TRABAJO DE GRADO
Opción Seminario.

Informe técnico de gestión de ciberseguridad organizacional
Caso de estudio: organización simulada agroindustrial y comercializadora

Corporación Universitaria Remington.
Facultad de Ingeniería
Especialización en Seguridad de la Información

Cristian Mauricio Piedrahita Berrocal, Rubén Darío Salas Usme.
Jorge Leonardo Ramírez Restrepo.
Seminario en Gestión de Ciberseguridad en las Organizaciones

Mayo 2026

Tabla de contenido

Resumen

El presente informe técnico analiza la gestión de ciberseguridad en una organización simulada agroindustrial y comercializadora. La operación depende de sistemas de información que soportan inventarios, despachos, facturación, nómina, comunicaciones corporativas, acceso remoto y respaldo de información. El objetivo es identificar activos críticos, relacionar amenazas y vulnerabilidades, valorar riesgos y proponer controles verificables que reduzcan la exposición frente a eventos que afecten la confidencialidad, integridad y disponibilidad de la información.

El trabajo se estructura bajo la relación personas, procesos y tecnología. Se toman como referentes la Ley 1581 de 2012, ISO/IEC 27001:2022, ISO/IEC 27005:2022, el NIST Cybersecurity Framework 2.0 y buenas prácticas de ENISA, aplicadas al contexto operativo de la organización y no como definiciones aisladas (Congreso de la República de Colombia, 2012; ENISA, 2023; ISO/IEC, 2022a, 2022b; NIST, 2024).

Los riesgos prioritarios identificados son ransomware sobre el ERP y las copias de seguridad, phishing contra usuarios con acceso a nómina o correo, compromiso de cuentas en Microsoft 365, uso indebido de credenciales privilegiadas, exposición por VPN y manipulación de registros de inventario o despacho. Para tratarlos se proponen controles de autenticación multifactor, mínimo privilegio, revisión periódica de accesos, endurecimiento de servidores, protección de endpoints, respaldo inmutable, pruebas de restauración, monitoreo de eventos, control de terceros, capacitación focalizada y respuesta formal ante incidentes. El resultado es una propuesta trazable entre activo, amenaza, vulnerabilidad, riesgo, control y riesgo residual esperado.

Palabras clave: Ciberseguridad organizacional; gestión de riesgos; activos de información; continuidad del negocio; controles de seguridad.

Marco conceptual y contextual

Marco conceptual

La seguridad de la información se entiende como la preservación de la confidencialidad, integridad y disponibilidad de la información. En una organización agroindustrial y comercializadora, estos principios tienen impacto directo: la confidencialidad protege datos personales y financieros; la integridad evita alteraciones en inventarios, nómina, facturación y despachos; y la disponibilidad permite mantener la operación logística y administrativa sin interrupciones no controladas.

ISO/IEC 27001:2022 se utiliza como marco de gestión para ordenar controles, responsabilidades, evidencias y mejora continua. En este informe no se afirma que la organización se encuentre certificada. La norma se emplea como criterio para estructurar una propuesta de gestión de seguridad de la información basada en riesgos y controles documentados (ISO/IEC, 2022a).

ISO/IEC 27005:2022 se aplica como referencia para la gestión de riesgos de seguridad de la información. Su aporte al caso consiste en exigir una relación lógica entre activo, amenaza, vulnerabilidad, probabilidad, impacto y tratamiento. Esta relación evita recomendaciones genéricas y permite justificar cada control con base en un riesgo identificable (ISO/IEC, 2022b).

El NIST Cybersecurity Framework 2.0 complementa el análisis mediante las funciones gobernar, identificar, proteger, detectar, responder y recuperar. Estas funciones permiten conectar la identificación de activos, la prevención, el monitoreo, la respuesta ante incidentes y la recuperación operativa (NIST, 2024).

La Ley 1581 de 2012 es relevante porque la organización trata datos personales de empleados, proveedores, clientes, usuarios internos y terceros logísticos. Por esta razón, los

riesgos sobre nómina, correo, ERP, repositorios documentales y accesos de terceros deben analizarse desde el cumplimiento legal y desde la continuidad operativa (Congreso de la República de Colombia, 2012).

Las guías y reportes de ENISA se usan como apoyo para reconocer amenazas actuales como ransomware, phishing, abuso de credenciales y compromiso de servicios en la nube. Su valor en este informe es contextual: ayuda a priorizar amenazas frecuentes sin sustituir el análisis propio de la organización (ENISA, 2023).

Marco contextual

La organización simulada agroindustrial y comercializadora desarrolla actividades de acopio, administración, inventarios, despachos, facturación, nómina, comunicaciones corporativas y gestión de proveedores. Su operación depende de la coordinación entre áreas administrativas, comerciales, logísticas y tecnológicas.

El entorno tecnológico incluye ERP, servidores virtualizados, firewall corporativo, VPN, Microsoft 365, Active Directory, estaciones de usuario, repositorios documentales y copias de seguridad. Estos componentes sostienen procesos que no pueden evaluarse de manera aislada, porque una falla en identidad, red, respaldo o ERP puede afectar varias áreas al mismo tiempo.

