

**Diseño de un Sistema de Gestión de Seguridad de la Información para el Área Comercial
de Bioconcentrados S.A.S. Bajo la Norma NTC-ISO/IEC 27001:2022 y el Marco MSPI de
MinTIC**

Sergio Andres Niño Barón

Universidad Piloto de Colombia

Facultad de Ingeniería

Especialización en Seguridad Informática

Bogotá

2026

Nota de Aceptación

Jurado

Jurado

Dedicatoria

En primer lugar gracias a Dios por concederme la sabiduría, la salud y la fortaleza necesarias para culminar con éxito esta etapa académica y profesional y a mis hijas, por ser mi motor inagotable y el cimiento de cada uno de mis sueños.

Agradecimientos

A la empresa Bioconcentrados S.A.S., por brindarme el espacio, la apertura y la información requerida para el desarrollo de esta propuesta de diseño en su área comercial.

Resumen

El presente proyecto plantea la propuesta de diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área comercial de la empresa Bioconcentrados S.A.S., tomando como marco normativo la NTC-ISO/IEC 27001:2022 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. El trabajo aborda la necesidad de proteger la información estratégica comercial frente a riesgos informáticos en entornos de trabajo móviles y soluciones SaaS.

La metodología, de alcance descriptivo-analítico, se desarrolló en cuatro fases: diagnóstico inicial e inventario de activos críticos; ponderación del riesgo inherente sobre escenarios representativos; diseño del Plan de Tratamiento del Riesgo (PTR) aplicando el algoritmo de atenuación del marco MSPI; y formulación de la Declaración de Aplicabilidad (SoA).

Como resultados principales, se caracterizaron los activos del proceso y se evaluó el impacto de amenazas críticas. La estimación del riesgo residual demostró cuantitativamente la efectividad de los controles en la atenuación de vulnerabilidades clave. Por su parte, la matriz SoA determinó un 79.6% de aplicabilidad (74 controles incluidos) para blindar la operación comercial y garantizar el cumplimiento de la Ley 1581 de 2012 (Hábeas Data), fundamentando técnicamente la exclusión del 20.4% (19 controles) por no corresponder a la realidad operativa del área.

Se concluye que el diseño propuesto entrega una arquitectura metodológica sólida y estandarizada que sirve de guía estructural para que la empresa ejecute la posterior fase de implementación real sobre la totalidad de los activos comerciales.

Palabras clave: SGSI, NTC-ISO/IEC 27001:2022, MSPI MinTIC, Gestión de Riesgos, Declaración de Aplicabilidad (SoA), Área Comercial.

Abstract

This project presents the design proposal for an Information Security Management System (ISMS) tailored for the commercial department at Bioconcentrados S.A.S., based on the NTC-ISO/IEC 27001:2022 standard and the Information Security and Privacy Model (MSPI - MinTIC) guidelines. The research addresses the need to protect strategic commercial data from information security risks within mobile workforce environments and SaaS architectures.

The methodology followed a descriptive-analytical approach structured in four phases: initial diagnosis and critical asset inventory; inherent risk assessment on representative scenarios; design of the Risk Treatment Plan (RTP) utilizing the MSPI attenuation algorithm; and formulation of the Statement of Applicability (SoA).

Key results include the characterization of process assets and the evaluation of critical threat impacts. Residual risk estimation quantitatively demonstrated control effectiveness in mitigating key vulnerabilities. Furthermore, the SoA matrix determined a 79.6% applicability rate (74 controls included) to safeguard commercial operations and ensure compliance with Law 1581 of 2012 (Data Protection), while providing technical justification for the exclusion of 20.4% (19 controls) outside the department's operational scope.

The study concludes that the proposed design provides a robust and standardized methodological framework, serving as a structural guide for the company to execute the subsequent physical implementation across all commercial assets.

Keywords: ISMS, NTC-ISO/IEC 27001:2022, MSPI MinTIC, Risk Management, Statement of Applicability (SoA), Commercial Process.

Tabla de Contenido

1	Introducción	13
2	Justificación	15
3	Problema de Investigación.....	17
3.1	Planteamiento del problema	17
3.2	Formulación del problema.....	18
4	Objetivos.....	19
4.1	Objetivo general.....	19
4.2	Objetivos específicos	19
5	Marco Teórico	20
5.1	La Información y su protección en el entornos empresariales	20
5.1.1	Concepto y Estructura de los Sistemas de Gestión de Seguridad de la Información .	21
5.2	Esquema operativo de la norma técnica colombiana ntc-iso/iec 27001:2022.....	21
5.3	Metodología de gestión de riesgos según ISO/IEC 27005:2022	22
5.4	Levantamiento, clasificación y ciclo de vida de los activos.....	23
5.5	Marco conceptual de la norma NTC-ISO 31000:2018.....	23
5.5.1	Identificación de Fuentes y Escenarios de Riesgo.....	23
5.6	Clasificación de amenazas y riesgos tecnológicos	24
5.7	Estructuración de la declaración de aplicabilidad	24
5.8	Formulación y niveles de las políticas de seguridad	25
5.9	Directrices específicas para el despliegue de controles.....	26
5.10	Plan de sensibilización, formación y cultura de seguridad.....	26
5.10.1	Proceso de Sensibilización y Gestión del Cambio.....	27

5.11	Marco Referencial	28
5.11.1	Bioconcentrados S.A.S	28
5.11.2	Direccionamiento Estratégico	28
5.11.3	Estructura Organizacional y Gestión Tecnológica	28
5.11.4	Mapa de Procesos y Relevancia del Área Comercial	29
5.11.5	Panorama Actual, Problemática y Justificación del Proyecto	30
6	Diseño Metodológico.....	33
6.1	Hipótesis	33
6.2	Sistema de variables	34
6.2.1	Variable Independiente.....	34
6.2.2	Variables Dependientes	34
6.2.3	Justificación Metodológica del Muestreo de Activos y Riesgos.....	34
6.3	Delimitación del Diagnóstico	35
6.4	Metodología y técnicas de recolección de la información	35
6.5	Instrumento de diagnóstico y escala oficial de valoración línea base (MINTIC - NTC-ISO/IEC 27001:2022)	36
6.5.1	Escala de Valoración de Madurez de Controles	36
6.5.2	Criterios de Consolidación y Ponderación del Instrumento MinTIC	37
6.6	Identificación y clasificación de activos de la información	39
6.6.1	Valoración de los activos de información	42
6.6.2	Identificación de amenazas ((NTC-ISO/IEC 27005:2022).....	44
6.7	Estructura y valoración de riesgos inherentes (NTC-ISO 31000:2018).....	46
6.7.1	Valoración y Algoritmo de Cálculo del Riesgo.....	47

6.8	Matriz de evaluación del riesgo inherente	49
6.9	Estrategia de tratamiento de riesgos	50
6.9.1	Tiempos Propuestos para la Ejecución del Tratamiento de Riesgos	51
6.9.2	Metodología de asignación de controles y estimación de efectividad.....	52
6.9.3	Aplicación y efectividad de los controles y cálculo del riesgo residual	54
6.9.4	Operaciones Matemáticas para el Cálculo del Riesgo Residual (RR).....	55
6.10	Justificación y Marco Metodológico del SoA en la Fase de Diseño	57
6.11	Criterios de Clasificación para Inclusión y Exclusión.....	58
6.12	Resumen de Aplicabilidad por Dominios.....	59
6.13	Matriz Detallada de la Declaración de Aplicabilidad (93 Controles - Anexo A).....	60
6.14	Vinculación Estratégica para la Futura Fase de Implementación.....	64
7	Conclusiones	65
8	Recomendaciones	66
9	Referencias Bibliográficas.....	67
10	Anexos	71

Lista de tablas

Tabla 1 Evaluación de Efectividad de controles	38
Tabla 2 Levantamiento de activos de información	40
Tabla 3 Clasificación por Confidencialidad (Ley 1712 / Ley 1581)	43
Tabla 4 Clasificación por Integridad.....	43
Tabla 5 Clasificación por Disponibilidad	44
Tabla 6 Valoración de Activos.....	44
Tabla 7 Amenazas	45
Tabla 8 Escala de Probabilidad de Ocurrencia	47
Tabla 9 Escala de Impacto Organizacional.....	47
Tabla 10 Matriz 3 X 3 de Calificación y Posicionamiento del Riesgo Inherente	48
Tabla 11 Criterios de Aceptación y Zonas de Tratamiento del Riesgo (RI).....	49
Tabla 12 Matriz General de Evaluación del Riesgo Inherente	49
Tabla 13 Cuadrante Resultante y Mapa de Calor del Riesgo Inherente	50
Tabla 14 Cronograma y Cronología para el Tratamiento de Riesgos Comercial	51
Tabla 15 Controles del Anexo A, Estrategia Sugerida y Porcentaje de Efectividad Esperado para los Activos de Información.....	53
Tabla 16 Ponderación Oficial de Atributos de Control.....	54
Tabla 17 Matriz General de Evaluación del Riesgo Residual	56
Tabla 18 Cuadrante de Ubicación del Riesgo Residual Resultante	57
Tabla 19 Resumen Consolidado de la Declaración de Aplicabilidad (SoA).	59
Tabla 20 Matriz Maestra de la Declaración de Aplicabilidad (SoA - ISO 27001:2022 / MSPI). 60	

Lista de figuras

Figura 1 Organigrama Institucional	29
Figura 2 Mapa de procesos	30
Figura 3 Resultado visual Brecha Resultados del Anexo A	39

Lista de Anexos

Anexo A Evaluación del nivel de cumplimiento	71
Anexo B Escala de Valoración de Controles ISO 27001:2022	81

1 Introducción

En la actualidad, la transformación digital de las organizaciones y el crecimiento exponencial de las amenazas cibernéticas han transformado radicalmente el panorama operativo global (Paez et al., 2022). Los incidentes informáticos no solo han aumentado en volumen, sino también en nivel de sofisticación, lo que expone a múltiples sectores productivos a pérdidas financieras multimillonarias y a severos daños reputacionales derivados de la interrupción del negocio o la fuga de datos estratégicos (Allianz, 2026). Ante esta realidad, la implementación de estrategias rigurosas de protección de la información ha dejado de ser una opción operativa para convertirse en un pilar esencial de la continuidad del negocio y de la gobernanza corporativa (Galarza et al., 2025).

En el contexto nacional, Bioconcentrados SAS se consolida como una organización clave en el sector agroindustrial colombiano. No obstante, dentro de su estructura funcional, el área comercial gestiona un volumen considerable de activos de información altamente sensibles, tales como listas de precios, bases de datos de clientes, contratos estratégicos, acuerdos de distribución y proyecciones de ventas. La movilidad constante de la fuerza de ventas en campo, sumada al uso recurrente de herramientas colaborativas en la nube y dispositivos corporativos y personales, incrementa la exposición frente a vectores de ataque como la ingeniería social, la interceptación de comunicaciones y el compromiso de credenciales. Una eventual vulneración en esta dependencia afectaría la confidencialidad de la información y la posición competitiva de la firma en el mercado (Fierro, 2026).

Frente a este escenario, surge la necesidad de diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) acotado al área comercial de Bioconcentrados SAS. Este marco debe permitir identificar de manera oportuna las vulnerabilidades inherentes a los procesos

comerciales, evaluar los riesgos asociados y establecer controles proporcionales a las necesidades operativas de la empresa. Para lograrlo, se toma como referente metodológico y normativo la NTC-ISO/IEC 27001:2022, estándar internacional estructurado bajo el ciclo de mejora continua (ciclo de Planificar, Hacer, Verificar y Actuar), el cual incorpora actualizaciones clave para abordar entornos digitales cambiantes y dinámicas de trabajo híbrido (ICONTEC, 2022).

El desarrollo de la presente propuesta busca entregar a Bioconcentrados SAS una arquitectura de seguridad práctica y ajustada a su realidad comercial. A través del análisis de brechas, la valoración de activos y el diseño de la Declaración de Aplicabilidad (SoA), el trabajo propone un conjunto de controles organizacionales, tecnológicos y operacionales orientados a fortalecer la postura de seguridad de la dependencia comercial, asegurando la confidencialidad, integridad y disponibilidad de la información crítica para el cumplimiento de los objetivos estratégicos de la compañía.

2 Justificación

En el entorno empresarial contemporáneo, el área comercial actúa como el motor de crecimiento organizacional y, de manera simultánea, como uno de los sectores más expuestos ante incidentes de ciberseguridad y ataques informáticos (Paez et al., 2022). Dinámicas como la suplantación de identidad, la interceptación de comunicaciones y el compromiso de cuentas corporativas representan amenazas constantes que buscan vulnerar la confidencialidad de la información estratégica o alterar datos críticos para la operación. En Bioconcentrados SAS, el equipo comercial gestiona diariamente activos de elevado valor estratégico como listas de precios, bases de datos de clientes, acuerdos de distribución, contratos y proyecciones de ventas a través de plataformas digitales, herramientas colaborativas y trabajo de campo, lo que exige contar con mecanismos de protección y controles de acceso sólidos.

A pesar de que la compañía dispone de ciertos esquemas y herramientas de seguridad tecnológica en su infraestructura, la ausencia de una arquitectura documental estructurada y de un marco formal de gobernanza de la información en el área comercial genera brechas operativas significativas. Actualmente no se dispone de políticas formales para la realización de respaldos sistemáticos de información en equipos móviles, protocolos claros para la transmisión segura de datos con clientes y aliados, ni programas continuos de concientización y cultura en seguridad dirigidos al personal comercial. Esta falta de controles procedimentales y organizacionales limita la capacidad de respuesta de la empresa ante posibles incidentes, exponiéndola a pérdidas económicas, sanciones legales y afectaciones reputacionales (Garavito et al., 2025).

Frente a esta realidad, el desarrollo de una propuesta de diseño para un Sistema de Gestión de Seguridad de la Información (SGSI) enfocado exclusivamente en el área comercial de Bioconcentrados SAS resulta ampliamente oportuno y conveniente. La adopción de la norma

NTC-ISO/IEC 27001 en su versión 2022 proporciona un marco de referencia internacionalmente reconocido, actualizado para hacer frente a las amenazas en entornos digitales y esquemas de trabajo híbridos. Al abordar esta problemática mediante una investigación aplicada con un diseño descriptivo, es posible caracterizar minuciosamente el estado actual de la dependencia, formalizar el inventario de sus activos de información, identificar sus vulnerabilidades clave y estructurar un conjunto de controles adaptados a su realidad operativa.

Desde la perspectiva académica e investigativa, el presente proyecto aporta un modelo metodológico de referencia para la aplicación integrada de la norma internacional NTC-ISO/IEC 27001:2022 y el marco normativo colombiano MSPI del MinTIC en Pymes del sector agroindustrial. Al articular el algoritmo cuantitativo de atenuación de riesgos de MinTIC sobre entornos de trabajo móviles y soluciones SaaS, la investigación enriquece el cuerpo de conocimiento sobre ciberseguridad aplicada, sirviendo como maqueta estandarizada para futuros estudios e intervenciones en procesos comerciales descentralizados.

Finalmente, este trabajo genera un impacto directo y positivo para Bioconcentrados SAS al sentar las bases normativas y procedimentales que garantizan los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. El diseño propuesto no solo protegerá la ventaja competitiva de la empresa y facilitará el cumplimiento del marco legal de protección de datos personales en el país, sino que transmitirá una imagen de confianza, madurez corporativa y responsabilidad operativa ante clientes, proveedores y socios de negocio.

3 Problema de Investigación

3.1 Planteamiento del problema

Bioconcentrados SAS es una empresa agroindustrial dedicada a la producción y comercialización de alimento balanceado para animales de granja, cuya operación abarca la venta a distribuidores y productores en zonas rurales. Dentro del departamento comercial se manejan activos de alto valor estratégico, como bases de datos de clientes, tarifas, registros de pedidos, acuerdos de crédito y rutas de despacho. Sin embargo, debido a la baja adopción tecnológica del cliente rural, la gestión de pedidos se realiza principalmente mediante llamadas telefónicas, mensajería instantánea y toma de datos en campo. Esta informalidad operativa genera vulnerabilidades críticas frente a la suplantación de identidad, la interceptación de solicitudes de crédito, la fuga de información comercial y la pérdida de datos en dispositivos móviles corporativos (Robles, 2025).

A pesar de contar con una infraestructura informática básica para soportar la facturación, el área comercial adolece de una estructura formal de gobernanza de la información. Actualmente no se dispone de un inventario valorado de activos informáticos y documentales, ni de políticas estandarizadas para la recepción segura de pedidos o el uso de equipos fuera de la oficina por parte de los asesores en ruta. La ausencia de estos controles procedimentales expone a Bioconcentrados SAS a fraudes comerciales, filtración de listados de precios hacia la competencia, interrupción del servicio y eventuales sanciones legales por el inadecuado tratamiento de datos personales de sus clientes (Rodríguez, 2024).

Para resolver esta problemática, se propone elaborar el diseño de un SGSI exclusivo para el área comercial de Bioconcentrados SAS, fundamentado en los requisitos de la norma NTC-ISO/IEC 27001:2022. Esta solución documental y metodológica permitirá evaluar el estado

actual de los canales de venta, inventariar los activos informáticos, analizar los riesgos inherentes al entorno rural y seleccionar los controles procedimentales y tecnológicos del Anexo A. De esta forma, el proyecto proporcionará la arquitectura organizativa requerida para resguardar la operación comercial, sirviendo como insumo técnico previo a cualquier etapa futura de implementación.

3.2 Formulación del problema

¿Cómo estructurar la propuesta de un diseño de un Sistema de Gestión de Seguridad de la Información alineado con la norma NTC-ISO/IEC 27001:2022 y los lineamientos del MSPI del MinTIC para identificación y tratamiento de los riesgos de seguridad de la información en el área comercial de Bioconcentrados SAS?

