta**
Suplantación de identidad	Sin correo corporativo ni	Proceso de ventas, pagos,	Financiero y reputacional	**Alta**

Amenaza	Vulnerabilidad	Activo(s) afectado(s)	Impacto	Criticidad
y engaño a clientes o proveedores	verificación de identidad	relación comercial		

Evaluación de Riesgos: Matriz de Riesgos

La evaluación de riesgos es el paso siguiente a la identificación de amenazas y vulnerabilidades dentro del ciclo de gestión de la seguridad de la información. Según el marco NIST (2018), esta etapa permite cuantificar la exposición de la organización mediante la relación entre la probabilidad de ocurrencia del riesgo y su impacto potencial. La fórmula aplicada es: **Nivel de Riesgo = Probabilidad × Impacto**. Los niveles resultantes se clasifican en: Crítico, Alto, Medio y Bajo.

Figura 1. Matriz de riesgos (probabilidad vs. impacto) – DistriFresh S.A.S.

Probabilidad / Impacto	Bajo	Medio	Alto
Alta	Riesgo Medio	Riesgo Alto	Riesgo Crítico (R1) Fuga datos (R3) Pérdida info (R4) Suplantación
Media	Riesgo Bajo	Riesgo Medio (R2) Fraude interno	Riesgo Alto
Baja	Riesgo Bajo	Riesgo Bajo	Riesgo Medio

Figura 1. Matriz de riesgos. Elaboración propia.

Tabla 3. Detalle de evaluación de riesgos – DistriFresh S.A.S.

ID	Riesgo	Causa (Vulnerabilidad)	Activo afectado	Consecuencia	Probabilidad	Impacto	Nivel
R1	Fuga de datos personales de clientes	Canales no cifrados (WhatsApp sin control)	Base de datos clientes	Sanciones Ley 1581, daño reputacional	Alta	Alto	Crítico

ID	Riesgo	Causa (Vulnerabilidad)	Activo afectado	Consecuencia	Probabilidad	Impacto	Nivel
R2	Fraude interno en registros financieros	Ausencia de control de acceso por roles (RBAC)	Información financiera	Pérdida económica directa, falta de trazabilidad	Media	Alto	Alto
R3	Pérdida irreversible de datos operativos	Sin backup centralizado; info en dispositivos personales	Conversaciones, pedidos, proveedores	Interrupción operativa, pérdida de clientes	Alta	Alto	Crítico
R4	Suplantación de identidad de empleados	Sin correo corporativo ni autenticación de identidad	Proceso ventas, pagos, relación comercial	Fraude a clientes y proveedores, daño reputacional	Alta	Alto	Crítico

Los cuatro riesgos identificados obtienen una valoración de crítico o alto, lo que refleja que la ausencia de controles básicos de seguridad en DistriFresh S.A.S. genera una exposición máxima. Esta situación exige la implementación inmediata de controles de seguridad priorizados por nivel de riesgo.

Por qué todos los riesgos son críticos en una empresa pequeña

Que los cuatro riesgos hayan alcanzado nivel crítico o alto no es casualidad ni exageración metodológica: es el resultado directo de la combinación de probabilidad alta e impacto alto que caracteriza el entorno de DistriFresh S.A.S. La probabilidad es alta porque las vulnerabilidades no son hipotéticas —están activas hoy, en cada turno de trabajo—: cada vez que un empleado envía un archivo por WhatsApp, la amenaza tiene la oportunidad de materializarse. El impacto es alto porque en una empresa de 15 personas, donde muchas funciones críticas dependen de un solo dispositivo, una sola persona o un solo archivo, no existe redundancia ni margen de error. Una organización grande puede perder la base de datos de un vendedor y tener siete copias de respaldo en distintos servidores; DistriFresh no. Por eso la ausencia de controles en una PYME amplifica el

riesgo de manera desproporcional respecto a lo que ocurriría con el mismo incidente en una empresa con infraestructura robusta. Esta realidad es la que justifica la urgencia de los controles propuestos en la sección siguiente: no son medidas de largo plazo para un plan de mejora futuro; son acciones que deberían haberse tomado antes y que cada día de retraso aumenta la probabilidad de un incidente real.