La presión operativa del negocio puede favorecer decisiones inseguras: compartir credenciales, aprobar accesos de terceros sin trazabilidad, responder correos de manera apresurada, postergar actualizaciones o no documentar pruebas de restauración. Por ello, el análisis integra personas, procesos y tecnología.

Definición del problema

La organización presenta exposición relevante por controles incompletos o insuficientemente evidenciados sobre sistemas críticos, gestión de accesos, autenticación

multifactor, respaldo de información, respuesta ante incidentes, acceso remoto y control de terceros. El problema no se formula como una debilidad general de seguridad, sino como una situación concreta: activos críticos dependen de controles que deben formalizarse, medirse y revisarse para evitar accesos no autorizados, pérdida de información, indisponibilidad del ERP, exposición de datos personales y afectación de procesos logísticos, financieros y administrativos.

El problema identificado no reside únicamente en la ausencia de herramientas tecnológicas, sino en la desconexión operativa entre los procesos de negocio y los controles de seguridad. Por ejemplo, la dependencia crítica del proceso de despachos frente a una base de datos ERP que carece de respaldo inmutable representa un riesgo de interrupción que la organización no podría absorber financieramente por más de 4 horas. Esta brecha evidencia que la seguridad actual es reactiva y no está alineada con los objetivos de continuidad del negocio exigidos por el mercado agroindustrial actual.

Desarrollo e implementación del aprendizaje

El desarrollo se organiza con trazabilidad mínima: activo, amenaza, vulnerabilidad, riesgo, valoración, política, control y riesgo residual esperado. Esta estructura convierte el informe en un análisis técnico y evita que la propuesta se limite a una descripción de herramientas.

Identificación de activos de información

El inventario se organiza por tipo de activo, activo, descripción, ubicación, responsable, criticidad y justificación. La criticidad se asigna según el impacto operativo, legal y financiero que tendría la afectación del activo.

Tabla 1

Inventario de activos de información

Activo	Descripción y justificación	Ubicación	Responsable	Criticidad
Datos: Base de datos ERP	Registros de inventarios, compras, ventas, facturación, despachos y trazabilidad operativa. Sostiene la operación comercial y logística; su indisponibilidad detiene registros, consultas y facturación.	Servidor ERP / repositorio de base de datos	Coordinador de tecnología y líderes de proceso	Alta
Datos: Información de nómina	Datos salariales, identificaciones, pagos, seguridad social y contratos de colaboradores. Contiene datos personales y financieros protegidos por Ley 1581; su exposición puede generar impacto legal y reputacional.	Sistema de nómina / ERP	Talento humano y contabilidad	Alta
Datos: Información financiera	Registros contables, cartera, pagos, facturación y soportes tributarios. Impacta ingresos, obligaciones tributarias, control financiero y toma de decisiones.	Correos, ERP y archivos contables	Contador / dirección financiera	Alta
Datos: Información de proveedores	Datos de contacto, acuerdos, pedidos, condiciones comerciales y soportes de abastecimiento. Permite continuidad de abastecimiento y relación con terceros estratégicos.	Correo electrónico, ERP y repositorio documental	Compras / logística	Media
Datos: Copias de seguridad	Respaldos de bases de datos, servidores, archivos críticos y configuraciones. Son la principal capacidad de recuperación ante ransomware, error humano o falla técnica.	Repositorio local y repositorio externo	Coordinador de tecnología	Alta
Personas: Usuarios comerciales	Personal que registra pedidos, consulta clientes y usa correo corporativo. Puede recibir phishing o registrar información errónea que afecte ventas y atención al cliente.	Área comercial	Líder comercial	Media
Personas: Personal contable	Usuarios que gestionan pagos, facturación, cartera y reportes financieros. Accede a información financiera sensible y puede ser objetivo de fraude o suplantación.	Área contable	Contabilidad	Alta
Personas: Personal logístico	Usuarios que registran entradas, salidas, entregas, novedades y coordinación de transporte. Maneja información operativa crítica para despachos, trazabilidad y cumplimiento de entregas.	Área operativa / logística	Líder logístico	Alta