4 Objetivos

4.1 Objetivo general

Diseñar de Sistema de Gestión de Seguridad de la Información (SGSI) para el área comercial de la empresa Bioconcentrados SAS, fundamentado en la norma NTC-ISO/IEC 27001:2022, mediante la formulación de una arquitectura de controles y un esquema de tratamiento de riesgos que sirva de guía para preservar la confidencialidad, integridad y disponibilidad de la información comercial

4.2 Objetivos específicos

- Analizar el estado actual de la seguridad de la información en el área comercial de Bioconcentrados S.A.S. para estructurar el inventario y la valoración de los activos de información del proceso.
- Ponderar los eventos de riesgo de seguridad de la información que impactan los activos del proceso comercial, mediante el modelado de la probabilidad e impacto bajo los lineamientos de la norma NTC-ISO/IEC 27001:2022.
- Diseñar la propuesta del Plan de Tratamiento del Riesgo (PTR) mediante la estimación del riesgo residual bajo los criterios de efectividad del algoritmo del marco MSPI (MinTIC).
- Formular la propuesta de la Declaración de Aplicabilidad (SoA) sobre los 93 controles del Anexo A de la NTC-ISO/IEC 27001:2022, estableciendo la matriz de inclusión y exclusión que fundamenta la arquitectura final del SGSI.

5 Marco Teórico

5.1 La Información y su protección en el entornos empresariales

La información representa el recurso neurálgico sobre el cual se articulan las transacciones y la toma de decisiones en el sector corporativo actual, lo que demanda salvaguardarla como un activo de indiscutible valor crítico (Kiteworks, 2024). El uso extensivo de soluciones tecnológicas dentro de la operación diaria ha dinamizado los negocios; no obstante, esta transformación digital impone el establecimiento de esquemas rigurosos para la preservación de los datos en sus diversos soportes (Marreros et al., 2024).

El aseguramiento de los activos informacionales se gestiona a través de tres propiedades esenciales:

- **Confidencialidad:** Restricción del acceso a los datos, permitiendo su consulta de manera exclusiva a personal, roles o aplicaciones expresamente autorizados.
- **Integridad:** Protección de la exactitud y totalidad de la información, previniendo alteraciones, borrados o manipulaciones no autorizadas.
- **Disponibilidad:** Garantía de acceso continuo e ininterrumpido a los recursos informáticos por parte de los usuarios legitimados cuando la labor operativa lo requiera (Herrera, 2025).

Con el objetivo de operativizar estas dimensiones, entidades internacionales han desarrollado marcos de referencia como la serie de normas ISO/IEC 27000 y el Cybersecurity Framework de NIST (National Institute of Standards and Technology, 2024). En Colombia, el Instituto Colombiano de Normas Técnicas y Certificación adopta estos estándares internacionales, facilitando que las organizaciones demuestren madurez institucional, resguarden su reputación y aseguren la información propia y la custodiada de terceros.

5.1.1 Concepto y Estructura de los Sistemas de Gestión de Seguridad de la Información

Un SGSI se define como el marco organizativo y directivo enfocado en administrar los riesgos informáticos globales del negocio, cuyo fin es diseñar, desplegar, supervisar, mantener y optimizar de forma continua la protección de los datos (Centro de Investigación y Estudios Estratégicos, 2024).

En concordancia con los postulados de la norma NTC-ISO/IEC 27000, un SGSI integra de forma sistémica políticas, lineamientos, procesos operacionales, asignación de recursos y actividades de control. Este enfoque metodológico permite tratar la exposición al riesgo en función de los niveles de tolerancia institucional definidos por la dirección (Cortés y Pulido, 2023).

Para el diseño efectivo de un SGSI bajo la NTC-ISO/IEC 27001:2022, la organización debe fundamentarse en los siguientes principios:

- Fomento de una cultura corporativa consciente de las vulnerabilidades y amenazas digitales.
- Asignación explícita de responsabilidades y autoridad en el manejo de la ciberseguridad.
- Respaldo manifiesto de la alta gerencia con el cumplimiento de las metas de seguridad.
- Valoración y gestión sistemática de los riesgos inherentes a los procesos.
- Adopción de una perspectiva integral que combine dimensiones humanas, procedimentales y tecnológicas (López y Martínez, 2021).

5.2 Esquema operativo de la norma técnica colombiana ntc-iso/iec 27001:2022

La NTC-ISO/IEC 27001:2022 es la norma técnica estándar orientada a especificar los requisitos verificables para el establecimiento, implementación y optimización continua de un SGSI (ICONTEC, 2022). El estándar exige la adopción de procesos formalizados de seguridad,

la definición de roles operativos y el involucramiento de la alta gerencia mediante políticas y directrices organizacionales.

El cuerpo normativo de la NTC-ISO/IEC 27001:2022 articula los siguientes requisitos de cumplimiento obligatorio⁷:

- **Contexto de la organización (Numeral 4):** Diagnóstico del entorno corporativo, determinación de las expectativas de las partes interesadas y fijación de los límites del SGSI.
- **Liderazgo (Numeral 5):** Compromiso de la alta dirección, emisión de la política general de seguridad y delegación de responsabilidades.
- **Planificación (Numeral 6):** Mecanismos para la identificación de riesgos y oportunidades, trazabilidad de objetivos y gestión de cambios del sistema.
- **Soporte (Numeral 7):** Asignación de recursos presupuestales, verificación de competencias del personal, programas de toma de conciencia y control documental.
- **Operación (Numeral 8):** Ejecución de la planificación operacional, valoración periódica de riesgos y despliegue del plan de tratamiento.
- **Evaluación del desempeño (Numeral 9):** Seguimiento mediante indicadores de gestión, desarrollo de auditorías internas y revisión por la dirección.
- **Mejora (Numeral 10):** Tratamiento de no conformidades, análisis de causa raíz e implementación de acciones correctivas (ICONTEC, 2022).

5.3 Metodología de gestión de riesgos según ISO/IEC 27005:2022

La norma internacional ISO/IEC 27005:2022 ofrece las pautas metodológicas específicas para la administración de riesgos en seguridad de la información dentro del marco de un SGSI.

Este referente detalla los procedimientos para la identificación de amenazas, el análisis de

vulnerabilidades tecnológicas o procedimentales y la estimación del impacto operacional ante eventuales incidentes (ICONTEC, 2022).

5.4 Levantamiento, clasificación y ciclo de vida de los activos

Un activo de información corresponde a cualquier componente lógico, físico, humano o documental que posee valor explícito para la organización y que, en consecuencia, requiere salvaguardas de protección (Procuraduría General de la Nación, 2025).

Bajo la NTC-ISO/IEC 27001:2022, las empresas deben inventariar sus activos analizando su ciclo de vida: creación, procesamiento, almacenamiento, transmisión y destrucción final. El inventario debe incluir los siguientes campos mínimos:

- **Nombre del activo:** Identificador único y preciso del recurso.
- **Descripción:** Detalle de su función dentro del flujo de trabajo.
- **Clasificación:** Nivel de confidencialidad o criticidad (público, interno, restringido).
- **Valoración:** Estimación cualitativa o cuantitativa de su importancia para el negocio (ICONTEC, 2022).

5.5 Marco conceptual de la norma NTC-ISO 31000:2018

La NTC-ISO 31000:2018 establece los principios genéricos para la estructuración de la gestión de riesgos en cualquier arquitectura corporativa, sin importar su tamaño o actividad económica (ICONTEC, 2018). Esta norma proporciona un lenguaje unificado para alinear las actividades de control dentro del gobierno corporativo.

5.5.1 Identificación de Fuentes y Escenarios de Riesgo

Esta fase tiene como propósito reconocer los eventos, causas de origen y escenarios de falla que amenazan el cumplimiento de los objetivos institucionales. Su resultado formal debe ser un registro consolidado de riesgos por proceso (Valencia, 2021).

5.6 Clasificación de amenazas y riesgos tecnológicos

Los riesgos tecnológicos representan eventos capaces de degradar o interrumpir el funcionamiento de los sistemas informáticos. Se clasifican en las siguientes categorías:

- **Riesgos de integridad:** Posibilidad de modificación, falsificación o corrupción indebida de los datos.
- **Riesgos de relación:** Exposición derivada del intercambio de archivos con clientes, proveedores o servicios externos.
- **Riesgos de acceso:** Vulnerabilidades asociadas a la autenticación deficiente o exceso de privilegios de usuario.
- **Riesgos de utilidad:** Pérdida de vigencia o validez operacional de los datos almacenados.
- **Riesgos de infraestructura:** Fallas en redes, equipos de cómputo, servidores o centros de datos (Ospina, 2026).

5.7 Estructuración de la declaración de aplicabilidad

La Declaración de Aplicabilidad es el instrumento normativo exigido por la NTC-ISO/IEC 27001:2022 en el cual la organización documenta formalmente la selección o exclusión de los 93 controles del Anexo A.

La selección de los controles dentro de la declaración de aplicabilidad debe sustentarse en criterios claros:

- Alineación con los marcos legales y reglamentarios vigentes.
- Objetivos de negocio de la organización.
- Factibilidad y restricciones técnicas u operacionales.
- Análisis costo-beneficio entre el valor del control y el daño evitado.

- Mecanismos para la evaluación continua de la efectividad de los controles (ICONTEC, 2022).

5.8 Formulación y niveles de las políticas de seguridad

Las Políticas de Seguridad y Privacidad de la Información corresponden al conjunto de orientaciones corporativas y reglas operativas de obligatorio cumplimiento dictadas por la dirección, cuya finalidad es mitigar la exposición al riesgo y establecer pautas claras para el uso de los activos de información (ICONTEC, 2018; Ospina, 2026). Dentro de la arquitectura del MSPI, la documentación normativa se articula en tres niveles jerárquicos de gestión:

- **Políticas de Primer Nivel (Estratégicas o Generales):** Documentos marco institucionales que expresan el compromiso formal de la alta gerencia con la ciberseguridad, delimitan los principios rectores del SGSI y aseguran el cumplimiento del marco normativo nacional (Alarcon y Tobón, 2021).
- **Políticas de Segundo Nivel (Tácticas o Específicas):** Directrices que reglamentan dominios tecnológicos o procesos concretos del negocio, tales como el control de acceso, la gestión de la identidad y la seguridad en dispositivos móviles (MinTIC, 2026).
- **Políticas de Tercer Nivel (Operativas u Operacionales):** Procedimientos, instructivos y guías paso a paso que norman la ejecución de las actividades técnicas y operativas cotidianas del personal.

En el contexto jurídico colombiano, la formulación de estas directrices debe integrarse armónicamente con las disposiciones del ordenamiento legal sobre Hábeas Data y tratamiento de datos personales, reguladas en la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012) y el Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013).

5.9 Directrices específicas para el despliegue de controles

En alineación con el catálogo de políticas de seguridad y privacidad del MSPI impulsado por el MinTIC, la organización debe estructurar un compendio de políticas tácticas y operativas enfocadas en materializar los controles del Anexo A de la norma NTC-ISO/IEC 27001:2022.

Este grupo de políticas abarca los siguientes dominios fundamentales (MinTIC, 2026):

- Privacidad y confidencialidad: Directrices para el tratamiento seguro de información sensible y custodia de bases de datos.
- Integridad de la información: Reglas para evitar la alteración no autorizada de registros comerciales y archivos corporativos.
- Disponibilidad y continuidad: Planes de contingencia tecnológica para garantizar la prestación ininterrumpida de servicios críticos.
- Gestión y control de activos: Normas para el inventariado, clasificación y uso aceptable de herramientas tecnológicas y datos.
- Control de accesos y autenticación: Políticas para la asignación de privilegios mínimos y contraseñas seguras.
- Gestión de incidentes: Procedimientos formales para el reporte, análisis y contención de eventos de seguridad.
- Seguridad en la gestión del talento humano: Mecanismos de selección, acuerdos de confidencialidad y formación continua en ciberseguridad (MinTIC, 2026).

5.10 Plan de sensibilización, formación y cultura de seguridad

Dado que el factor humano constituye el eslabón de mayor sensibilidad dentro de los flujos operacionales, el numeral 7.3 y el control A.6.3 de la norma NTC-ISO/IEC 27001:2022 exigen la puesta en marcha de un programa sistemático de toma de conciencia (ICONTEC, 2022;

Rodríguez y Ruiz, 2021). Para responder a este requisito, se adoptan los lineamientos de la Guía de Planeación de Estrategias de Sensibilización, Comunicación y Capacitación del MSPI, marco metodológico institucional diseñado por el Gobierno Digital para fortalecer la cultura de ciberseguridad en las organizaciones (MinTIC, 2026).

5.10.1 Proceso de Sensibilización y Gestión del Cambio

De acuerdo con el modelo metodológico del MinTIC (MinTIC, 2026), la sensibilización se concibe como una intervención pedagógica y comunicacional estructurada que busca transformar los hábitos y comportamientos del personal frente al uso de las tecnologías de la información. Su implementación comprende las siguientes fases de desarrollo (Rubio, 2025):

- **Diagnóstico de necesidades:** Evaluación del nivel de madurez y grado de conocimiento previo de los colaboradores respecto a las amenazas digitales.
- **Diseño de la estrategia comunicacional:** Elaboración de contenidos claros orientados a la prevención de riesgos cotidianos (como phishing, ingeniería social y manejo seguro de credenciales).
- **Ejecución y despliegue:** Desarrollo de capacitaciones, talleres prácticos, campañas informativas y ejercicios de simulación.
- **Evaluación de impacto:** Medición del cambio conductual en el equipo de trabajo y análisis de la efectividad del programa.

Asimismo, las reglas de conducta promovidas durante la sensibilización deben estar respaldadas por el reglamento interno y el marco sancionatorio de la empresa, asegurando que los usuarios conozcan las responsabilidades derivadas del incumplimiento de las políticas de seguridad.

5.11 Marco Referencial

5.11.1 *Bioconcentrados S.A.S*

Bioconcentrados S.A.S. es una empresa colombiana orientada al sector agropecuario, dedicada a la fabricación y comercialización de alimentos balanceados para animales, con sede administrativa y planta de producción ubicadas en el municipio de Girón, Santander. La compañía orienta su actividad al desarrollo de soluciones de nutrición animal integral, atendiendo a productores de los sectores avícola, porcino, ganado bovino, equino, cunícola y de mascotas a nivel regional (Bioconcentrados S.A.S., 2026).

5.11.2 *Direccionamiento Estratégico*

- **Misión:** Producir y comercializar alimentos balanceados para animales, asegurando productos conformes, trazables y técnicamente respaldados, que satisfagan las necesidades de nuestros clientes en los sectores avícola, ganadero, porcino, equino, cunícola y de mascotas.
- **Visión:** Para el año 2030, Bioconcentrados S.A.S. será reconocida como una empresa competitiva y confiable en el mercado regional de alimentos balanceados para animales, con capacidad para participar en segmentos de mayor tamaño y exigencia, donde compiten las principales empresas del sector. La organización se proyecta como una entidad sólida, orientada a la calidad, la trazabilidad, la oportunidad en el servicio, el respaldo técnico veterinario, la innovación en sus líneas de producto y la mejora continua del Sistema de Gestión de la Calidad.

5.11.3 *Estructura Organizacional y Gestión Tecnológica*

La estructura organizacional de Bioconcentrados S.A.S. responde a un modelo funcional en el que la toma de decisiones estratégicas se concentra en la Dirección General y las

direcciones de área. Dentro de esta arquitectura, el soporte operativo e informático recae exclusivamente en la figura del Líder de Sistemas como lo muestra la figura 1.

Figura 1
Organigrama Institucional



Fuente: Bioconcentrados S.A.S. (2026).

Esta concentración de responsabilidades en un solo rol evidencia una centralización crítica de la gestión tecnológica, donde la administración de la red, el soporte informático a usuarios, la custodia de copias de seguridad y la seguridad de la información dependen de una sola persona, generando un cuello de botella operacional y una elevada vulnerabilidad ante eventuales incidentes informáticos.

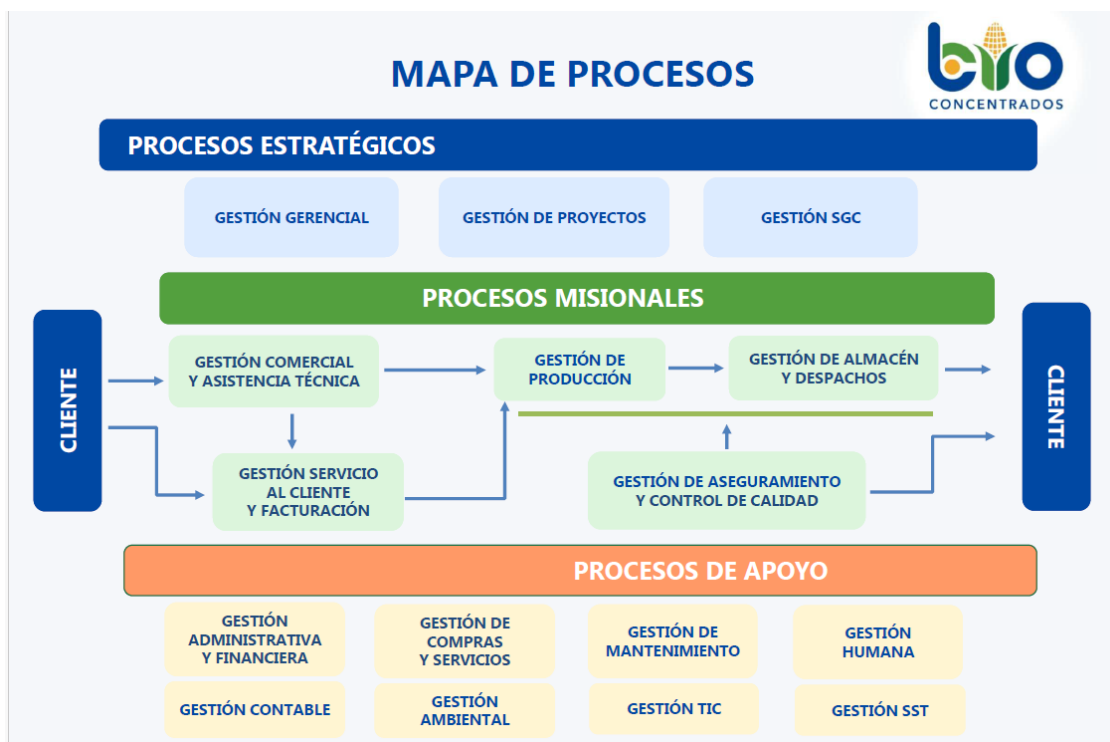
5.11.4 Mapa de Procesos y Relevancia del Área Comercial

El mapa de procesos de Bioconcentrados S.A.S, figura 2, articula los procesos estratégicos, misionales y de apoyo. Dentro de esta cadena de valor, la Gestión Comercial se posiciona como un proceso misional crítico, siendo el motor de ingresos de la compañía al

gestionar la venta, la toma de pedidos, la atención al cliente, la gestión de crédito y cartera, y la coordinación logístico-comercial para la distribución de alimentos balanceados.