Propuesta de Controles de Seguridad

Con base en los riesgos evaluados y siguiendo las directrices del Anexo A de la norma ISO 27001 (2022) y las funciones de Protección y Recuperación del marco NIST (2018), a continuación se proponen controles de seguridad específicos para cada riesgo identificado en DistriFresh S.A.S. Los controles se clasifican como: **Preventivos** (evitan que el riesgo se materialice), **Detectivos** (permiten identificar incidentes en curso) y **Correctivos** (facilitan la recuperación tras un incidente).

Tabla 4. Controles de seguridad propuestos para DistriFresh S.A.S.

Riesgo	Control propuesto	Descripción del control	Tipo	Marco de referencia	Responsable	Prioridad
R1	Plataforma centralizada en la nube con control de acceso	Migrar las bases de datos de clientes a Google Drive o OneDrive con permisos por usuario, eliminando el intercambio de archivos por WhatsApp	Preventivo	ISO 27001 A.8.1 / NIST Proteger	Gerencia / Área de TI	**Inmediata**
R1	Cifrado de comunicaciones	Implementar correos corporativos con cifrado TLS y capacitar al personal sobre el manejo seguro de datos de clientes según la Ley 1581 de 2012	Preventivo	Ley 1581 / ISO 27001 A.10	Gerencia	**Inmediata**
R2	Control de acceso basado en roles (RBAC)	Definir y aplicar permisos diferenciados por cargo: solo el contador accede a archivos financieros, los vendedores únicamente a datos de pedidos y clientes	Preventivo	ISO 27001 A.9 / NIST Proteger	Administrador / Gerencia	**Alta**
R2	Registro y auditoría de accesos	Habilitar logs de auditoría en la plataforma de almacenamiento para registrar quién accede, modifica o elimina archivos financieros	Detectivo	ISO 27001 A.12.4 / NIST Detectar	Administrador	**Alta**

Riesgo	Control propuesto	Descripción del control	Tipo	Marco de referencia	Responsable	Prioridad
R3	Política de copias de seguridad automáticas	Establecer backups automáticos diarios en la nube (Google Drive, OneDrive o Dropbox) para toda la información operativa crítica de la empresa	Correctivo / Preventivo	ISO 27001 A.12.3 / NIST Recuperar	Administrador / Todos	Inmediata
R4	Correo corporativo y verificación de identidad	Adoptar un dominio corporativo (@distrifresh.com) para todas las comunicaciones comerciales, y establecer protocolos de verificación de identidad para autorizaciones de pago	Preventivo	ISO 27001 A.9 / NIST Proteger	Gerencia	Inmediata
R4	Capacitación en ingeniería social y phishing	Diseñar y ejecutar sesiones de capacitación para todo el personal sobre reconocimiento de fraudes, suplantación de identidad y manejo seguro de solicitudes de pago	Preventivo	NIST Proteger / ISO 27001 A.7	Gerencia / RRHH	Alta

La implementación de estos controles debe realizarse de manera progresiva, priorizando aquellos marcados como de prioridad inmediata. Aunque DistriFresh S.A.S. es una empresa pequeña, la mayoría de los controles propuestos tienen un costo bajo o nulo, dado que se basan en herramientas en la nube de libre acceso y en cambios en las prácticas internas del equipo.

Plan de Implementación Operativa de Controles y Políticas

Proponer controles es apenas el primer paso; la parte crítica —y la que más frecuentemente se omite en organizaciones sin madurez en seguridad— es definir cómo se implementan operativamente. Un control que existe en papel pero que nadie ejecuta no reduce ningún riesgo. Por eso, a continuación, se desarrolla el plan concreto de puesta en

marcha de cada política propuesta para DistriFresh S.A.S., con responsables, plazos y criterios de verificación.

Política 1: Protección de Datos de Clientes — Implementación operativa

En la práctica, esta política exige tres acciones concretas que deben ejecutarse en la primera semana: primero, la gerencia debe crear una carpeta compartida en Google Drive o OneDrive con permisos restringidos por usuario, y migrar allí las bases de datos de clientes que actualmente circulan por WhatsApp; segundo, el administrador debe revocar el acceso a los archivos compartidos por WhatsApp y comunicar por escrito a todo el equipo el nuevo canal oficial de almacenamiento; tercero, se debe establecer una regla operativa clara: ninguna información de clientes puede enviarse por mensajería personal. El incumplimiento de esta regla debe quedar registrado en el código de conducta digital. El criterio de verificación es simple: en un plazo de 15 días, ningún archivo de clientes debe existir fuera de la plataforma centralizada.

Política 2: Control de Acceso por Roles (RBAC) — Implementación operativa

La implementación de esta política requiere que el administrador defina una matriz de permisos antes de migrar los archivos a la plataforma centralizada. Dicha matriz debe especificar qué carpetas o documentos puede ver, editar o eliminar cada cargo: el contador accede exclusivamente a los archivos de facturación y pagos; los vendedores tienen acceso de lectura y escritura solo sobre la carpeta de pedidos y clientes; la gerencia mantiene acceso total. Los logs de auditoría deben habilitarse desde el primer día de uso de la plataforma. Una vez al mes, el administrador debe revisar estos registros y reportar a

gerencia cualquier acceso inusual. Este control no requiere software adicional: Google Drive y OneDrive incluyen estas funcionalidades en sus versiones gratuitas o de bajo costo.

Política 3: Respaldo y Continuidad — Implementación operativa

La política de respaldo se operacionaliza de la siguiente manera: el administrador configura en Google Drive o OneDrive la sincronización automática de todos los archivos críticos. Adicionalmente, una vez a la semana se debe exportar manualmente una copia consolidada de la base de datos de clientes y del registro financiero a una segunda ubicación en la nube (por ejemplo, Dropbox como repositorio secundario). El criterio de continuidad es que, ante la pérdida total de cualquier dispositivo, la empresa sea capaz de restaurar la totalidad de su información operativa en menos de 24 horas. Para verificar que el sistema funciona, se debe realizar una prueba de restauración simulada cada trimestre: borrar un archivo de prueba y confirmar que se puede recuperar desde el respaldo sin contratiempos.

Política 4: Autenticación e Identidad Corporativa — Implementación operativa

Esta política se implementa en dos fases. La primera, en el corto plazo (primer mes): la gerencia contrata un dominio corporativo (@distrifresh.com) y crea cuentas de correo institucional para todos los empleados. A partir de ese momento, toda comunicación comercial con clientes y proveedores —incluyendo confirmaciones de pedidos, facturas y autorizaciones de pago— debe realizarse exclusivamente desde estos correos. La segunda fase, en el mediano plazo (segundo mes): se establece un protocolo de verificación de identidad para solicitudes de pago. Cualquier transferencia o cambio de cuenta bancaria

debe confirmarse mediante una llamada telefónica directa al contacto conocido, independientemente de si llegó por correo o WhatsApp. Este simple paso elimina prácticamente el riesgo de fraude por suplantación. El costo de implementación de un dominio corporativo en Colombia es inferior a 150.000 COP anuales, lo que lo hace completamente viable para una PYME.

Incidentes y Respuesta

Durante el periodo de análisis de DistriFresh S.A.S. no se registraron incidentes formales de seguridad, dado que la empresa no cuenta con mecanismos de reporte ni canales definidos para identificar, registrar o escalar eventos de seguridad. Sin embargo, con base en las vulnerabilidades identificadas y en las amenazas detectadas, es posible anticipar los tipos de incidentes que podrían materializarse si no se implementan los controles propuestos.

Incidentes potenciales identificados:

- Fuga de datos de clientes mediante acceso no autorizado a grupos de WhatsApp o reenvío accidental de archivos a terceros (relacionado con R1).
- Manipulación o eliminación de registros financieros por parte de un empleado con acceso indebido a los archivos contables (relacionado con R2).
- Pérdida total de información operativa por daño o robo de un dispositivo móvil que no cuenta con copia de seguridad (relacionado con R3).
- Suplantación de identidad de un empleado para solicitar transferencias fraudulentas a clientes o proveedores (relacionado con R4).