Figura 2

Mapa de procesos



Fuente: Bioconcentrados S.A.S. (2026).

5.11.5 Panorama Actual, Problemática y Justificación del Proyecto

En el marco de la expansión operativa de Bioconcentrados S.A.S., el área comercial opera bajo una modalidad híbrida que combina el trabajo en sede administrativa (Girón, Santander) con desplazamientos continuos de asesores comerciales hacia zonas rurales y fincas agropecuarias de la región. En esta interacción operativa se gestionan de manera constante activos de información altamente sensibles:

- **Datos de Clientes y Cartera:** Pagars físicos, acuerdos de crédito, historiales de pago y datos personales de pequeños y medianos productores (sujetos a la Ley 1581 de 2012).

- **Herramientas de Venta y Movilidad:** Equipos portátiles, dispositivos móviles corporativos y aplicaciones de mensajería (WhatsApp Business) utilizados en campo sin políticas formales de cifrado o conexión segura.
- **Sistemas de Información:** Acceso remoto o local al sistema ERP para facturación y consulta de inventarios de producción.

A pesar de la importancia estratégica del área comercial, la empresa enfrenta un panorama de vulnerabilidad informática caracterizado por:

- **Ausencia de Controles Formales de Seguridad:** Inexistencia de políticas, procedimientos o normativas escritas de seguridad y privacidad de la información que regulen el manejo de datos en campo.
- **Exposición de Activos en Rutas Rurales:** Riesgo latente de hurto o pérdida de equipos portátiles que contienen información comercial confidencial y bases de datos de clientes.
- **Manejo Descentralizado e Informal de Comunicaciones:** Transferencia de listas de precios, descuentos y solicitudes de pedidos a través de canales no controlados (chats e imágenes), sin políticas de retención ni respaldo de la información.
- **Tratamiento de Datos Personales:** Riesgo de sanciones legales y regulatorias por la gestión de información de clientes y distribuidores sin los controles exigidos por la normativa de protección de datos.

El desarrollo de este proyecto responde a la necesidad urgente de estructurar una propuesta metodológica y técnica para el Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) guiado por los estándares internacionales NTC-ISO/IEC 27001:2022 y las directrices del MSPI del MinTIC.

- **Proteger los activos críticos:** Salguardar la integridad, confidencialidad y disponibilidad de la información comercial y de cartera.
- **Establecer una cultura organizacional de seguridad:** Dotar al personal comercial y al Líder de Sistemas de un marco claro de políticas, lineamientos y un plan de concientización.
- **Mitigar los riesgos del negocio:** Reducir la probabilidad e impacto de incidentes informáticos, pérdida de datos o sanciones regulatorias.
- **Fortalecer la competitividad:** Alinear la seguridad de la información con la Visión 2030, asegurando la confiabilidad, trazabilidad y continuidad de las operaciones comerciales de Bioconcentrados S.A.S.

6 Diseño Metodológico

El desarrollo metodológico de la investigación se enmarca en un estudio de tipo aplicado con alcance descriptivo y un enfoque mixto (cualitativo y cuantitativo) (Hernández y Mendoza, 2018). Este enfoque permite diagnosticar de manera integral la gestión de la información en el área comercial de Bioconcentrados SAS para fundamentar la propuesta de diseño del SGSI.

El componente cualitativo abarca la revisión de la documentación existente, la caracterización de los flujos de ventas y el análisis conceptual de los controles procedimentales. Por su parte, el componente cuantitativo se concreta en la medición porcentual del nivel de madurez o brecha (Gap Analysis) frente a las cláusulas de la norma NTC-ISO/IEC 27001:2022, así como en la estimación numérica de la probabilidad e impacto para la valoración del riesgo inherente bajo la norma NTC-ISO 31000:2018.

6.1 Hipótesis

- Hipótesis de Investigación (Hi): La formulación de un diseño de SGSI basado en la NTC-ISO/IEC 27001:2022 y el algoritmo de efectividad del MSPI (MinTIC) reduce de manera estadísticamente significativa la exposición al riesgo residual (RR) frente al riesgo inherente (RI) en los activos críticos del área comercial de Bioconcentrados S.A.S.
- Hipótesis Nula o de Negación (H0): La formulación de un diseño de SGSI basado en la NTC-ISO/IEC 27001:2022 y el algoritmo de efectividad del MSPI (MinTIC) no genera una reducción significativa en la exposición al riesgo residual (RR) respecto al riesgo inherente (RI) en los activos críticos del área comercial de Bioconcentrados S.A.S.

6.2 Sistema de variables

6.2.1 *Variable Independiente*

- Nivel de Madurez Operativo: Grado de formalización y cumplimiento actual de los procesos de venta, atención al cliente rural y administración de datos en el área comercial de Bioconcentrados SAS frente a las mejores prácticas de ciberseguridad.

6.2.2 *Variables Dependientes*

- Diseño del SGSI: estructura documental y metodológica fundamentada en los requisitos de la norma NTC-ISO/IEC 27001:2022.
- Riesgo en Seguridad de la Información: exposición a la pérdida de confidencialidad, integridad o disponibilidad de la información comercial rural, calculada mediante la combinación de probabilidad e impacto.
- Controles de Seguridad: conjunto de salvaguardas organizacionales, de personas, físicas y tecnológicas seleccionadas del Anexo B para la mitigación del riesgo.

6.2.3 *Justificación Metodológica del Muestreo de Activos y Riesgos*

El universo del área comercial de Bioconcentrados S.A.S. comprende un total de 21 activos de información y 37 escenarios de riesgo identificados en el inventario general. No obstante, al enmarcarse el presente trabajo en un alcance de propuesta de diseño y guía metodológica, se seleccionó de manera no probabilística por juicio de expertos un muestreo intencional representativo de 5 activos críticos y 10 escenarios de riesgo (R01, R02, R03, R12, R13, R20, R21, R22, R36 y R37).

Esta muestra abarca la totalidad de las tipologías del universo (bases de datos de clientes, software de SO/ERP, hardware de escritorio/portátil y servicios de red ISP) y representa las zonas de mayor severidad (Crítico, Alto, Medio y Bajo). La selección actúa como una maqueta

metodológica estandarizada que demuestra la validez matemática del algoritmo de atenuación de MinTIC sin redundancia documental, dejando establecidas las pautas para que la organización, en su posterior fase de implementación real, replique el procedimiento sobre el 100% del universo evaluado.

6.3 Delimitación del Diagnóstico

El diagnóstico interno se delimita de manera exclusiva a las actividades y canales del área comercial de la empresa Bioconcentrados SAS. La evaluación centrará su atención en los siguientes aspectos críticos:

- Canales de recepción y gestión de pedidos (llamadas telefónicas, mensajería instantánea y toma de datos en campo).
- Seguridad en dispositivos móviles corporativos empleados por asesores comerciales en rutas rurales.
- Custodia y tratamiento de bases de datos de clientes, distribuidores y acuerdos de precios (cumplimiento Ley 1581 de 2012).
- Procedimientos de respaldo de información comercial y control de acceso a archivos compartidos.

6.4 Metodología y técnicas de recolección de la información

La ejecución del proyecto se desarrollará a través de una revisión sistemática de información primaria y secundaria. Como instrumento principal para el diagnóstico inicial, se aplicará una lista de chequeo (checklist) estructurada bajo la norma NTC-ISO/IEC 27001:2022 al personal clave del área comercial y al líder de sistemas.

El proceso metodológico contempla las siguientes técnicas:

- Revisión Documental: Análisis de formatos de pedido, listas de precios, contratos de distribución y procedimientos informales vigentes en la compañía.
- Entrevistas Semiestructuradas: Diálogo con el equipo comercial para caracterizar las dinámicas de venta con distribuidores y productores rurales.
- Cuestionario / Lista de Chequeo: Aplicación del instrumento cuantitativo para calcular la línea base de cumplimiento frente a los numerales 5 al 8 y el Anexo A de la norma ISO 27001:2022.

6.5 Instrumento de diagnóstico y escala oficial de valoración línea base (MINTIC - NTC-ISO/IEC 27001:2022)

Para la recolección de información y determinación del estado actual en el área comercial de Bioconcentrados SAS, la investigación adopta formalmente la matriz y los parámetros del Instrumento de Identificación de la Línea Base de Seguridad (NTC-ISO/IEC 27001:2022 Anexo A), diseñado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2021).

El diagnóstico se ejecuta aplicando la herramienta oficial en sus cuatro dominios normativos: Controles Organizacionales (A.5), Controles de Personas (A.6), Controles Físicos (A.7) y Controles Tecnológicos (A.8).

6.5.1 Escala de Valoración de Madurez de Controles

De acuerdo con la Escala de Valoración de Controles ISO 27001:2022 (Ver Anexo B) del instrumento oficial del MinTIC (2021), cada uno de los 93 controles del Anexo A se evalúa cualitativamente según su grado de adopción en la práctica comercial, asignándole la calificación numérica fija estandarizada por el Modelo MSPI.

6.5.2 *Criterios de Consolidación y Ponderación del Instrumento MinTIC*

La evaluación de la efectividad de los controles se consolida de forma automatizada en el herramental oficial siguiendo los parámetros nativos de la herramienta del MinTIC.

- **Calificación Promedio por Dominio:** Para cada uno de los cuatro dominios del Anexo A, la herramienta calcula la calificación actual utilizando la función de promedio aritmético simple redondeado al entero más cercano sobre el total de controles correspondientes.
- **Promedio Evaluación de Controles (Línea Base Global):** En la hoja "Portada" del instrumento, la calificación global del SGSI se obtiene mediante el promedio aritmético de las calificaciones consolidadas de los cuatro dominios.
- **Determinación del Nivel de Madurez Cualitativo:** El nivel de madurez final se asigna automáticamente en la matriz mediante la estructura jerárquica condicional de la herramienta oficial:
 - Inexistente: Calificación menor o igual a 1.
 - Inicial: Calificación entre 2 y 20.
 - Repetible: Calificación entre 21 y 40.
 - Efectivo: Calificación entre 41 y 60.
 - Gestionado: Calificación entre 61 y 80.
 - Optimizado: Calificación entre 81 y 100.

Integrando los resultados de los cuatro dominios se tiene los siguientes promedios reflejados en la siguiente tabla.

Tabla 1
Evaluación de Efectividad de controles

No.	Evaluación de Efectividad de controles			
	Dominio	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	Controles organizacionales	14	100	Inicial
A.6	Controles de personas	20	100	Inicial
A.7	Controles físicos	34	100	Repetible
A.8	Controles tecnológicos	15	100	Inicial
	Promedio Evaluación de Controles	21	100	Repetible

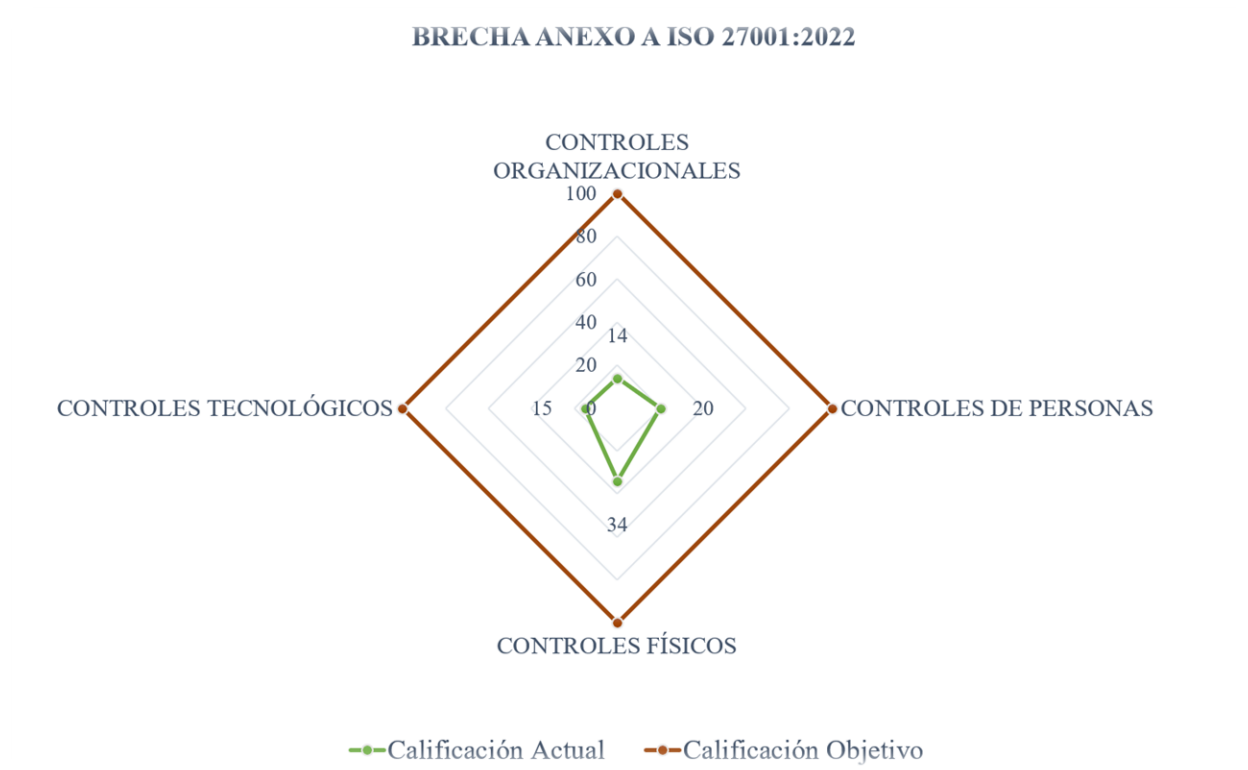
Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones – MinTIC (2022). Autodiagnostico MSPI

El diagnóstico consolida un porcentaje global de cumplimiento del 21% y una brecha operacional del 79%, fundamentando que la postura de seguridad de la empresa depende de hábitos individuales no estandarizados y justificando formalmente la elaboración de la propuesta de diseño del SGSI.

El comportamiento de la figura1 demuestra una acentuada asimetría en la postura de seguridad de la dependencia. Mientras la serie objetivo define el estándar ideal de conformidad (100%), la serie actual permanece replegada hacia el centro de la matriz con un promedio consolidado del 21%, lo que representa una brecha global del 79%.

Este resultado visual evidencia cuantitativamente que los mayores riesgos no se concentran en el perímetro físico, sino en los componentes lógicos, procedimentales y humanos del proceso de ventas, justificando de forma concluyente el desarrollo de la propuesta de diseño del SGSI orientada prioritariamente a los dominios A.5, A.6 y A.8.

Figura 3*Resultado visual Brecha Resultados del Anexo A*

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y Comunicaciones – MinTIC (2022). Autodiagnostico MSPI

6.6 Identificación y clasificación de activos de la información

Con el fin de establecer el inventario base para la gestión de riesgos en el área comercial de Bioconcentrados SAS, y en cumplimiento del control A.5.9 (Inventario de información y otros activos asociados) de la norma NTC-ISO/IEC 27001:2022, se llevó a cabo el levantamiento sistemático de los activos informáticos y procedimentales que intervienen en la atención a distribuidores, gestión de cartera y ventas en rutas rurales.

Para la categorización y caracterización del inventario, la presente investigación adopta la Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional del MSPI dictada por el Ministerio de Tecnologías de la

Información y las Comunicaciones (MinTIC, 2021). Esta metodología clasifica los activos según su naturaleza operacional en cinco categorías fundamentales:

- **Información (INF):** Datos de clientes, pagarés, expedientes de crédito y listas de precios..
- **Software (SOFT):** Aplicaciones informáticas, sistema ERP comercial, antivirus y herramientas de mensajería.
- **Hardware (HW):** Dispositivos de cómputo (PC de escritorio y portátiles), equipos de red y periféricos.
- **Servicios (SERV):** Canales de conectividad a Internet ISP y redes corporativas.
- **Personas / Intangibles (PER):** Conocimiento operativo y roles del proceso.

La recolección de información se estructuró de forma concertada con el líder del proceso comercial y el encargado de la infraestructura tecnológica, identificando un total de 21 activos críticos (Ver Tabla 2). Para cada elemento se especificó su tipo, descripción técnica, ubicación física o lógica, y el rol del propietario/custodio responsable de su preservación dentro del diseño del SGSI.

Tabla 2
Levantamiento de activos de información

Identificador	Macropr.	Proceso	Tipo de Activo (MinTIC)	Nombre del Activo	Propietario del Activo (Responsable)	Custodio del Activo
COM-100-01	Gestión Comercial	Gestión de Servicio al cliente facturación	de Información	Base de datos de clientes, distribuidores y cartera	Dirección y Comercial	Lider de TI
COM-100-02	Gestión Comercial	Gestión de Servicio al cliente facturación	de Información	Expedientes físicos pagarés, garantías remisiones	de Servicio al Cliente y	al Servicio al Cliente / Archivo

COM-100-03	Gestión Comercial	Gestión de Servicio al cliente facturación	Software	Sistema ERP / Facturación Comercial	Dirección Comercial	Lider de TI
COM-100-04	Gestión Comercial	Gestión TIC	Software	Antivirus Sophos Endpoint Protection	Lider de TI	Lider de TI
COM-100-05	Gestión Comercial	Gestión TIC	Software	Sistema Operativo Windows (Pro / Home)	Lider de TI	Lider de TI
COM-100-06	Gestión Comercial	Gestión de Servicio al cliente facturación	Software	Suite Microsoft Office (2019 / 2021 / 2024)	Dirección Comercial	Lider de TI
COM-100-07	Gestión Comercial	Gestión de Servicio al cliente facturación	Software	Correo Electrónico Institucional	Dirección Comercial	Lider de TI
COM-100-08	Gestión Comercial	Gestión de Servicio al cliente facturación	Software	WhatsApp Business Corporativo	Dirección Comercial	Asesores Comerciales
COM-100-09	Gestión Comercial	Gestión de Servicio al cliente facturación	Hardware	PC Escritorio Compumax (PC-10)	Servicio al Cliente (Shirley Villalba)	Lider de TI
COM-100-10	Gestión Comercial	Gestión de Servicio al cliente facturación	Hardware	PC Escritorio HP Pro SFF400 G9 (PC-22)	Servicio al Cliente (Armando Pantevis)	Lider de TI
COM-100-11	Gestión Comercial	Gestión Comercial y Asistencia Técnica	Hardware	Portátil ASUS ExpertBook B2402FB (PC-33)	Ventas (Nelson Rincón)	Lider de TI
COM-100-12	Gestión Comercial	Gestión de Servicio al cliente facturación	Hardware	Portátil HP 240 G9 (PC-42)	Ventas (Armando Pantevis)	Lider de TI
COM-100-13	Gestión Comercial	Gestión Comercial y Asistencia Técnica	Hardware	Portátil HP 240R G9 (PC-45)	Dirección Comercial (Franklin Ramírez)	Lider de TI
COM-100-14	Gestión Comercial	Gestión Comercial y Asistencia Técnica	Hardware	Portátil Lenovo V14 G4 (PC-47)	Dirección Comercial (Oscar Castillo)	Lider de TI
COM-100-15	Gestión Comercial	Gestión Comercial y Asistencia Técnica	Hardware	Portátil Acer Aspire Lite 14 (PC-32)	Ventas (Felipe Rincón)	Lider de TI

COM-100-16	Gestión Comercial	Gestión Comercial y Asistencia Técnica	Hardware	Portátil Lenovo ThinkPad E14 Gen 6 (PC-27)	Ventas (Faiver Andrés Cali)	Lider de TI
COM-100-17	Gestión Comercial	Gestión TIC	Hardware	Firewall Fortinet FortiGate 50G	Lider de TI	Lider de TI
COM-100-18	Gestión Comercial	Gestión TIC	Hardware	Switch gestionable Ruijie NBS5200-24GT4XS-P	RG- Lider de TI	Lider de TI
COM-100-19	Gestión Comercial	Gestión TIC	Hardware	Access Point Inalámbrico Ruijie AP RG-RAP2200E	Lider de TI	Lider de TI
COM-100-20	Gestión Comercial	Gestión de Servicio al cliente y facturación	Hardware	Impresora Multifuncional Kyocera Ecosys FS-2100DN	Servicio al Cliente	al Servicio al Cliente
COM-100-21	Gestión Comercial	Gestión TIC	Servicios	Canal Dedicado ISP Internet	Lider de TI	Proveedor ISP / TIC

Fuente: elaboración propia.

6.6.1 Valoración de los activos de información

Para determinar el nivel de protección requerido y el grado de criticidad de los activos de información del área comercial de Bioconcentrados SAS, la investigación adopta el Esquema de Clasificación de Activos de Información del MSP (MinTIC, 2021), alineado con los requisitos de la norma NTC-ISO/IEC 27001:2022, la Ley 1712 de 2014 y la Ley 1581 de 2012.

La tabla 3, 4 y 5 determinan la valoración considerando las tres dimensiones fundamentales de la seguridad de la información: Disponibilidad, Confidencialidad e Integridad (CID).

Para transformar las categorías normativas y cualitativas de la guía del MinTIC en métricas evaluables dentro del proyecto, se establece la escala discreta de impacto.

- **3 (Impacto Alto / Máxima Restricción):** Exposición a sanciones legales (Ley 1581 o Ley 1712), pérdidas económicas o parálisis del proceso comercial.

- **2 (Impacto Medio / Restricción Parcial):** Reprocesos administrativos o afectación operacional moderada.
- **1 (Impacto Bajo / Sin Restricción):** Impacto leve, sin implicaciones legales ni pérdidas financieras.

Tabla 3*Clasificación por Confidencialidad (Ley 1712 / Ley 1581)*

Criterio Cualitativo	Valor	Nivel de Impacto	Descripción del Criterio Normativo Aplicado
Información pública reservada	3	Alto	Información exenta de acceso público por ley o que protege decisiones estratégicas. Su divulgación causa daño grave a la entidad.
Información pública clasificada	3	Alto	Información que contiene datos personales (Ley 1581 de 2012) o secretos comerciales. Su divulgación vulnera la intimidad o la propiedad intelectual.
Información pública	1	Bajo	Información sin restricciones de acceso que puede ser entregada o publicada sin causar daño a la empresa o a terceros.
No clasificada	3	Alto	Activos no evaluados. Por principio de precaución normativa del MinTIC, se ponderan de manera preventiva como Reservada (3).

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones – MinTIC (2022). Autodiagnostico MSPI.

Tabla 4*Clasificación por Integridad*

Criterio Cualitativo (MinTIC)	Valor (VI)	Nivel de Impacto	Descripción del Criterio Operacional
Alta (A)	3	Alto	La pérdida de exactitud o alteración no autorizada del activo conlleva un <u>impacto negativo de índole legal, económica o daño severo de imagen.</u>
Media (M)	2	Medio	La alteración del activo conlleva un impacto económico o administrativo moderado, o retrasos parciales en las funciones de ventas.
Baja (B)	1	Bajo	La pérdida de exactitud del activo conlleva un impacto no significativo para la entidad o entes externos.
No Clasificada	3	Alto	Tratada preventivamente como Integridad Alta (3).

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones – MinTIC (2022). Autodiagnostico MSPI.

Tabla 5
Clasificación por Disponibilidad

Criterio Cualitativo	Valor	Nivel de Impacto	Descripción del Criterio Operacional
1 (Alta)	3	Alto	La no disponibilidad del activo genera un impacto negativo de índole legal, económica severa o la paralización inmediata del proceso de ventas.
2 (Media)	2	Medio	La no disponibilidad conlleva un impacto de índole económica o retraso moderado en las funciones operativas de la entidad.
3 (Baja)	1	Bajo	La no disponibilidad afecta la rutina normal, pero no conlleva implicaciones legales, financieras ni pérdida de imagen.
No Clasificada	3	Alto	Tratada preventivamente como Disponibilidad Alta (3).

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones – MinTIC (2022). Autodiagnostico MSPI

La tabla 6 da una guía de valoración para los activos 01-05-09-10 y 21 identificados de acuerdo a los niveles de criticidad expuestos anteriormente.

Tabla 6
Valoración de Activos

ID Activo	Nombre del Activo de Información	Tipo	Confidencialidad (Ley 1712 / Ley 1581)	Integridad	Disponibilidad
COM-100-01	Base de datos de clientes, distribuidores y cartera	Información	3	3	3
COM-100-05	Sistema Operativo Windows (Pro / Home)	Software	3	2	2
COM-100-09	PC Escritorio Compumax (PC-10 - Shirley Villalba)	Hardware	3	2	2
COM-100-10	PC Escritorio HP Pro SFF400 G9 (PC-22 - A. Pantevis)	Hardware	3	2	2
COM-100-21	Canal Dedicado ISP Internet	Servicios	3	3	3

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones – MinTIC (2022). Autodiagnostico MSPI

6.6.2 Identificación de amenazas ((NTC-ISO/IEC 27005:2022))

Para determinar los eventos potenciales que pueden vulnerar la confidencialidad, integridad o disponibilidad de los 21 activos de información del área comercial de Bioconcentrados SAS, la investigación adopta el catálogo de amenazas clásicas (Tabla 7) de la Norma Internacional ISO/IEC 27005:2022.

El estándar clasifica los factores de riesgo según su naturaleza operacional y caracteriza el Tipo de Fuente de Riesgo bajo la siguiente convención:

- **D (Deliberada):** Acciones intencionadas dirigidas a dañar, sustraer o comprometer los activos de información.
- **A (Accidental):** Acciones humanas no intencionadas, negligencias, errores de uso u omisiones operativas.
- **E (Entorno / Medioambiental):** Fenómenos climáticos, naturales o eventos no basados en la acción humana directa.

Tabla 7
Amenazas

Categoría (ISO 27005:2022)	Código	Descripción de la Amenaza	Fuente de Riesgo
Amenazas Físicas	TP01	Fuego / Incendio	A, D, E
Amenazas Físicas	TP02	Agua / Inundación en instalaciones	A, D, E
Amenazas Físicas	TP04	Accidente grave	A, D, E
Amenazas Físicas	TP06	Polvo, corrosión, humedad o agentes ambientales	A, D, E
Amenazas Naturales	TN01	Fenómeno climático o meteorológico severo	E
Fallas en las Infraestructuras	TI01	Fallas en el sistema de suministro básico	A, D
Fallas en las Infraestructuras	TI03	Pérdida del suministro de energía eléctrica	A, D, E
Fallas en las Infraestructuras	TI04	Falla de una red de telecomunicaciones / Canal ISP	A, D, E
Fallas en las Infraestructuras	TI05	Falla del equipo de telecomunicaciones (Switch / AP / Firewall)	A, D
Fallas Técnicas	TT01	Falla de dispositivos informáticos o sistemas (Laptops / PCs)	A
Fallas Técnicas	TT02	Saturación del sistema de información / Caída del ERP	A, D
Fallas Técnicas	TT03	Vulneración o falta de mantenimiento del sistema	A, D
Acciones Humanas	TH01	Atentado, ataque o sabotaje	D
Acciones Humanas	TH02	Ingeniería social (Phishing / Suplantación telefónica)	D
Acciones Humanas	TH06	Robo de medios de almacenamiento o documentos	D
Acciones Humanas	TH07	Robo de equipos de cómputo o móviles de ruta comercial	D
Acciones Humanas	TH08	Robo de identidad digital o de credenciales de acceso	D

Acciones Humanas	TH10	Divulgación no autorizada de información confidencial	A, D
Acciones Humanas	TH11	Entrada de datos de fuentes no fiables	A, D
Acciones Humanas	TH12	Manipulación no autorizada del hardware	D
Acciones Humanas	TH13	Manipulación o alteración del software	A, D
Acciones Humanas	TH16	Tratamiento no autorizado de datos personales (Ley 1581)	A, D
Acciones Humanas	TH17	Entrada no autorizada a instalaciones de la empresa	D
Acciones Humanas	TH18	Uso no autorizado de dispositivos informáticos	D
Acciones Humanas	TH19	Uso incorrecto de los dispositivos corporativos	A, D
Acciones Humanas	TH20	Daño físico de dispositivos o medios de almacenamiento	A, D
Acciones Humanas	TH22	Uso de software falsificado o copiado sin licencia	A, D
Acciones Humanas	TH23	Corrupción de bases de datos o archivos	D
Acciones Humanas	TH25	Envío o distribución de malware / Ransomware	A, D, E
Compromiso de Funciones / Servicios	TC01	Error involuntario en el uso de los sistemas	A
Compromiso de Funciones / Servicios	TC02	Abuso de derechos o permisos de acceso	A, D
Compromiso de Funciones / Servicios	TC03	Falsificación de derechos o permisos	D
Amenazas a la Organización	TO02	Falta de recursos financieros o tecnológicos	A, E
Amenazas a la Organización	TO03	Falla o incumplimiento de los proveedores de servicios TIC	A, E
Amenazas a la Organización	TO04	Violación de la legislación o la normativa vigente	A, D

Fuente. Adaptado de la norma internacional ISO/IEC 27005:2022.

6.7 Estructura y valoración de riesgos inherentes (NTC-ISO 31000:2018)

El análisis de riesgos adopta la misma matriz discreta de 1 a 3 para las variables de Probabilidad e Impacto, estructurando una matriz de evaluación de 3x3 con valores de riesgo inherente ajustados a la norma NTC-ISO 31000:2018 (MinTIC, 2021).

Tabla 8
Escala de Probabilidad de Ocurrencia

Valor (P)	Criterio	Descripción de la Frecuencia Adaptada al Proceso Comercial	Frecuencia Anual Estimada
3	Alta	Evento altamente probable o latente debido al trabajo en rutas rurales o a la falta de controles informáticos.	Ocurrencia frecuente (más de 12 veces al año)
2	Media	Evento de ocurrencia ocasional vinculado a fallas operativas o fallas de proveedores de tecnología.	Ocurrencia esporádica (entre 3 y 11 veces al año)
1	Baja	Evento raro o poco frecuente en la rutina operativa de la dependencia comercial.	Ocurrencia rara (menos de 2 veces al año)

Fuente: elaboración propia.

Tabla 9
Escala de Impacto Organizacional

Valor (I)	Criterio	Descripción de Consecuencias en Bioconcentrados SAS	Impacto Operativo / Financiero
3	Alto	Parálisis total del proceso de ventas/facturación, multas por incumplimiento de la Ley 1581 o pérdida de activos de alto valor.	Impacto Severo / Financiero Alto
2	Medio	Retrasos en la atención de pedidos, reprocesos administrativos o fallas corregibles a corto plazo.	Impacto Moderado / Reprocesos
1	Bajo	Incumplimientos menores que no afectan la continuidad del negocio ni generan pérdidas económicas.	Impacto Leve no significativo

Fuente: elaboración propia.

6.7.1 Valoración y Algoritmo de Cálculo del Riesgo

La valoración cuantitativa y cualitativa del riesgo se obtiene al multiplicar el valor de la probabilidad de ocurrencia por el nivel de impacto estimado (Impacto X Probabilidad). Estos parámetros fueron concertados en mesas de trabajo con el Director Comercial y el encargado de la infraestructura tecnológica de Bioconcentrados SAS al momento de exponer las amenazas normativas (NTC-ISO/IEC 27005:2022) a las que se encuentran expuestos los 21 activos de información identificados.

De esta manera, como se ilustra en la Tabla 10, se consolida la matriz 3 X 3 para obtener el valor del riesgo inherente, el cual ubica a cada evento dentro de una coordenada cartesiana para definir su correspondiente estrategia de tratamiento operativo.

Tabla 10*Matriz 3 X 3 de Calificación y Posicionamiento del Riesgo Inherente*

Impacto (I)	Probabilidad Baja (1)	Probabilidad Media (2)	Probabilidad Alta (3)
Alto (3)	3 (Riesgo Medio)	6 (Riesgo Alto)	9 (Riesgo Crítico)
Medio (2)	2 (Riesgo Bajo)	4 (Riesgo Medio)	6 (Riesgo Alto)
Bajo (1)	1 (Riesgo Bajo)	2 (Riesgo Bajo)	3 (Riesgo Medio)

Fuente. elaboración propia con base en la norma NTC-ISO 31000:2018.

El propósito de realizar esta valoración radica en fundamentar objetivamente la toma de decisiones gerenciales, comparando los resultados cuantitativos del análisis con los criterios de aceptabilidad y tolerancia al riesgo previamente definidos por la organización. Este procedimiento conduce a tres decisiones fundamentales frente al tratamiento de las amenazas:

- **Asumir el riesgo:** Aplicable a aquellos eventos ubicados en niveles bajos, donde la probabilidad de ocurrencia o el impacto financiero no comprometen la continuidad de la empresa, requiriendo un seguimiento periódico.
- **Reducir el riesgo:** Aplicable a riesgos de nivel medio, en los cuales se implementan controles procedimentales sugeridos del Anexo A de la NTC-ISO/IEC 27001:2022 para minimizar la probabilidad de que la amenaza se materialice.
- **Mitigar o transferir el riesgo:** Aplicable a los activos con mayor criticidad o expuestos a zonas de riesgo alto o crítico. Se exige la aplicación estricta de controles tecnológicos, políticas obligatorias e intervenciones inmediatas de la alta dirección.

Con base en estas premisas, en la Tabla 11 se establecen las zonas de riesgo inherente y sus respectivos lineamientos de tratamiento institucional dentro del diseño del SGSI.

Tabla 11*Criterios de Aceptación y Zonas de Tratamiento del Riesgo (RI)*

Zona de Riesgo	Valoración (RI)	Criterio y Acción de Tratamiento Institucional
Zona de Riesgo Bajo (Verde)	1 – 2	El riesgo se asume por parte del área comercial y se realiza seguimiento operacional periódico.
Zona de Riesgo Medio (Amarillo)	3 – 4	El riesgo se debe reducir mediante la aplicación procedimental de controles sugeridos.
Zona de Riesgo Alto / Crítico (Rojo)	6 – 9	Se debe mitigar o transferir el riesgo de forma prioritaria con la aplicación estricta de controles normativos.

Fuente: elaboración propia adaptado de la norma NTC-ISO 31000:2018.

6.8 Matriz de evaluación del riesgo inherente

A continuación en la tabla 12, se presenta la matriz adaptada para los 5 activos que se tomaron como muestra de Bioconcentrados SAS, vinculando el catálogo de amenazas de la ISO/IEC 27005:2022.