Plan de respuesta a incidentes propuesto:

Siguiendo la función de Responder del marco NIST (2018) y el control A.16 de la norma ISO 27001 (2022), se propone que DistriFresh S.A.S. adopte un protocolo básico de respuesta a incidentes estructurado en cuatro fases:

1. Detección y reporte: cualquier empleado que identifique una anomalía (acceso no autorizado, pérdida de dispositivo, mensaje sospechoso) debe reportarlo de inmediato a la gerencia mediante un canal designado.

2. Contención: revocar de inmediato el acceso del empleado o dispositivo comprometido, bloquear cuentas afectadas y aislar los archivos comprometidos para evitar mayor propagación del daño.

3. Recuperación: restaurar la información desde la copia de seguridad más reciente, restablecer los accesos bajo el principio de mínimo privilegio y verificar la integridad de los datos recuperados.

4. Lecciones aprendidas: documentar el incidente, analizar su causa raíz, y actualizar las políticas y controles para prevenir su recurrencia. Este registro constituye la base de una memoria institucional de seguridad.

Escenario Práctico Simulado: Incidente de Fuga de Datos en DistriFresh S.A.S.

El siguiente escenario simula un incidente real que podría ocurrir en DistriFresh S.A.S. dadas las vulnerabilidades identificadas en este informe. Su propósito es ilustrar, paso a paso, cómo se desarrolla un evento de fuga de datos y cómo debe activarse el plan

de respuesta propuesto. Este tipo de ejercicio es consistente con las recomendaciones del control A.16 de la norma ISO 27001 (2022) y la función de Responder del marco NIST (2018), que plantean la importancia de que las organizaciones practiquen sus protocolos antes de que ocurra un incidente real.

Contexto del escenario

Martes, 10:15 a.m. Andrés, vendedor del área comercial de DistriFresh S.A.S., recibe un mensaje de WhatsApp de un número desconocido que se identifica como un nuevo cliente mayorista interesado en hacer un pedido grande. El supuesto cliente le pide a Andrés que le envíe la lista de precios actualizada y los datos de contacto de otros clientes como referencia. Andrés, confiado en que parece una oportunidad de venta, reenvía desde el grupo de WhatsApp del equipo el archivo Excel con la base de datos completa de clientes: 430 registros con nombres, teléfonos, direcciones de entrega e historial de compras. Dos horas después, varios clientes de DistriFresh empiezan a recibir mensajes de un competidor ofreciéndoles los mismos productos a precios más bajos.

Paso 1 — Detección y reporte (hora 0)

A las 12:30 p.m., uno de los clientes afectados llama a gerencia para preguntar cómo obtuvieron su número. La gerente, Sandra, identifica de inmediato que se trata de una fuga de datos. Llama a Andrés, quien reconoce haber enviado el archivo. Sandra activa el protocolo de respuesta: notifica al administrador del sistema y al contador, designa a Andrés como informante del incidente y le garantiza que no habrá represalias si colabora completamente. Esto es posible porque la política de reporte sin sanciones ya estaba

establecida. Sin esa política, Andrés probablemente habría ocultado el error por miedo, y la respuesta habría llegado demasiado tarde.

Paso 2 — Contención (hora 0 a hora 2)

El administrador toma tres acciones simultáneas: primero, elimina el archivo Excel de la base de datos del grupo de WhatsApp (aunque ya fue enviado, se limita su circulación futura); segundo, cambia los permisos del archivo en la plataforma centralizada para que solo el área comercial pueda visualizarlo, sin opción de descarga ni reenvío; tercero, bloquea el número desconocido del que provino la solicitud. Sandra redacta un mensaje breve para los clientes afectados informándoles del incidente, pidiéndoles que ignoren cualquier contacto de terceros con su información y reafirmando el compromiso de DistriFresh con la protección de sus datos. Comunicar el incidente a los afectados no es opcional: la Ley 1581 de 2012 (Congreso de la República, 2012) exige a las organizaciones notificar a los titulares cuando sus datos personales hayan sido comprometidos.