Tabla 12*Matriz General de Evaluación del Riesgo Inherente*

ID Activo	Nombre del Activo	ID Amenaza (ISO 27005)	Descripción de la Amenaza Evaluada	Impacto (I)	Probabilidad (P)	Riesgo Inherente (RI=I×P)	ID Riesgo	Zona de Riesgo Resultante
COM-100-01	Base de datos de clientes y cartera	TH16	Tratamiento no autorizado de datos personales	3	3	9	R01	Riesgo Crítico
COM-100-01	Base de datos de clientes y cartera	TH10	Divulgación no autorizada de información	3	3	9	R02	Riesgo Crítico
COM-100-01	Base de datos de clientes y cartera	TH23	Corrupción de datos de cartera y precios	3	2	6	R03	Riesgo Alto
COM-100-05	Sistema Operativo Windows	TH25	Infección por malware o ransomware local	3	3	9	R12	Riesgo Crítico
COM-100-05	Sistema Operativo Windows	TT03	Falta de parches de seguridad (Hardening)	2	3	6	R13	Riesgo Alto
COM-100-09	PC Escritorio Compumax (PC-10)	TT01	Falla de hardware por desgaste o uso	2	2	4	R20	Riesgo Medio
COM-100-09	PC Escritorio Compumax (PC-10)	TI03	Pérdida de energía eléctrica sin respaldo	2	2	4	R21	Riesgo Medio

COM-100-10	PC Escritorio HP Pro (PC-22)	TT01	Falla de disco SSD o componentes	2	1	2	R22	Riesgo Bajo
COM-100-21	Canal Dedicado ISP Internet	TI04	Corte del servicio de telecomunicaciones	3	3	9	R36	Riesgo Crítico
COM-100-21	Canal Dedicado ISP Internet	TO03	Incumplimiento del proveedor de internet	3	2	6	R37	Riesgo Alto

Fuente: elaboración propia.

Teniendo en cuenta los riesgos inherentes para todos los activos de información, posteriormente se ubican en una tabla denominada cuadrante resultante la cual nos sirve de guía para ver el estado actual de los activos y que los riesgos se puedan materializar. La tabla 13 muestra como seria este cuadrante para los 5 activos de muestra.

Tabla 13

Cuadrante Resultante y Mapa de Calor del Riesgo Inherente

Impacto (I)	Probabilidad Baja (1)	Probabilidad Media (2)	Probabilidad Alta (3)
Alto (3)	Sin eventos (RI = 3: Riesgo Medio)	R03, R37 (RI = 6: Riesgo Alto)	R01, R02, R12, R36 (RI = 9: Riesgo Crítico)
Medio (2)	R22 (RI = 2: Riesgo Bajo)	R20, R21 (RI = 4: Riesgo Medio)	R13 (RI = 6: Riesgo Alto)
Bajo (1)	Sin eventos (RI = 1: Riesgo Bajo)	Sin eventos (RI = 2: Riesgo Bajo)	Sin eventos (RI = 3: Riesgo Medio)

Fuente: elaboración propia.

6.9 Estrategia de tratamiento de riesgos

Con base en la valoración del riesgo inherente ($RI = I \times P$) efectuada sobre los 5 activos de información de ejemplo de la dependencia comercial, y tras los espacios de concertación con la Dirección Comercial y el área de Tecnología de Bioconcentrados S.A.S., se establecen las directrices para la selección e integración de los controles del Anexo A de la NTC-ISO/IEC 27001:2022.

La finalidad de esta etapa es contener la probabilidad de exposición ante las amenazas y reducir su impacto hasta un umbral de tolerancia aceptable para la compañía. Para articular la ejecución de las actividades de mitigación, la organización determinó un esquema de

priorización temporal enfocado en las amenazas ubicadas en los rangos Medio, Alto y Crítico.

Este marco temporal define plazos de respuesta, horizontes de despliegue y una periodicidad estricta para el seguimiento de la efectividad de las medidas adoptadas como lo muestra la tabla 14.

Tabla 14

Cronograma y Cronología para el Tratamiento de Riesgos Comercial

Zona de Riesgo (Matriz 3 x 3)	Nivel de Riesgo	Valoración (RI)	Tiempo Propuesto de Tratamiento	Planificación e Implementación	Seguimiento y Revisión
Zona Verde	Riesgo Bajo	1 – 2	N/A (Se asume)	N/A	Anual
Zona Amarilla	Riesgo Medio	3 – 4	4 Meses	3 Meses	Mensual
Zona Roja (Media)	Riesgo Alto	6	2 Meses	2 Meses	Mensual
Zona Roja (Alta)	Riesgo Crítico	9	2 Meses	2 Meses	Mensual

Fuente: elaboración propia.

6.9.1 Tiempos Propuestos para la Ejecución del Tratamiento de Riesgos

Con el fin de garantizar un despliegue ordenado y sostenible de los controles del Anexo A en la dependencia comercial de Bioconcentrados S.A.S., se estructuran los plazos operativos según la categoría de severidad resultante:

- **Riesgos de Nivel Medio (RI = 3 o 4):** Al tratarse de vulnerabilidades de naturaleza operativa o procedimental que requieren reducción gradual, se destina una fase de planificación de 4 meses. Este tiempo se enfoca en el análisis, selección y estructuración de herramientas o instructivos que faciliten su adopción. Posterior a ello, se establece un periodo de implementación de 3 meses, lapso que contempla la fase de prueba, estabilización y evaluación inicial de resultados. Finalmente, se instaura un esquema de monitoreo periódico de frecuencia mensual para asegurar la contención del riesgo.

- **Riesgos de Nivel Alto (RI = 6):** Para los eventos que presentan un impacto severo sobre la continuidad del negocio o la integridad de los datos, se define una fase de planificación de 2 meses. Durante este periodo se prioriza la búsqueda, selección y cotización de soluciones tecnológicas o el acompañamiento de proveedores externos capacitados para mitigar la amenaza. A continuación, se ejecuta un periodo de implementación de 2 meses enfocado en el despliegue técnico y la obtención de evidencias operativas, complementado con un seguimiento continuo de carácter mensual que garantice la efectividad permanente del control.
- **Riesgos de Nivel Crítico / Extremo (RI = 9):** Esta categoría agrupa los escenarios de mayor severidad (tales como la pérdida de información confidencial de clientes o el hurto de activos de alta movilidad en rutas rurales). Su atención exige controles estrictos e intervenciones especializadas; por tanto, se plantea una etapa de planificación de 2 meses orientada al estudio de mercado y contratación de servicios o herramientas avanzadas de protección (como software de cifrado o plataformas especializadas). Se establece un periodo de ejecución e implementación de 2 meses para la puesta en marcha de los controles, complementado con supervisión e inspección obligatoria de periodicidad mensual.

6.9.2 Metodología de asignación de controles y estimación de efectividad

Teniendo en cuenta el tratamiento de los riesgos sugerido y los tiempos indicados por la gerencia de Bioconcentrados S.A.S. para su implementación, en la tabla 15 se realizó la asignación de controles del Anexo A de la norma NTC-ISO/IEC 27001:2022 para los 5 activos que se tienen de base de los riesgos con mayor probabilidad e impacto de materialización en el área comercial esto con el fin de ser una guía para su ejecución para todos los activos del área.

De esta forma, se busca reducir la exposición ante las amenazas y generar un resultado esperado de mitigación que garantice un nivel de riesgo residual aceptable para la organización. La efectividad de los controles se evaluó de manera cuantitativa utilizando la metodología estandarizada por la Guía de Administración del Riesgo del MinTIC, ponderando los atributos técnicos de cada medida según su tipo (Preventivo: 25%, Detectivo: 15%, Correctivo: 10%) y su modo de implementación (Automático: 25%, Manual: 10% - 15%).

Bajo este modelo oficial, la efectividad se calcula mediante la combinación matemática de dos atributos característicos del control propuesto del Anexo A de la NTC-ISO/IEC 27001:2022

$$EC = \{\text{Peso del Tipo de Control}\} + \{\text{Peso del Modo de Implementación}\}$$

Tabla 15

Controles del Anexo A, Estrategia Sugerida y Porcentaje de Efectividad Esperado para los Activos de Información.

ID Activo	ID Riesgo	Controles Anexo A	Descripción del Control	Estrategia de Implementación en Bioconcentrados S.A.S.	Tipo de Control (MinTIC)	Modo de Implem.	% Efectividad del Control
COM-100-01	R01	A.5.34	Protección de datos personales	Protocolo formal de Hábeas Data (Ley 1581) para la recolección de información de clientes y cartera.	Preventivo (25%)	Manual (15%)	40%
COM-100-01	R02	A.8.3	Restricción de acceso a la información	Matriz de permisos de lectura y edición sobre las carpetas compartidas de la base de clientes.	Preventivo (25%)	Automático (25%)	50%
COM-100-01	R03	A.8.13	Respaldo de información	Copias de seguridad incrementales automatizadas para la base de datos de cartera.	Preventivo (25%) + Detectivo (15%)	Automático (25%)	65%
COM-100-05	R12	A.8.1	Dispositivos de usuario final	Políticas de grupo (GPO) para el bloqueo de sesión y descarga automática de parches de Windows.	Preventivo (25%)	Automático (25%)	50%
COM-100-05	R13	A.8.8	Gestión de vulnerabilidades técnicas	Ventana mensual de actualización de parches de seguridad en sistemas operativos de escritorio.	Detectivo (15%)	Automático (25%)	40%
COM-100-09	R20	A.7.13	Mantenimiento de equipos	Plan técnico preventivo trimestral de limpieza y	Preventivo (25%)	Manual (15%)	40%

				mantenimiento físico de hardware.			
COM-100-09	R21	A.7.11	Suministros de soporte	Conexión de computadores de escritorio a la red de respaldo ininterrumpido por UPS.	Correctivo (10%)	Automático (25%)	35%
COM-100-10	R22	A.7.13	Mantenimiento de equipos	Diagnóstico semestral del estado de salud de discos de estado sólido (SSD) e inspección técnica.	Detectivo (15%)	Manual (15%)	30%
COM-100-21	R36	A.8.21	Servicios de red	Contratación de canal de conectividad redundante (Failover) ante caídas del proveedor ISP principal.	Preventivo (25%) + Correctivo (10%)	Automático (25%)	60%
COM-100-21	R37	A.5.21	Cadena de suministro TIC	Firma de Acuerdos de Nivel de Servicio (SLA) con el proveedor de internet con respuesta < 4 horas.	Preventivo (25%)	Manual (15%)	40%

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones. MinTIC (2022). Riesgos de la seguridad de la información MSPI

6.9.3 Aplicación y efectividad de los controles y cálculo del riesgo residual

Con la selección de los controles del Anexo A de la NTC-ISO/IEC 27001:2022, se realiza la evaluación de efectividad sobre las variables de Probabilidad (P) e Impacto (I), proyectando la reducción de los eventos de riesgo evaluados sobre los activos del área comercial de Bioconcentrados S.A.S.

El diseño adopta la Herramienta MSPI. La efectividad del control (%EC) se obtiene mediante la suma algorítmica de sus atributos operacionales:

$$\%EC = \text{Peso por Tipo de Control} + \text{Peso por Modo de Implementación}$$

Tabla 16
Ponderación Oficial de Atributos de Control

Atributo del Control	Categoría Operativa	Peso Porcentual Ponderado	Criterio de Aplicación en Bioconcentrados S.A.S.
Tipo de Control	Preventivo	25%	Previene la causa raíz para evitar la materialización de la amenaza.
	Detectivo	15%	Alerta o identifica la ocurrencia de la falla o incidente.
	Correctivo	10%	Restablece el servicio o contiene el daño tras la falla.
Modo de Implementación	Automático	25%	Ejecución lógica por software/sistema sin sesgo de error humano.

Manual	10%	Ejecución sujeta al procedimiento o verificación del personal.
--------	-----	--

Fuente. Elaboración propia con base en la Herramienta de Riesgos MSPI – MinTIC

6.9.4 Operaciones Matemáticas para el Cálculo del Riesgo Residual (RR)

Para la aplicación del modelo de gestión de riesgos en Bioconcentrados S.A.S., se establece una regla algorítmica estricta basada en la naturaleza del control seleccionado del Anexo A de la norma NTC-ISO/IEC 27001:2022 y la matriz del MSPI.

En el proceso de recálculo del riesgo, un control no ataca indiscriminadamente ambas variables del riesgo (Impacto y Probabilidad) a menos que esté diseñado operacionalmente para ello. Por lo tanto, el responsable del proceso debe identificar el campo de acción del control (Atributo de Afectación) bajo las siguientes tres reglas operativas:

- **Controles de Afectación a la Probabilidad (Controles Preventivos):** Son controles diseñados para evitar la causa raíz o reducir la frecuencia de ocurrencia del evento (e.g., políticas de Hábeas Data, capacitaciones de Phishing, restricciones de acceso):

Nuevo Impacto (NI): No cambia. Se copia el mismo número inicial ($NI = I$).

Nueva Probabilidad (NP): Se usa la formula:

$NP = \text{Redondear}[P \times (1 - \%EC)]$ (las fórmulas de recálculo aplican la función de redondeo al entero discreto más cercano (1, 2, 3))

- **Controles de Afectación al Impacto (Controles Correctivos o de Contención):** Son controles enfocados en mitigar la severidad del daño o garantizar la continuidad una vez que el incidente se ha materializado (e.g., copias de seguridad/backups, pólizas de garantía, planes de redundancia UPS/Failover).

Nuevo Impacto (NI): Se usa la formula:

$NI = \text{Redondear}[I \times (1 - \%EC)]$ (las fórmulas de recálculo aplican la función de redondeo al entero discreto más cercano (1, 2, 3))

- **Nueva Probabilidad (NP):** No cambia. Se copia el mismo número inicial ($NP = P$).
- **Controles de Afectación Dual (Controles Combinados o de Protección Integral):**

Ocurre cuando la estrategia asignada combina salvaguardas tecnológicas de prevención y contención lógica en el mismo activo (e.g., Cifrado BitLocker con borrado remoto A.8.1, o sistemas EDR/Antivirus centralizado A.8.7).

Nuevo Impacto (NI): Se usa la formula:

$NI = \text{Redondear}[I \times (1 - \%EC)]$ (las fórmulas de recálculo aplican la función de redondeo al entero discreto más cercano (1, 2, 3))

Nueva Probabilidad (NP): Se usa la formula:

$NP = \text{Redondear}[P \times (1 - \%EC)]$ (las fórmulas de recálculo aplican la función de redondeo al entero discreto más cercano (1, 2, 3))

La Tabla 17, muestra como se estaría calculando el riesgo residual con base en los criterios expuestos para los riesgos R01, R02, R03, R12, R13, R20, R21, R22, R36 y R37 que se trabajaron como ejemplo en la tabla 15.

Tabla 17
Matriz General de Evaluación del Riesgo Residual

ID Riesgo	ID Amenaza	Impacto (I)	Probabilidad (P)	Riesgo Inherente (RI)	Control Anejo A	Afectación	Tipo de Control (MinTIC)	Implementación (MinTIC)	% Efectividad (%EC)	Nuevo Impacto (NI)	Nueva Probabilidad (NP)	Riesgo Residual (RR=NI × NP)	Zona Residual Resultante
R01	TH16	3	3	9 (Crítico)	A.5.34	Probabilidad	Preventivo (25%)	Manual (10%)	35%	3	2	6	Riesgo Alto (En Tratamiento)
R02	TH10	3	3	9 (Crítico)	A.8.3	Dual (\$I / PS)	Preventivo (25%)	Automático (25%)	50%	2	2	4	Riesgo Medio (Tolerable)
R03	TH23	3	2	6 (Alto)	A.8.13	Impacto	Correctivo (10%)	Automático (25%)	35%	2	2	4	Riesgo Medio (Tolerable)

R12	TH25	3	3	9 (Crítico)	A.8.1	Dual (\$I / P\$)	Preventivo (25%)	Automático (25%)	50%	2	2	4	Riesgo Medio (Tolerable)
R13	TT03	2	3	6 (Alto)	A.8.8	Probabilidad	Preventivo (25%)	Automático (25%)	50%	2	2	4	Riesgo Medio (Tolerable)
R20	TT01	2	2	4 (Medio)	A.7.13	Probabilidad	Preventivo (25%)	Manual (10%)	35%	2	1	2	Riesgo Bajo (Aceptable)
R21	TI03	2	2	4 (Medio)	A.7.11	Impacto	Correctivo (10%)	Automático (25%)	35%	1	2	2	Riesgo Bajo (Aceptable)
R22	TT01	2	1	2 (Bajo)	A.7.13	Probabilidad	Detectivo (15%)	Manual (10%)	25%	2	1	2	Riesgo Bajo (Aceptable)
R36	TI04	3	3	9 (Crítico)	A.8.21	Dual (\$I / P\$)	Preventivo (25%)	Automático (25%)	50%	2	2	4	Riesgo Medio (Tolerable)
R37	TO03	3	2	6 (Alto)	A.5.21	Probabilidad	Preventivo (25%)	Manual (10%)	35%	3	1	3	Riesgo Medio (Tolerable)

Fuente. elaboración propia con base en la Herramienta MSPI – MinTIC

La tabla 18, muestra como estaria el cuadrante del riesgo residual.

Tabla 18

Cuadrante de Ubicación del Riesgo Residual Resultante

Impacto (I) \ Probabilidad (P)	Probabilidad Baja (1)	Probabilidad Media (2)	Probabilidad Alta (3)
Alto (3)	R37	R01	Ninguno
Medio (2)	R20, R22	R02, R03, R12, R13, R36	Ninguno
Bajo (1)	Ninguno	R21	Ninguno

Fuente. elaboración propia.