Paso 3 — Recuperación (hora 2 a hora 24)

El administrador verifica que la versión de la base de datos en la plataforma centralizada esté íntegra y no haya sido modificada. Dado que los controles RBAC ya estaban implementados, se confirma que solo Andrés tuvo acceso al archivo en las últimas 48 horas, lo cual delimita con precisión el alcance de la fuga. No fue necesario restaurar desde backup porque la información no se perdió, solo se expuso; sin embargo, se registra el incidente en la bitácora de seguridad con fecha, hora, actor involucrado, activo comprometido y acción tomada. Este registro es el punto de partida para la última fase.

Paso 4 — Lecciones aprendidas (día siguiente)

Sandra convoca al equipo completo a una reunión de 20 minutos. Presenta el caso sin mencionar nombres ni buscar culpables: explica qué ocurrió, cómo se detectó y qué se hizo. La lección central que comunica es que la táctica del falso cliente es una forma conocida de ingeniería social, y que ningún cliente legítimo necesita la base de datos de otros clientes como referencia. Se establece como nueva regla operativa: cualquier solicitud inusual de información debe verificarse con la gerencia antes de responderse, sin excepciones. Esta regla se incorpora al código de conducta digital. Adicionalmente, se activa la restricción de descarga en todos los archivos de la plataforma centralizada: los empleados pueden visualizar y editar, pero no descargar ni reenviar archivos de clientes desde sus dispositivos personales.

Análisis del escenario: qué falló y qué funcionó

Este incidente demuestra algo que vale la pena subrayar: ningún sistema de seguridad elimina completamente el error humano. Andrés había recibido capacitación básica, conocía la política de protección de datos y aun así cayó en una táctica de ingeniería social. Eso es normal y esperable; por eso los controles deben construirse asumiendo que el error ocurrirá, no esperando que nunca pase. Lo que falló fue la ausencia de una restricción técnica de descarga sobre los archivos de clientes: si el archivo no se puede descargar ni reenviar desde la plataforma, el daño es imposible aunque el empleado quiera hacerlo. Lo que funcionó fue la política de reporte sin sanciones —que permitió contener el incidente en horas en lugar de días—, el control RBAC —que delimitó el alcance de la fuga— y la bitácora de auditoría —que permitió rastrear con exactitud quién accedió a qué

y cuándo. Este escenario confirma que los controles propuestos en este informe no son teóricos: son las herramientas que determinan la diferencia entre un incidente contenido en horas y una crisis que destruye la confianza de los clientes en semanas.

Cultura Organizacional

El análisis de la cultura organizacional en materia de seguridad de la información es un componente fundamental del informe técnico, ya que los comportamientos y prácticas del equipo humano determinan en gran medida la efectividad de cualquier control técnico implementado. Según el Anexo A de la norma ISO 27001 (2022), la concienciación y la formación del personal (control A.7) son pilares esenciales de un sistema de gestión de seguridad de la información.

Comportamientos y prácticas identificadas en DistriFresh S.A.S.:

- Uso generalizado de WhatsApp personal para compartir información sensible de clientes y pedidos, sin distinción entre canales personales y laborales.
- Ausencia de conciencia sobre la confidencialidad: los empleados comparten archivos con datos de clientes sin percibir que esto representa un riesgo legal y operativo.
- Falta de protocolos internos: no existen procedimientos documentados para el manejo de información, lo que genera prácticas informales e inconsistentes entre áreas.

- Resistencia implícita al cambio: al no existir políticas formales previas, los empleados han normalizado las prácticas inseguras como parte del flujo de trabajo habitual.