6.10 Justificación y Marco Metodológico del SoA en la Fase de Diseño

En cumplimiento estricto del numeral 6.1.3 d de la norma NTC-ISO/IEC 27001:2022 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI - MinTIC), se formula la propuesta de la SoA para el área comercial de Bioconcentrados S.A.S.

Es fundamental precisar que el presente documento constituye una guía metodológica y un plano de diseño para el SGSI. La demostración analítica de la matriz se realiza sobre una muestra representativa de 10 eventos de riesgo priorizados (R01, R02, R03, R12, R13, R20, R21, R22, R36 y R37) de los 37 identificados en el inventario general del área comercial. Esta simplificación ilustrativa permite establecer las pautas para que, en la posterior fase de ejecución e implementación real por parte de la organización, la metodología sea replicada sobre la totalidad de los activos y riesgos del proceso comercial.

Como instrumento de gobernanza dentro del diseño del SGSI, la propuesta de SoA justifica de manera transparente:

- **Inclusión de Controles:** Las salvaguardas seleccionadas para mitigar los 10 riesgos muestreados de la gestión comercial, así como aquellas requeridas por mandatos legales vigentes en Colombia (ej. Ley 1581 de 2012 de Protección de Datos Personales).
- **Exclusión de Controles:** Las razones técnicas y operativas por las cuales determinados controles del Anexo A no aplican al alcance delimitado, evitando que la empresa incurra en sobrecostos o esfuerzos innecesarios en la futura etapa de implementación.

6.11 Criterios de Clasificación para Inclusión y Exclusión

De acuerdo con la metodología del MSPI (MinTIC) y la NTC-ISO/IEC 27001:2022, la asignación de aplicabilidad sobre los controles del Anexo A se fundamentó en tres criterios operacionales:

- **Aplicable por Mitigación de Riesgos (A-R):** El control es técnicamente indispensable para reducir la Probabilidad o el Impacto de los eventos de riesgo de la muestra (R01, R02, R03, R12, R13, R20, R21, R22, R36 y R37).

- **Aplicable por Cumplimiento Legal / Normativo (A-L):** El control se adopta de forma obligatoria para dar cumplimiento a leyes nacionales (Hábeas Data), regulaciones del sector agroindustrial o políticas corporativas de Bioconcentrados S.A.S.
- **No Aplicable / Excluido (NA):** El control no aplica a la operación del área comercial debido a la delimitación del alcance en el diseño. Las principales exclusiones responden a:

Ausencia de Desarrollo Interno de Software: Las herramientas informáticas del área comercial (ERP, CRM) son contratadas bajo modalidad de software en la nube (SaaS), no desarrolladas internamente.

Perímetro de Seguridad Industrial: Losn controles de infraestructura física industrial o centro de datos principal están a cargo del área corporativa central de TIC y no de la fuerza comercial descentralizada.

6.12 Resumen de Aplicabilidad por Dominios

La versión 2022 de la NTC-ISO/IEC 27001 reestructuró los controles en 4 dominios temáticos. En la tabla 21 se consolida la distribución ejecutiva planteada en este diseño para la muestra representativa de riesgos de Bioconcentrados S.A.S.:

Tabla 19

Resumen Consolidado de la Declaración de Aplicabilidad (SoA).

Dominio del Anexo A (ISO 27001:2022)	Total Controles	Aplicables (Incluidos)	No Aplicables (Excluidos)	Justificación General en el Diseño
1. Organizacionales (A.5.1 a A.5.37)	37	31	6	Incluidos: Políticas, roles, gestión de activos y Hábeas Data. Excluidos: Continuidad industrial y gestión de proyectos de software propio.
2. Personas (A.6.1 a A.6.8)	8	8	0	Incluidos (100%): Selección de personal, acuerdos de confidencialidad, concienciación e instrucción para teletrabajo.
3. Físicos (A.7.1 a A.7.14)	14	9	5	Incluidos: Seguridad de equipos en campo, mantenimiento y destrucción

				de Excluidos: Barreras físicas perimetrales y centros de datos industriales.
4. Tecnológicos (A.8.1 a A.8.34)	34	26	8	Incluidos: Autenticación MFA, cifrado BitLocker, respaldos en nube y parches. Excluidos: Ciclo de vida de desarrollo seguro de software y acceso a código fuente.
Totales Consolidados	93	74 (79.6%)	19 (20.4%)	Estructura completa propuesta del SGSI para el proceso comercial.

Fuente. elaboración propia con base en la NTC-ISO/IEC 27001:2022 y la herramienta de gestión de riesgos del MSPI - MinTIC.

6.13 Matriz Detallada de la Declaración de Aplicabilidad (93 Controles - Anexo A)

A continuación se presenta el desglose de la propuesta metodológica sobre los 93 controles del Anexo A, vinculando de manera explícita los 10 riesgos tomados como ejemplo en el documento (R01, R02, R03, R12, R13, R20, R21, R22, R36 y R37) para orientar la futura implementación en Bioconcentrados S.A.S.:

Tabla 20

Matriz Maestra de la Declaración de Aplicabilidad (SoA - ISO 27001:2022 / MSPI).

Código	Nombre del Control (ISO 27001:2022)	¿Aplica?	Justificación Técnica de Inclusión / Exclusión	Criterio / Origen Muestreado
1. Controles Organizacionales (A.5.1 - A.5.37)				
A.5.1	Políticas para la seguridad de la información	SÍ	Directrices generales de cumplimiento para la fuerza comercial.	MSPI / SGSI
A.5.2	Funciones y responsabilidades en seguridad	SÍ	Asignación de responsabilidades de custodia de activos en ventas.	MSPI / SGSI
A.5.3	Segregación de funciones	SÍ	Prevención de fraude en cotizaciones, descuentos y facturación.	Riesgo R01
A.5.4	Responsabilidades de la dirección	SÍ	Compromiso gerencial con la asignación de recursos.	MSPI / SGSI
A.5.5	Contacto con autoridades	SÍ	Protocolo de reporte ante la SIC o la Policía Nacional/Cai Virtual.	MSPI / SGSI
A.5.6	Contacto con grupos de interés especial	SÍ	Participación en gremios comerciales y de seguridad TIC.	Buenas Prácticas
A.5.7	Inteligencia sobre amenazas	SÍ	Monitoreo de nuevas modalidades de phishing y fraude en el sector.	MSPI / SGSI
A.5.8	Seguridad en la gestión de proyectos	NO	Excluido. El área comercial no ejecuta proyectos de desarrollo de TIC.	Operación Comercial
A.5.9	Inventario de información y otros activos	SÍ	Mantenimiento del inventario de los activos comerciales.	Base del SGSI
A.5.10	Uso aceptable de la información y activos	SÍ	Reglamento de uso de portátiles, móviles y ERP comercial.	MSPI / SGSI

A.5.11	Devolución de activos	SÍ	Procedimiento de entrega de equipos al finalizar el contrato.	MSPI / SGSI
A.5.12	Clasificación de la información	SÍ	Categorización de listas de precios y datos de clientes.	MSPI / Ley 1581
A.5.13	Etiquetado de la información	SÍ	Marcado de documentos como Confidencial o Uso Interno.	MSPI / SGSI
A.5.14	Transferencia de información	SÍ	Protocolos de envío seguro de bases de datos por correo/canales.	Ley 1581 / MSPI
A.5.15	Control de acceso	SÍ	Políticas de asignación de permisos según el rol comercial.	Riesgos R02, R12
A.5.16	Gestión de identidades	SÍ	Administración del ciclo de vida de usuarios en ERP y CRM.	Riesgo R02
A.5.17	Información de autenticación	SÍ	Gestión de credenciales y contraseñas seguras.	Riesgo R02
A.5.18	Derechos de acceso	SÍ	Revocación inmediata de accesos tras retiros de personal.	MSPI / SGSI
A.5.19	Seguridad en las relaciones con proveedores	SÍ	Acuerdos de seguridad con plataformas de software en la nube.	MSPI / SGSI
A.5.20	Direccionamiento de la seguridad en acuerdos de proveedores	SÍ	Cláusulas contractuales con proveedores de conectividad y CRM.	Riesgo R37
A.5.21	Seguridad en la cadena de suministro de TIC	NO	Excluido. La gestión de proveedores de TIC base es centralizada por TI corporativa.	Alcance Operativo
A.5.22	Monitoreo y revisión de servicios de proveedores	NO	Excluido. La revisión de SLA informáticos corresponde a la Dirección de TI.	Alcance Operativo
A.5.23	Seguridad en el uso de servicios en la nube	SÍ	Gobernanza sobre Google Workspace / Microsoft 365.	Riesgo R03
A.5.24	Planificación y preparación de gestión de incidentes	SÍ	Plan de respuesta ante fuga de datos o interrupción comercial.	MSPI / SGSI
A.5.25	Evaluación y decisión sobre eventos de seguridad	SÍ	Clasificación de anomalías detectadas por vendedores.	MSPI / SGSI
A.5.26	Respuesta a incidentes de seguridad	SÍ	Procedimiento de contención tras infecciones por malware.	MSPI / SGSI
A.5.27	Aprendizaje derivado de incidentes de seguridad	SÍ	Retroalimentación para ajustar políticas tras un incidente.	MSPI / SGSI
A.5.28	Recopilación de evidencia	NO	Excluido. La custodia forense digital legal es gestionada por Jurídico / TI central.	Alcance Operativo
A.5.29	Seguridad en la interrupción de la operación	SÍ	Garantía de ventas mediante canales alternos manuales/contingencia.	Riesgo R36
A.5.30	Preparación de las TIC para la continuidad del negocio	NO	Excluido. La infraestructura base es gestionada por TI central.	Alcance Operativo
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	SÍ	Mapeo de obligaciones normativas en materia de comercio.	MSPI / SGSI
A.5.32	Derechos de propiedad intelectual	NO	Excluido. El control de licencias corporativas es administrado por TI central.	Alcance Operativo
A.5.33	Protección de registros	SÍ	Protección de pedidos, contratos e historial de facturación.	Riesgo R01
A.5.34	Protección de datos y privacidad de datos personales	SÍ	Cumplimiento estricto de Hábeas Data en la base de clientes.	Ley 1581 / R01

A.5.35	Revisión independiente de la seguridad	SÍ	Auditorías periódicas de cumplimiento al proceso comercial.	MSPI / SGSI
A.5.36	Cumplimiento de políticas y normas de seguridad	SÍ	Verificación del acatamiento de lineamientos en ventas.	MSPI / SGSI
A.5.37	Procedimientos operativos documentados	SÍ	Manuales de uso seguro para sistemas de cotización y ventas.	MSPI / SGSI
2. Controles sobre Personas (A.6.1 - A.6.8)				
A.6.1	Selección de personal	SÍ	Verificación de antecedentes de ejecutivos y asesores comerciales.	MSPI / SGSI
A.6.2	Términos y condiciones de empleo	SÍ	Inclusión de cláusulas de confidencialidad en contratos de trabajo.	MSPI / SGSI
A.6.3	Concienciación, educación y formación en seguridad	SÍ	Capacitación continua en phishing e ingeniería social para ventas.	MSPI / SGSI
A.6.4	Proceso disciplinario	SÍ	Sanciones por fuga inapropiada de información confidencial.	MSPI / SGSI
A.6.5	Responsabilidades tras la terminación o cambio de empleo	SÍ	Firma de compromiso de no divulgación de clientes al retirarse.	MSPI / SGSI
A.6.6	Acuerdos de confidencialidad o no divulgación (NDA)	SÍ	Firma formal de NDA para el manejo de secretos comerciales.	Ley 1581 / R01
A.6.7	Trabajo remoto	SÍ	Políticas de seguridad para teletrabajo y asesores en campo.	MSPI / SGSI
A.6.8	Notificación de eventos de seguridad de la información	SÍ	Canal obligatorio de reporte para extravío de dispositivos o fraudes.	MSPI / SGSI
3. Controles Físicos (A.7.1 - A.7.14)				
A.7.1	Perímetros de seguridad física	NO	Excluido. La fuerza de ventas es móvil y no gestiona sedes.	Operación Campo
A.7.2	Entrada física	NO	Excluido. Mantenido bajo la infraestructura central corporativa.	Operación Campo
A.7.3	Aseguramiento de oficinas, despachos y recursos	SÍ	Protección básica de archivos físicos y facturación comercial.	MSPI / SGSI
A.7.4	Monitoreo de la seguridad física	NO	Excluido. No aplica a ventas ambulantes/rurales de campo.	Operación Campo
A.7.5	Protección contra amenazas físicas y ambientales	SÍ	Resguardo de portátiles y contratos ante lluvias o humedad en campo.	MSPI / SGSI
A.7.6	Trabajo en áreas aseguradas	NO	Excluido. El personal comercial no opera en zonas de alta restricción.	Operación Campo
A.7.7	Escritorio y pantalla limpios	SÍ	Bloqueo automático de pantalla y bloqueo de carpetas físicas.	Riesgos R20, R22
A.7.8	Emplazamiento y protección de equipos	SÍ	Seguridad física de portátiles corporativos en viajes comerciales.	MSPI / SGSI
A.7.9	Seguridad de los activos fuera de las instalaciones	SÍ	Norma de custodia de celulares y laptops en vehículos de ventas.	MSPI / SGSI
A.7.10	Medios de almacenamiento reutilizables	SÍ	Control del uso de memorias USB en la extracción de listas.	MSPI / SGSI
A.7.11	Suministros de servicio (Energía/Agua)	SÍ	Uso de reguladores y power banks para dispositivos en ruta.	Riesgo R21
A.7.12	Seguridad del cableado	NO	Excluido. La conectividad en ventas se realiza por red móvil o Wi-Fi.	Operación Campo
A.7.13	Mantenimiento de equipos	SÍ	Mantenimiento preventivo periódico de portátiles comerciales.	Riesgo R20
A.7.14	Disposición o reciclaje seguro de equipos	SÍ	Borrado seguro e higienización de discos antes de dar de baja un equipo.	MSPI / SGSI
4. Controles Tecnológicos (A.8.1 - A.8.34)				

A.8.1	Dispositivos de usuario final (Endpoint Security)	SÍ	Cifrado de disco (BitLocker) y control centralizado en portátiles.	Riesgo R12
A.8.2	Derechos de acceso privilegiado	SÍ	Restricción de permisos de administrador en laptops de ejecutivos.	MSPI / SGSI
A.8.3	Restricción de acceso a la información	SÍ	Segmentación de vistas en el ERP según el perfil de ventas.	Riesgo R02
A.8.4	Acceso al código fuente	NO	Excluido. Se utiliza software comercial sin acceso a código fuente.	Tipo de Software
A.8.5	Autenticación segura (MFA)	SÍ	Doble factor de autenticación obligatorio para correo y ERP.	MSPI / SGSI
A.8.6	Gestión de capacidad	SÍ	Monitoreo del almacenamiento en la nube comercial.	MSPI / SGSI
A.8.7	Protección contra código malicioso (Antivirus/EDR)	SÍ	Antivirus corporativo centralizado en todos los endpoints.	MSPI / SGSI
A.8.8	Gestión de vulnerabilidades técnicas	SÍ	Instalación de parches de seguridad en el sistema operativo.	Riesgo R13
A.8.9	Gestión de configuración	SÍ	Estandarización de la imagen del sistema operativo en ventas.	MSPI / SGSI
A.8.10	Eliminación de información	SÍ	Procedimientos de borrado definitivo de datos temporales.	Ley 1581 / SGSI
A.8.11	Enmascaramiento de datos	SÍ	Ocultamiento parcial de datos sensibles en reportes públicos.	Ley 1581 / R01
A.8.12	Prevención de fuga de datos (DLP)	SÍ	Reglas para evitar el reenvío masivo de clientes a correos personales.	Riesgo R01
A.8.13	Respallos de información (Backups)	SÍ	Copias de seguridad automáticas en la nube para el ERP/CRM.	Riesgo R03
A.8.14	Redundancia de las instalaciones de procesamiento de información	SÍ	Sistemas redundantes garantizados por el proveedor de nube.	Riesgo R03
A.8.15	Registros de actividad (Logging)	SÍ	Auditoría de inicios de sesión y cambios en pedidos de venta.	MSPI / Ley 1273
A.8.16	Monitoreo de actividades	SÍ	Supervisión de picos inusuales de descarga de archivos.	MSPI / SGSI
A.8.17	Sincronización de relojes	SÍ	Sincronización automática de hora (NTP) para validez de logs.	MSPI / SGSI
A.8.18	Uso de programas de utilidad con privilegios	SÍ	Restricción de herramientas de diagnóstico técnico en laptops.	MSPI / SGSI
A.8.19	Instalación de software en sistemas en producción	SÍ	Prohibición de instalación de software no autorizado.	MSPI / SGSI
A.8.20	Seguridad en las redes	SÍ	Uso de VPN corporativa para conexiones desde redes públicas.	MSPI / SGSI
A.8.21	Seguridad de los servicios de red	SÍ	Protocolos cifrados (HTTPS/TLS) para el portal comercial.	Riesgo R36
A.8.22	Segmentación de redes	SÍ	Aislamiento de la VLAN comercial de la red de invitados.	MSPI / SGSI
A.8.23	Filtrado web	SÍ	Bloqueo de acceso a sitios maliciosos o no laborales.	MSPI / SGSI
A.8.24	Uso de criptografía	SÍ	Cifrado de datos en tránsito y almacenamiento para cotizaciones.	MSPI / SGSI
A.8.25	Ciclo de vida de desarrollo seguro	NO	Excluido. No se desarrolla código fuente en la empresa.	Tipo de Software
A.8.26	Requisitos de seguridad de las aplicaciones	SÍ	Evaluación de seguridad previa a la compra del CRM comercial.	MSPI / SGSI
A.8.27	Principios de arquitectura e ingeniería de sistemas seguros	NO	Excluido. La arquitectura es administrada por el proveedor SaaS.	Tipo de Software

A.8.28	Codificación segura	NO	Excluido. Sin programación ni desarrollo de código propio.	Tipo de Software
A.8.29	Pruebas de seguridad en el desarrollo y aceptación	NO	Excluido. Pruebas a cargo del fabricante comercial.	Tipo de Software
A.8.30	Desarrollo subcontratado	NO	Excluido. No se contrata fábrica de software a la medida.	Tipo de Software
A.8.31	Separación de entornos de desarrollo, prueba y producción	NO	Excluido. El software SaaS se adquiere directamente en producción.	Tipo de Software
A.8.32	Gestión de cambios	SÍ	Procedimiento para solicitar cambios de configuración en ERP.	MSPI / SGSI
A.8.33	Información sobre pruebas	NO	Excluido. No se emplean bases reales en entornos de prueba.	Tipo de Software
A.8.34	Protección de los sistemas de información durante las pruebas	SÍ	Evitar la ejecución de pruebas invasivas sobre la base comercial activa.	MSPI / SGSI

Fuente. elaboración propia basada en la propuesta de diseño para el área comercial bajo la NTC-ISO/IEC 27001 (2022) y el marco MSPI - MinTIC.

6.14 Vinculación Estratégica para la Futura Fase de Implementación

La propuesta de esta Declaración de Aplicabilidad (SoA) deja sentadas las bases para que la organización desarrolle la posterior fase de ejecución e implementación real:

- **Modelo Guía para la Totalidad de Riesgos:** Los 74 controles declarados como aplicables sirven de patrón estructurado. Aunque el presente trabajo ilustra la metodología sobre 10 eventos prioritarios (R01, R02, R03, R12, R13, R20, R21, R22, R36 y R37), la guía metodológica permite a Bioconcentrados S.A.S. extender este mismo esquema de control a la totalidad de los 37 riesgos del área comercial.
- **Alineación con Marcos de Cumplimiento:** Articula el diseño con la Ley 1581 de 2012 (Hábeas Data) y la Ley 1273 de 2009 (Delitos Informáticos en Colombia) mediante controles como A.5.34, A.6.6, A.8.11 y A.8.12.
- **Optimización de Recursos en la Implementación:** La fundamentación de las 19 exclusiones orienta a la alta gerencia para no presupuestar recursos en controles de desarrollo informático o seguridad física pesada que no corresponden al modelo comercial de la empresa.

7 Conclusiones

Se identificaron y valoraron los activos de información críticos del proceso comercial según los criterios de Confidencialidad, Integridad y Disponibilidad (CID), estableciendo la línea base para la evaluación de amenazas y vulnerabilidades.

Mediante la gestión de la NTC-ISO 31000:2018 y la ISO 27001:2022, se ponderó el riesgo inherente ($RI = P \times I$) sobre la muestra representativa de escenarios comerciales, priorizando las amenazas de mayor impacto sobre la base de clientes y los sistemas ERP/CRM.

Con el algoritmo de efectividad del marco MSPI (MinTIC), se estructuró la propuesta del Plan de Tratamiento de Riesgos (PTR), demostrando cuantitativamente que la asignación de controles atenuadores reubica el riesgo residual (RR) en niveles de aceptabilidad gerencial.

Se evaluaron los 93 controles del Anexo A de la NTC-ISO/IEC 27001:2022, determinando una aplicabilidad del 79.6% (74 controles incluidos) para blindar la operación y garantizar el cumplimiento de la Ley 1581 de 2012 (Hábeas Data). Asimismo, se fundamentó la exclusión del 20.4% (19 controles) correspondientes a desarrollo de software y seguridad industrial, optimizando la asignación de recursos.

La propuesta de diseño desarrollada constituye una guía metodológica integral. La articulación de las matrices, los algoritmos de atenuación de MinTIC y el SoA dejan sentadas las bases para que la organización, en su posterior fase de ejecución e implementación real, extienda este mismo modelo estandarizado a la totalidad de los activos y eventos de riesgo del área comercial de Bioconcentrados S.A.S.

8 Recomendaciones

Despliegue y Replicación Metodológica: Utilizar la presente arquitectura de diseño como guía maestra para escalar la identificación y valoración de riesgos a la totalidad de los 37 eventos del inventario comercial, asegurando que la metodología de atenuación del algoritmo MSPI se aplique de forma homogénea en la posterior fase de ejecución.

Formalización de Políticas y SoA: Presentar ante la alta gerencia y el comité directivo la matriz del Statement of Applicability (SoA) y las políticas asociadas a la Ley 1581 de 2012 (Hábeas Data), con el fin de institucionalizar las decisiones de inclusión (74 controles) y exclusión (19 controles) antes de iniciar la asignación de presupuestos.

Programa de Concienciación y Cultura Digital: Diseñar una ruta de capacitación continua enfocada en la fuerza de ventas (presencial y en campo), priorizando la prevención de riesgos humanos críticos como el phishing, la ingeniería social y el manejo seguro de dispositivos móviles fuera de las instalaciones.

Evolución del Plan de Tratamiento (PTR): Establecer un cronograma de implementación por fases para las salvaguardas tecnológicas clave (como la masificación del cifrado BitLocker, el doble factor de autenticación MFA y la gestión centralizada de backups en la nube), garantizando que los riesgos residuales se mantengan en los niveles de aceptabilidad definidos.

Mantenimiento y Auditoría Periódica: Programar revisiones semestrales sobre el inventario de activos comerciales y la matriz de aplicabilidad del Anexo A, adaptando el SGSI ante eventuales cambios en las herramientas tecnológicas (ERP/CRM) o nuevas regulaciones del sector agroindustrial en Colombia.

9 Referencias Bibliográficas

- Alarcon Posso, A., & Tobón Quiceno, L. L. (2021). Documentación del sistema de gestión de la seguridad de la información del laboratorio clínico patológico López Correa bajo los requisitos de la norma NTC/ISO/IEC 27001: 2013.
- Allianz. (2026). *Allianz Risk Barometer: Identifying the major business risks for 2026*.
<https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
- Bioconcentrados S.A.S. (2026). *Bioconcentrados*. <https://www.bioconcentrados.com>
- Centro de Investigación y Estudios Estratégicos [CIEE]. (2024). *Gobernanza digital y ciberseguridad: Un análisis conceptual y relacional*.
<https://doi.org/10.6028/NIST.CSWP.29>
- 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. 48.583. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
- Cortés Malagón, J. C., & Pulido Espinosa, J. A. (2023). Diseño de un sistema de gestión de seguridad de la información (SGSI) para los procesos críticos de summum project basado en la norma NTC-ISO-IEC-27001: 2022.
- Fierro Garcia, M. A. (2026). Análisis de las vulnerabilidades en la ciberseguridad colombiana ante el espionaje digital: un enfoque en la protección de datos personales y corporativos.
<https://repository.unad.edu.co/handle/10596/80837>
- Galarza-Sánchez, P. C., Herrera-Ramírez, C. D., & Borja-Almeida, L. G. (2025). Seguridad informática y prevención de ataques cibernéticos en sistemas organizacionales. *Revista Científica Enfoques del Conocimiento*, 2(3), 49-73.
- Garavito Castro, V. D. J. G., Nova, M. A. M., & Herrera, H. M. H. (2025). Propuesta de Controles Organizacionales en Seguridad de la Información y Ciberseguridad Basados en ISO/IEC 27001: 2022 y 27002: 2022 para Ingenierías y Servicios SAS. *Apuntes de Ciencia e Ingeniería*, 4(2). DOI: <https://doi.org/10.37511/apuntesci.v4n2a5>

- Granada Leguizamo, A. (2024). Implementación de un sistema de gestión de seguridad de la información con base en los lineamientos definidos en la NTC-ISO-IEC-27001: 2022 seguridad de la información, ciberseguridad y protección de la privacidad.
<https://hdl.handle.net/11059/15679>
- Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.
- Herrera Mosquera, A. E. (2025). Implementación Centralizada de Control de Acceso a Información de Identificación Personal: requisitos de Control de Acceso para la Recolección, Procesamiento y Almacenamiento de Información de Identificación Personal. <https://bibdigital.epn.edu.ec/handle/15000/26515>
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2022). *Sistemas de gestión de la seguridad de la información: Requisitos (NTC-ISO/IEC 27001:2022)*. ICONTEC.
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad: Sistema de gestión de seguridad de la información (NTC-ISO/IEC 27001:2022)*. ICONTEC.
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2018). *Gestión del riesgo: Principios y directrices (NTC-ISO 31000:2018)*. ICONTEC.
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2018). *Gestión del riesgo: Principios y directrices (NTC-ISO 31000:2018)*. ICONTEC.
- International Organization for Standardization [ISO] & International Electrotechnical Commission [IEC]. (2022). *Information security, cybersecurity and privacy protection—Information security controls (ISO/IEC 27002:2022)*. ISO.
- Kiteworks. (2024). *¿Qué es la gobernanza de seguridad de la información en ciberseguridad?*
<https://www.kiteworks.com/es/gestion-de-riesgos-de-ciberseguridad/gobernanza-seguridad-en-ciberseguridad/>

- López Garcés, J. J., & Martínez Ojeda, J. M. (2021). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma NTC ISO/IEC 27001: 2013 en el área de desarrollo de la empresa Ikatech Solutions.
- Marreros, J., Acosta, D., & Mendoza, A. (2024). Mecanismos de seguridad de la información en una organización: una revisión sistemática. *Revista Científica Ciencias Ingenieriles*, 4(1), 79-90.
- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2026). *Estrategia de Gobierno Digital: Modelo de Seguridad y Privacidad de la Información (MSPI)—Lineamiento marco*.
<https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>
- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2021). *Estrategia de Gobierno Digital: Modelo de Seguridad y Privacidad de la Información (MSPI)—Herramienta de autodiagnóstico de línea base ISO/IEC 27001:2022* [Archivo Excel].
<https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>
- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2021). *Estrategia de Gobierno Digital: Modelo de Seguridad y Privacidad de la Información (MSPI)—Lineamientos para el inventario y clasificación de activos de información e infraestructura crítica cibernética nacional*.
https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401773_recurso_1.pdf/
- National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Ospina Garcia, J. D. (2026). Evaluación de Riesgos y Propuesta de Controles Críticos en Centros Médicos: Un Enfoque Alineado con la Serie de Normas ISO/IEC-27000 y la ISO/IEC 27001: 2022.

Paez Gabriunas, I. L. O. P., Rangel, J. M. S., Gauthier-Umaña, V., Romero, R. A. M., & Rivera, L. (2022). Transformación digital en las organizaciones. DOI: 10.12804/urosario9789587848366

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Diario Oficial No. 48.834. <http://www.suin-juriscol.gov.co/viewDocument.asp?id=1255860>

Procuraduría General de la Nación. (2025). *Procedimiento: Identificación y clasificación de activos de información*. https://apps.procuraduria.gov.co/portal/media/file/modulo_calidad/mapa_proceso//1710_DO-P-11%20IDENTIFICACI%C3%93N%20Y%20CLASIFICACI%C3%93N%20DE%20ACTIVOS%20DE%20INFORMACI%C3%93N.pdf

Robles Puentes, H. A. R. (2025). Desarrollo de un modelo de ciberseguridad basado en SCRUM para MiPyMEs del Huila, asegurando su viabilidad y escalabilidad. <https://repository.unad.edu.co/handle/10596/77829>

Rodríguez Arteaga, G. F. (2024). Analizar las políticas y los controles básicos de seguridad de la información en función de las nuevas necesidades que tienen las Pymes del sector comercial en tiempos COVID-19. <https://repository.unad.edu.co/handle/10596/56391>

Rodríguez Diaz, J. A., & Ruiz Rojas, Y. A. (2021). Diseño de un sistema de gestión de seguridad de la información para el área de talento humano de la secretaria de educación de Fusagasugá basado en la norma NTC-IEC ISO 27001: 2013. <http://repository.unipiloto.edu.co/handle/20.500.12277/9854>

Rubio Contreras, F. D. (2025). Ciberseguridad para usuarios “no técnicos” en sistemas. <https://doi.org/10.60909/bdigital/handle.001.14023>

Valencia Duque, F. J. (2021). Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. <https://repositorio.unal.edu.co/handle/unal/80158>

10 Anexos

Anexo A

Evaluación del nivel de cumplimiento

Sección A5. Controles Organizacionales					
Código	Control Anexo A	Criterio Específico de Evaluación en Bioconcentrados SAS	Calificación MinTIC	Nivel de Madurez	Justificación del Diagnóstico y Brecha Identificada
5.1	Políticas para la seguridad	¿Existen políticas escritas y aprobadas para la protección de la información?	0	Inexistente	Total falta de proceso reconocible. Las pautas de trabajo se manejan de manera verbal.
5.2	Funciones y responsabilidades	¿Los contratos del personal especifican sus deberes en ciberseguridad?	20	Inicial	Se asume la responsabilidad tácitamente, pero sin manuales ni documentos formalizados.
5.3	Segregación de funciones	¿Se separan las funciones de toma de pedidos, aprobación de crédito y facturación?	40	Repetible	Sigue un patrón regular por costumbre de trabajo, pero diferentes vendedores ejecutan la toma de pedidos de formas distintas.
5.4	Responsabilidades de dirección	¿La gerencia exige explícitamente el cumplimiento de pautas de seguridad?	20	Inicial	Acción reactiva. La gerencia prioriza metas de venta sin exigir lineamientos de seguridad escritos.
5.5	Contacto con autoridades	¿Existen canales definidos para reportar incidentes legales o brechas ante la SIC?	0	Inexistente	No se aplican controles ni existe un protocolo institucional de contacto formal.
5.6	Contacto con grupos de interés	¿Se participa en foros o redes de ciberseguridad del sector agroindustrial?	0	Inexistente	Total falta de interacción o participación en grupos de interés en seguridad de la información.
5.7	Inteligencia sobre amenazas	¿Se analizan las modalidades de fraude y suplantación telefónica en la zona rural?	20	Inicial	Se comentan casos entre asesores de forma informal y reactiva cuando ocurren fraudes en la zona.
5.8	Seguridad en gestión de proyectos	¿Se contemplan requisitos de seguridad al habilitar nuevos canales informáticos de venta?	0	Inexistente	Las iniciativas comerciales digitales se adoptan por necesidad operativa sin análisis de riesgo.
5.9	Inventario de activos	¿Se cuenta con un inventario formalizado y valorado de bases de datos de clientes?	0	Inexistente	Total falta de control. Cada asesor conserva sus listas de contactos en cuadernos o teléfonos propios.
5.10	Uso aceptable de activos	¿Existen normas para el uso seguro de WhatsApp y celulares corporativos?	20	Inicial	El uso depende de cada individuo de manera empírica, sin directrices formales.

5.11	Devolución de activos	¿Existen protocolos para recuperar equipos y datos al retirar un vendedor?	20	Inicial	Práctica reactiva. Se devuelve el teléfono físico, pero sin borrado seguro de datos.
5.12	Clasificación de información	¿Se etiquetan los documentos comerciales según su nivel de sensibilidad?	0	Inexistente	No se aplican controles. Todos los archivos y listas de precios se manejan abiertamente.
5.13	Etiquetado de información	¿Se cuenta con un procedimiento para marcar archivos digitales y físicos?	0	Inexistente	Total ausencia de marcas de agua o símbolos de clasificación en la documentación.
5.14	Transferencia de información	¿Se utilizan canales seguros para enviar presupuestos a distribuidores?	20	Inicial	Envío informal de archivos por correo o mensajería abierta sin cifrado ni claves.
5.15	Control de acceso	¿El acceso a carpetas compartidas de cartera de clientes está restringido?	40	Repetible	Existen claves en el servidor que siguen patrones regulares, pero se comparten entre personas y hay riesgo de error.
5.16	Gestión de identidades	¿Cada asesor comercial cuenta con una cuenta de usuario única e intransferible?	60	Efectivo	El correo corporativo se encuentra documentado, comunicado y asignado formalmente a cada funcionario.
5.17	Información de autenticación	¿Existen políticas de contraseñas seguras y renovaciones periódicas?	20	Inicial	Las claves son simples y su actualización depende de la voluntad del usuario, sin forzado automático.
5.18	Derechos de acceso	¿Se revisan y revocan los permisos de acceso al personal que se retira?	20	Inicial	Proceso reactivo. La cancelación de permisos se realiza días después del retiro tras solicitudes informales.
5.19	Seguridad con proveedores	¿Se exigen acuerdos de seguridad a los terceros de soporte de software?	0	Inexistente	No se aplican controles. Los contratos con proveedores omiten cláusulas de seguridad.
5.20	Seguridad en acuerdos de terceros	¿Se establecen salvaguardas en los contratos con distribuidores?	0	Inexistente	Los acuerdos comerciales se limitan a metas de venta y plazos de pago.
5.21	Cadena de suministro TIC	¿Se evalúa la seguridad de las herramientas tecnológicas adquiridas para ventas?	0	Inexistente	Adquisición comercial. Se contrata software sin auditar su postura de seguridad.
5.22	Monitoreo de proveedores	¿Se audita periódicamente el cumplimiento de seguridad de los proveedores TIC?	0	Inexistente	No hay métricas, revisiones periódicas ni auditorías de desempeño informático.
5.23	Servicios en la nube	¿Se evalúan los riesgos de seguridad al	20	Inicial	Se utiliza almacenamiento en la nube de forma esporádica sin

		almacenar carpetas en servicios cloud?			configuraciones de seguridad.
5.24	Gestión de incidentes	¿Existe un plan para actuar ante fuga de clientes o ataques de phishing?	0	Inexistente	Total ausencia de plan. Las fallas de seguridad se atienden de manera improvisada.
5.25	Evaluación de eventos	¿Se cuenta con un procedimiento para clasificar eventos de seguridad?	0	Inexistente	No existe registro ni procedimiento formal de evaluación técnica de fallas.
5.26	Respuesta a incidentes	¿Existen protocolos documentados para contener brechas en la data comercial?	0	Inexistente	No existen roles ni procedimientos de respuesta rápida ante incidentes.
5.27	Aprendizaje de incidentes	¿Se documentan los fraudes comerciales para actualizar los controles?	0	Inexistente	Los incidentes o fraudes no se registran ni analizan para generar lecciones aprendidas.
5.28	Recolección de evidencia	¿Se conservan pruebas forenses en caso de fraudes telefónicos o mensajería?	0	Inexistente	Se borran o no se custodian los chats y correos que respaldan transacciones sospechosas.
5.29	Interrupción operativa	¿Se garantiza la protección de datos si los sistemas caen durante las ventas?	20	Inicial	Se toma nota en papel por costumbre cuando falla el sistema, sin resguardo posterior.
5.30	Continuidad de TIC	¿Existen planes de respaldo para continuar vendiendo ante caídas del sistema?	20	Inicial	Dependencia de procedimientos manuales imprecisos creados empíricamente por los vendedores.
5.31	Requisitos legales	¿Se identifican las obligaciones legales aplicables a la data (Ley 1581)?	40	Repetible	Los avisos de privacidad siguen un patrón regular, pero la forma de aplicarlos en campo varía según el asesor.
5.32	Propiedad intelectual	¿Se protegen las fórmulas de alimentos frente a accesos de ventas?	60	Efectivo	Las fórmulas de producción están restringidas en el sistema ERP y aisladas efectivamente.
5.33	Protección de registros	¿Se garantiza el almacenamiento seguro de registros de ventas y pedidos?	20	Inicial	Los archivos digitales y físicos se conservan por costumbre sin tabla de retención.
5.34	Protección de datos personales	¿Se aplica una política formal de datos en la toma de pedidos rurales?	20	Inicial	Práctica informal. No se solicita autorización escrita o grabada de hábeas data.
5.35	Revisión independiente	¿Se realizan evaluaciones o auditorías externas sobre la seguridad de ventas?	0	Inexistente	El proceso de ventas jamás ha sido sometido a revisiones de seguridad.
5.36	Cumplimiento de políticas	¿La gerencia supervisa periódicamente que se apliquen pautas de seguridad?	0	Inexistente	Al no existir políticas formalizadas, no se efectúan verificaciones de cumplimiento.