Influencia de la cultura en la seguridad e incidentes:

Los comportamientos descritos están directamente relacionados con los riesgos e incidentes potenciales identificados en este informe. La normalización del uso de WhatsApp sin control es el principal habilitador del riesgo R1 (fuga de datos de clientes). La falta de conciencia sobre los roles y accesos facilita el riesgo R2 (fraude interno). La ausencia de procedimientos documentados impide una respuesta organizada ante cualquier incidente, amplificando el impacto de los riesgos R3 y R4. En síntesis, la cultura organizacional actual de DistriFresh S.A.S. actúa como una vulnerabilidad transversal que potencia todos los riesgos identificados.

Evaluación de la cultura frente a las políticas propuestas:

Al comparar las prácticas actuales del equipo con las políticas de seguridad propuestas en este informe, se evidencia una brecha significativa entre el comportamiento observado y el comportamiento esperado. La Política 1 (Protección de Datos de Clientes) exige dejar de usar WhatsApp para compartir archivos sensibles, lo cual implica un cambio cultural importante. La Política 2 (Control de Acceso por Roles) requiere que los empleados acepten restricciones sobre la información a la que pueden acceder, algo que hasta ahora no ha sido necesario en la empresa. La Política 3 (Respaldo y Continuidad) demanda nuevos hábitos de almacenamiento en la nube. La Política 4 (Autenticación e

Identidad Corporativa) implica adoptar correos corporativos y verificar siempre la identidad antes de procesar pagos o compartir información. Esta evaluación confirma que la implementación técnica de los controles debe ir acompañada de un proceso de cambio cultural activo.

Propuesta de mejoras organizacionales:

- Desarrollar una jornada de sensibilización en ciberseguridad dirigida a todos los empleados, haciendo énfasis en el manejo de datos de clientes, el reconocimiento de fraudes y el uso adecuado de los canales de comunicación.

- Designar un responsable de seguridad de la información dentro del equipo (puede ser el administrador o un líder de área) que actúe como punto de contacto para dudas, reportes y actualizaciones de políticas.

- Establecer un código de conducta digital que defina claramente qué información puede compartirse, por qué canales y bajo qué condiciones, alineado con la Ley 1581 de 2012 y las políticas internas propuestas.

- Realizar revisiones periódicas (trimestrales) del cumplimiento de las políticas por parte del equipo, con el fin de reforzar los cambios de comportamiento y ajustar las medidas según la evolución de la empresa.

- Fomentar una cultura de reporte sin sanciones, donde los empleados se sientan seguros al informar errores o situaciones sospechosas sin temor a represalias, lo que permite detectar incidentes de forma temprana.

Estrategias de cambio cultural: por qué no basta con entrenar una vez

El mayor error que cometen las organizaciones pequeñas al intentar mejorar su seguridad es creer que con una charla de sensibilización el problema queda resuelto. La experiencia en gestión del cambio organizacional demuestra lo contrario: los hábitos arraigados, como compartir archivos por WhatsApp o usar cuentas personales para comunicaciones laborales, no se modifican con una sola intervención. Se necesita una estrategia sostenida que opere en tres niveles simultáneos: el nivel del individuo, el del equipo y el de la estructura organizacional.

Nivel 1 — El individuo: hacer que la seguridad sea fácil de cumplir

Las personas no incumplen las políticas de seguridad porque sean negligentes; las incumplen porque el comportamiento inseguro es más rápido y cómodo que el seguro. Si enviar un archivo por WhatsApp tarda 5 segundos y hacerlo por la plataforma centralizada tarda 2 minutos, la mayoría elegirá WhatsApp. La solución no es prohibir más fuertemente, sino hacer que el canal seguro sea el más conveniente. Esto implica que el administrador debe configurar accesos directos en los equipos y teléfonos del equipo hacia la carpeta compartida, y que la primera experiencia con la nueva herramienta debe ser acompañada, no solo anunciada. Cada empleado necesita que alguien le muestre, con su propio dispositivo y en su propio flujo de trabajo, cómo hacer lo que habitualmente hace pero de forma segura.

Nivel 2 — El equipo: crear normas grupales alrededor de la seguridad

La norma social es más poderosa que cualquier política escrita. Cuando un empleado envía un archivo sensible por WhatsApp y sus compañeros lo reciben sin

cuestionarlo, ese comportamiento se refuerza como aceptable. La estrategia de cambio a nivel de equipo consiste en crear momentos de visibilidad colectiva: en la reunión semanal del equipo, el responsable de seguridad dedica cinco minutos a mencionar un caso real de incidente en otra empresa, o a comentar cómo va el uso de la plataforma centralizada. Esto no es para hacer seguimiento punitivo, sino para mantener el tema en la conversación del equipo. Cuando la seguridad deja de ser un tema exclusivo del área de tecnología y se convierte en parte de la rutina del equipo, los cambios de comportamiento se sostienen en el tiempo.

Nivel 3 — La estructura: institucionalizar la seguridad como parte del negocio

El cambio cultural se consolida cuando deja de depender de la voluntad individual y pasa a estar integrado en los procesos de la organización. Para DistriFresh S.A.S., esto significa tres cosas concretas: primero, que el proceso de vinculación de nuevos empleados incluya desde el primer día una induccción sobre las políticas de seguridad y el código de conducta digital; segundo, que la evaluación de desempeño anual (o semestral) incluya un componente de cumplimiento de buenas prácticas de seguridad, lo que envía una señal clara de que esto es parte del trabajo, no un extra; y tercero, que cada vez que se detecte un incidente —por menor que sea— se documente, se analice y se comunique al equipo la lección aprendida, sin buscar culpables sino entendiendo qué falló en el proceso. Una organización que aprende de sus errores en seguridad es una organización que mejora continuamente su postura frente al riesgo.

En definitiva, el cambio cultural no es un proyecto con fecha de cierre; es un proceso continuo. Para DistriFresh S.A.S., el punto de partida es hacer que la seguridad sea

visible, fácil y compartida. Con una empresa de 15 personas, las condiciones están dadas para lograrlo: los canales de comunicación son directos, las decisiones se toman rápido y el impacto de una práctica nueva se puede sentir en toda la organización en cuestión de semanas. Lo que hace falta es voluntad gerencial y consistencia en el seguimiento.

Conclusiones

- El análisis realizado evidencia que DistriFresh S.A.S. presenta una exposición significativa al riesgo en materia de seguridad de la información, principalmente porque no existen controles formales sobre cómo se accede, maneja y comparte la información dentro de la empresa. Los activos más críticos identificados son la base de datos de clientes y la información financiera, cuya exposición puede generar impactos económicos y legales significativos.

- Se identificaron cuatro amenazas principales —fuga de datos, fraude interno, pérdida de información y suplantación de identidad—, todas de criticidad alta, directamente relacionadas con vulnerabilidades concretas y verificables en la operación actual de la empresa.

- La aplicación de la matriz de riesgos (probabilidad × impacto) permitió cuantificar la exposición de la organización y priorizar la implementación de controles. Tres de los cuatro riesgos identificados alcanzaron un nivel crítico, lo que subraya la urgencia de actuar.

- Los controles propuestos, alineados con el Anexo A de ISO 27001 y las funciones del marco NIST, son viables para una empresa del tamaño de DistriFresh S.A.S. y pueden implementarse con recursos tecnológicos disponibles en la nube a bajo costo. La gestión progresiva de estos controles permite completar el ciclo: identificar → evaluar → proponer.

- La Ley 1581 de 2012 (Congreso de la República, 2012) impone obligaciones legales que DistriFresh S.A.S. no puede postergar. El

incumplimiento en la protección de datos personales puede derivar en sanciones administrativas y económicas que afecten la sostenibilidad del negocio.

- La implementación de buenas prácticas basadas en ISO 27001 y el marco NIST, incluso en sus versiones más básicas, permitiría a la empresa mejorar progresivamente su nivel de seguridad, construir confianza con sus clientes y proveedores, y reducir considerablemente la probabilidad de incidentes que comprometan su continuidad operativa.

Referencias

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.

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

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (NIST Cybersecurity Framework v1.1).* NIST. https://doi.org/10.6028/NIST.CSWP.04162018

Ramírez Restrepo, J. L. (2026). *Seminario de Ciberseguridad Organizacional* [Material de clase]. Corporación Universitaria Remington.