5.37	Documentación operativa	¿Los procedimientos de atención al cliente están documentados con seguridad?	0	Inexistente	Total ausencia de manuales operativos que incorporen salvaguardas de ciberseguridad.
Sección A6. Controles de Personas					
Código	Control Anexo A	Criterio Específico de Evaluación en Bioconcentrados SAS	Calificación MinTIC	Nivel Madurez	Justificación del Diagnóstico y Brecha Identificada
6.1	Selección de personal (<i>Screening</i>)	¿Se realizan verificaciones de antecedentes de seguridad antes de contratar asesores comerciales?	60	Efectivo	Gestión Humana valida antecedentes judiciales y referencias laborales de forma documentada y efectiva, aunque sin evaluar competencias de ciberseguridad.
6.2	Términos y condiciones del empleo	¿Los contratos de trabajo definen explícitamente las responsabilidades en seguridad de la información?	20	Inicial	Existen cláusulas genéricas de confidencialidad en los contratos, sin especificar la custodia de la cartera de clientes ni bases de precios de forma explícita.
6.3	Toma de conciencia y formación en seguridad	¿El personal comercial recibe capacitaciones para detectar ingeniería social o engaños telefónicos en zonas rurales?	0	Inexistente	Total falta de proceso. El equipo de ventas jamás ha recibido formación ni sensibilización en ciberseguridad o prevención de fraudes.
6.4	Proceso disciplinario	¿Existe un régimen de sanciones formalizado e informado para el personal que viole la seguridad de la información?	20	Inicial	Se aplica el Reglamento Interno de Trabajo genérico de manera reactiva, sin tipificar infracciones específicas sobre datos digitales o comerciales.
6.5	Responsabilidades tras la terminación o cambio	¿Se revocan accesos y se exige el compromiso de confidencialidad al personal comercial que se retira?	20	Inicial	Desafiliación de cuentas de correo de forma empírica tras el retiro, sin firma de compromisos formales de no divulgación posteriores.
6.6	Acuerdos de confidencialidad o no divulgación (NDA)	¿Se firman acuerdos de confidencialidad dedicados con	0	Inexistente	No se suscriben acuerdos de no divulgación (NDA)

		vendedores que gestionan precios y clientes?			específicos para la protección de la información estratégica del proceso de ventas.
6.7	Trabajo remoto y trabajo fuera de la oficina	¿Existen normas operativas de seguridad para la toma de pedidos y custodia de móviles en rutas rurales?	20	Inicial	El trabajo en campo se realiza a criterio individual del asesor de manera empírica, sin directrices escritas para proteger dispositivos fuera de la sede.
6.8	Reporte de eventos de seguridad	¿Existe un procedimiento sencillo para que el equipo comercial reporte el extravío de un móvil o intentos de fraude?	20	Inicial	Reporte verbal e informal ante el jefe de ventas cuando se pierde un equipo, sin contar con un canal escrito ni formulario de registro.

Sección A7. Controles Físicos

Código	Control Anexo A	Criterio Específico de Evaluación en Bioconcentrados SAS	Calificación MinTIC	Nivel de Madurez	Justificación del Diagnóstico y Brecha Identificada
7.1	Perímetros de seguridad física	¿Las instalaciones cuentan con barreras físicas de acceso?	60	Efectivo	La planta agroindustrial cuenta con cerramiento y control de portería general documentado y efectivo, aunque sin barrera exclusiva en ventas.
7.2	Ingreso físico	¿Se registra y controla el ingreso de visitantes al área comercial?	40	Repetible	Existe registro de entrada a planta que sigue un patrón regular, pero los visitantes transitan libremente por los escritorios del área de ventas.
7.3	Aseguramiento de recintos e instalaciones	¿Las dependencias comerciales se mantienen cerradas fuera del horario laboral?	60	Efectivo	Las oficinas y carpetas de archivo se mantienen cerradas con llave al finalizar la jornada de forma documentada.
7.4	Monitoreo de seguridad física	¿Existen sistemas de videovigilancia (CCTV) en las instalaciones de la empresa?	60	Efectivo	Sistema CCTV operativo y monitoreado en accesos principales y pasillos de la empresa.
7.5	Protección contra amenazas ambientales	¿Los expedientes físicos de clientes están protegidos	20	Inicial	Almacenamiento en carpetas de cartón expuestas al polvo de la planta agroindustrial y

		contra incendios o humedad?			sin sistemas especializados de extinción.
7.6	Trabajo en áreas seguras	¿Se prohíbe fotografiar documentos de crédito o listados de precios en escritorios?	0	Inexistente	Total falta de proceso. No hay restricción ni políticas sobre el uso de cámaras de celulares en escritorios ni sobre pizarras comerciales.
7.7	Escritorio limpio y pantalla limpia	¿Se bloquean pantallas y guardan documentos al ausentarse del puesto?	20	Inicial	Práctica informal de bloqueo de pantalla y limpieza de escritorio que depende del hábito individual de cada funcionario.
7.8	Emplazamiento y protección de equipos	¿Los equipos de cómputo están protegidos contra oscilaciones eléctricas?	60	Efectivo	Equipos protegidos con UPS y reguladores en la sede principal de forma efectiva.
7.9	Seguridad de activos fuera de instalaciones	¿Se resguardan los celulares corporativos durante las visitas a rutas rurales?	20	Inicial	Custodia de celulares corporativos en ruta rural sujeta al cuidado personal del asesor sin guayas ni fundas seguras.
7.10	Medios de almacenamiento	¿Los discos externos o USB con datos comerciales se custodian de forma segura?	0	Inexistente	Memorias USB y medios extraíbles se conservan en cajones sin llave sin control de custodia ni registro.
7.11	Suministros de soporte	¿Se cuenta con respaldo eléctrico ante cortes de luz durante la toma de pedidos?	60	Efectivo	Planta eléctrica general de respaldo en la empresa para garantizar continuidad operacional ante cortes de luz.
7.12	Seguridad del cableado	¿El cableado de red y telefonía comercial está protegido contra manipulaciones?	20	Inicial	Cableado a la vista en la oficina comercial, expuesto a desconexiones accidentales o interferencias mecánicas.
7.13	Mantenimiento de equipos	¿Se realiza mantenimiento preventivo periódico a los computadores comerciales?	60	Efectivo	Mantenimiento preventivo de computadores ejecutado periódicamente por el área de TIC de forma documentada.
7.14	Disposición segura de equipos	¿Se aplica borrado seguro o destrucción de discos en equipos dados de baja?	0	Inexistente	Baja de equipos almacenada en bodega sin borrado seguro de bajo nivel ni protocolo

					de destrucción de discos duros.
Sección A8. Controles Tecnológicos					
Código	Control Anexo A	Criterio Específico de Evaluación en Bioconcentrados SAS	Calificación MinTIC	Nivel de Madurez	Justificación del Diagnóstico y Brecha Identificada
8.1	Dispositivos de usuario final	¿Existen configuraciones estándar para computadores y celulares corporativos de ventas?	20	Inicial	Dispositivos con antivirus básico, pero los asesores pueden instalar aplicaciones sin restricción por directiva.
8.2	Privilegios de acceso	¿Los derechos en el software comercial se limitan estrictamente al rol de cada usuario?	60	Efectivo	Derechos de acceso en el sistema ERP restringidos por perfil de usuario de forma documentada y efectiva.
8.3	Restricción de acceso a la información	¿Se limita el acceso a las listas de precios estratégicas y márgenes de ganancia?	20	Inicial	Acceso a plantillas de cotización y precios en carpetas compartidas sin cifrado ni restricción estricta.
8.4	Acceso al código fuente	¿Se protege el código fuente o scripts de bases de datos de la empresa?	0	Inexistente	Total falta de proceso. Sin control de versiones ni protección sobre scripts de bases de datos.
8.5	Autenticación segura	¿Se exige autenticación robusta o doble factor (MFA) para acceder a los sistemas?	0	Inexistente	Autenticación simple mediante usuario y clave sin doble factor (MFA) en correo ni en sistemas.
8.6	Gestión de capacidad	¿Se monitorea la capacidad de almacenamiento del servidor comercial?	20	Inicial	Revisión de capacidad de almacenamiento únicamente cuando el servidor genera alertas de espacio o lentitud.
8.7	Protección contra código malicioso	¿Los equipos cuentan con licencias activas y actualizadas de software antivirus?	60	Efectivo	Software antivirus con licencia activa en computadores de oficina, pero ausente en móviles de ruta rural.
8.8	Gestión de vulnerabilidades técnicas	¿Se identifican y corrigen periódicamente las vulnerabilidades informáticas?	0	Inexistente	Sin escaneos ni análisis de vulnerabilidades técnicas en la infraestructura comercial de la empresa.

8.9	Gestión de la configuración	¿Existen plantillas de configuración segura (<i>Hardening</i>) para servidores y equipos?	0	Inexistente	Sin plantillas de configuración segura (<i>Hardening</i>) para equipos y servidores de ventas.
8.10	Eliminación de información	¿Se utiliza software de borrado seguro para eliminar bases de datos obsoletas?	0	Inexistente	Eliminación de archivos mediante la papelera de reciclaje estándar sin borrado seguro de bajo nivel.
8.11	Enmascaramiento de datos	¿Se ocultan o enmascaran los números de cédula o datos financieros de clientes?	0	Inexistente	Despliegue de datos de clientes, contratos y cédulas en texto plano sin enmascaramiento.
8.12	Prevención de fuga de datos (DLP)	¿Existen herramientas que bloqueen el envío masivo de datos a USB o correos personales?	0	Inexistente	Sin herramientas de prevención de fuga de datos (DLP) ni bloqueos a USB/correos personales.
8.13	Respaldo de información (<i>Backup</i>)	¿Se realizan copias de respaldo periódicas y automatizadas de la data comercial?	60	Efectivo	Respaldo nocturno automatizado en el servidor principal, pero sin respaldo de laptops de vendedores en campo.
8.14	Redundancia de procesamiento	¿Los sistemas informáticos de comercialización cuentan con servidores redundantes?	0	Inexistente	Servidor único para gestión comercial sin redundancia ni esquema de alta disponibilidad.
8.15	Registro de eventos (<i>Logging</i>)	¿Se generan y conservan registros de auditoría sobre quién consulta o modifica la data?	20	Inicial	Registros básicos de fecha de creación de pedidos en el ERP, sin auditoría de descargas o consultas de datos.
8.16	Actividades de monitoreo	¿Se supervisan anomalías o comportamientos inusuales en la red y cuentas comerciales?	0	Inexistente	Sin monitoreo en tiempo real ni supervisión de comportamientos anómalos en la red.
8.17	Sincronización del reloj	¿Los servidores y computadores comerciales están sincronizados con un servidor NTP?	60	Efectivo	Sincronización automática de reloj de equipos con el dominio de Active Directory de Windows.
8.18	Servicios privilegiados	¿Se restringe el uso de herramientas de mantenimiento que alteren bases de datos?	20	Inicial	Uso de herramientas de administración por soporte de TIC sin

					registro formal de autorización previa.
8.19	Instalación de software en sistemas	¿Se bloquea la instalación de programas no autorizados en los equipos comerciales?	20	Inicial	Bloqueos parciales de software por directivas de grupo no estrictas en los equipos de ventas.
8.20	Seguridad en redes	¿La red Wi-Fi empleada para pedidos está protegida de accesos no autorizados?	60	Efectivo	Red Wi-Fi corporativa protegida con clave de acceso gestionada por el área de TIC.
8.21	Servicios de red	¿Los proveedores de internet garantizan parámetros de seguridad y cifrado?	20	Inicial	Contratación de internet comercial estándar sin acuerdos de nivel de servicio (SLA) de ciberseguridad.
8.22	Segregación de redes	¿La red del área comercial se encuentra segmentada mediante VLANs respecto a otras áreas?	0	Inexistente	Red plana sin segmentación por VLANs entre planta agroindustrial, administración y ventas.
8.23	Filtrado web	¿Se restringe el acceso desde computadores comerciales a sitios web maliciosos?	20	Inicial	Filtro web básico por el antivirus local sin servidor proxy ni control centralizado de contenidos.
8.24	Uso de criptografía	¿Se exige el cifrado de archivos confidenciales que contienen ofertas comerciales enviadas?	0	Inexistente	Sin cifrado de archivos confidenciales o presupuestos enviados por correo o mensajería pública.
8.25	Ciclo de vida de desarrollo seguro	¿Se aplican criterios de seguridad al solicitar mejoras en el módulo informático de ventas?	0	Inexistente	Sin criterios de seguridad en el ciclo de vida de cambios al sistema de ventas.
8.26	Requisitos de seguridad de aplicaciones	¿Se especifican requisitos de seguridad cuando se contrata software comercial?	0	Inexistente	Adquisición de software según criterios operativos de costo sin requerimientos formales de seguridad.
8.27	Arquitectura de sistemas seguros	¿Los sistemas comerciales se diseñan bajo el principio de menor privilegio y defensa en profundidad?	0	Inexistente	Arquitectura de sistemas basada en crecimiento empírico sin principios de ingeniería segura.
8.28	Codificación segura	¿Los consultores externos aplican	0	Inexistente	Sin exigencia de prácticas de

		estándares de código seguro en los parches del sistema?			codificación segura a proveedores de desarrollo de software.
8.29	Pruebas de seguridad	¿Se ejecutan pruebas de penetración (<i>pentesting</i>) antes de lanzar actualizaciones del sistema?	0	Inexistente	Sin pruebas de penetración (<i>pentesting</i>) ni análisis de vulnerabilidades previas a producción.
8.30	Desarrollo subcontratado	¿Se supervisan las actividades de los programadores externos que modifican las bases de datos?	0	Inexistente	Acceso remoto total a proveedores de software sin supervisión ni registro de sus intervenciones.
8.31	Separación de entornos	¿Los datos reales de clientes están aislados de los entornos de prueba de software?	20	Inicial	Copia de bases de datos reales a ambientes de pruebas de forma informal por el personal de soporte.
8.32	Gestión de cambios	¿Se lleva un registro formal de autorización para cada cambio técnico en los servidores?	20	Inicial	Solicitud de cambios informáticos por correo informal sin comité formal de aprobación.
8.33	Información de pruebas	¿Se enmascaran los datos comerciales cuando se emplean en pruebas de software?	0	Inexistente	Uso de datos reales sin enmascarar en pruebas de generación de informes o facturas.
8.34	Protección en pruebas de auditoría	¿Se verifican los accesos a la red cuando se realizan revisiones o soporte informático?	20	Inicial	Revisiones de soporte en horario operativo sin aislamiento de bases de datos de ventas.

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones. MinTIC (2022). Autodiagnóstico MSPI.

Anexo B*Escala de Valoración de Controles ISO 27001:2022*

Calificación Oficial	Nivel de Madurez	Criterio de Evaluación Institucional MinTIC
0	Inexistente	Total falta de cualquier proceso reconocible. La organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
20	Inicial	1) Hay evidencia de que la organización reconoce el problema, pero no hay procesos estandarizados. La implementación depende de cada individuo y es reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos ni aplicados.
40	Repetible	Los procesos y controles siguen un patrón regular desarrollado hasta el punto en que diferentes personas siguen procedimientos distintos. No hay formación formal ni estándares. Hay dependencia en el conocimiento individual.
60	Efectivo	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección oportuna de desviaciones.
80	Gestionado	Los controles se monitorean y se miden. Es posible medir el cumplimiento de los procedimientos y tomar acciones de corrección cuando los procesos no funcionan eficientemente.
100	Optimizado	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: elaboración propia con base en Ministerio de Tecnologías de la Información y

Comunicaciones. MinTIC (2022). Autodiagnóstico MSPI.