Personas: Administrador de tecnología	Responsable de servidores, usuarios, accesos, firewall, respaldos y soporte. Concentra permisos privilegiados; su cuenta o ausencia puede afectar recuperación y control de incidentes.	Área de tecnología	Gerencia administrativa	Alta
Procesos: Proceso de ventas	Registro, validación y seguimiento de pedidos, clientes y condiciones comerciales. Fallas en este proceso afectan ingresos y relación con clientes.	ERP / área comercial	Ventas	Alta
Procesos: Validación de pagos	Confirmación de transacciones, cartera, soportes y conciliaciones. Errores o fraudes afectan ingresos, control financiero y cumplimiento contable.	Contabilidad / ERP	Contador	Alta
Procesos: Gestión de inventarios	Registro de entradas, salidas, existencias, ajustes y trazabilidad. Una alteración impacta disponibilidad de producto, despachos y decisiones comerciales.	ERP / bodega / logística	Logística	Alta
Procesos: Gestión de accesos	Alta, modificación, revisión y retiro de permisos en ERP, correo, VPN y red. Permite limitar privilegios, retirar cuentas innecesarias y prevenir accesos indebidos.	Active Directory, ERP y Microsoft 365	Tecnología y líderes de área	Alta
Procesos: Gestión de incidentes	Registro, análisis, contención, recuperación y cierre de eventos de seguridad. Reduce improvisación, preserva evidencia mínima y mejora la recuperación.	Procedimiento interno	Coordinador de tecnología	Alta
Procesos: Proceso de entrega	Coordinación de despachos, transportistas, novedades y confirmación de entrega. Afecta satisfacción del cliente, cumplimiento de pedidos y trazabilidad operativa.	Logística / ERP / comunicaciones	Logística	Media
Tecnología: Firewall corporativo y VPN	Control perimetral, acceso remoto seguro, filtrado y registro de eventos. Un error de configuración puede exponer servicios internos o permitir acceso remoto indebido.	Perímetro de red	Coordinador de tecnología	Alta
Tecnología: Microsoft 365	Correo electrónico, colaboración, almacenamiento y autenticación asociada. Es canal crítico de comunicación y vector frecuente de phishing, suplantación y fuga de información.	Nube	Coordinador de tecnología	Alta
Tecnología: Active Directory	Gestión centralizada de usuarios, equipos, grupos y políticas. Un compromiso de identidad facilita	Servidor de identidad	Coordinador de tecnología	Alta

	movimiento lateral y acceso a múltiples servicios.

Análisis de amenazas y vulnerabilidades

Una amenaza no produce riesgo por sí sola. El riesgo aparece cuando la amenaza puede aprovechar una vulnerabilidad sobre un activo con valor para el negocio. Esta relación es coherente con el enfoque de gestión de riesgos de ISO/IEC 27005:2022 (ISO/IEC, 2022b).

Tabla 2

Relación entre activos, amenazas y vulnerabilidades

Activo	Amenaza	Vulnerabilidad	Consecuencia
Base de datos ERP	Ransomware	Servidores o estaciones sin endurecimiento suficiente, parches pendientes o control débil de ejecución.	Indisponibilidad del ERP, interrupción de inventarios, facturación y despachos.
Información de nómina	Phishing o vishing	Capacitación insuficiente, exceso de confianza y MFA incompleto.	Exposición de datos personales y financieros de colaboradores.
Información financiera	Suplantación o fraude por correo	Ausencia de verificación por canal alterno para pagos o cambios de cuenta.	Pagos indebidos, pérdida financiera o registros contables incorrectos.
Copias de seguridad	Ransomware o error operativo	Backups sin inmutabilidad, segregación o pruebas periódicas de restauración.	Pérdida de capacidad real de recuperación ante incidente.
Administrador de tecnología	Ingeniería social o abuso de privilegios	Cuentas privilegiadas sin revisión, uso compartido o almacenamiento inseguro de credenciales.	Acceso no autorizado a sistemas críticos y posible escalamiento del incidente.
Microsoft 365	Compromiso de cuenta	MFA parcial, monitoreo insuficiente o reenvíos no revisados.	Suplantación, fuga de información y envío de mensajes maliciosos.
Firewall corporativo y VPN	Acceso remoto indebido	Reglas permisivas, cuentas de terceros permanentes o VPN sin MFA.	Acceso no autorizado a recursos internos.
Gestión de inventarios	Manipulación interna o error humano	Permisos excesivos y ausencia de segregación de funciones.	Diferencias de inventario, despachos incorrectos o pérdida de trazabilidad.
Proceso de entrega	Falla operativa o pérdida de comunicación	Procedimiento manual no documentado y dependencia de canales informales.	Retrasos, errores de entrega y afectación de servicio.

Evaluación y priorización de riesgos

La evaluación usa una escala de 1 a 5 para probabilidad e impacto. El nivel de riesgo corresponde a Probabilidad x Impacto. La clasificación adoptada es: bajo de 1 a 5, medio de 6 a 10, medio-alto de 11 a 14, alto de 15 a 19 y crítico de 20 a 25. Esta escala permite priorizar riesgos sobre datos personales, continuidad operativa e información financiera.

Tabla 3

Matriz de evaluación y tratamiento de riesgos

Activo / Amenaza	Vulnerabilidad	Riesgo	P × I = Nivel	Control propuesto	Riesgo residual esperado
Base de datos ERP Amenaza: Ransomware	Hardening y control de ejecución insuficientes	Indisponibilidad del sistema operativo y comercial	4 × 5 = 20 (Crítico)	EDR, parches, segmentación, control de aplicaciones y respaldo inmutable	Medio
Información de nómina Amenaza: Phishing / vishing	MFA incompleto y baja sensibilización	Exfiltración de datos personales y financieros	4 × 5 = 20 (Crítico)	MFA obligatorio, capacitación, alertas de inicio de sesión y clasificación de datos	Medio
Información financiera Amenaza: Fraude por suplantación	Falta de confirmación por canal alterno	Pago no autorizado o alteración de instrucciones financieras	3 × 5 = 15 (Alto)	Doble validación, segregación de funciones y bitácora de aprobaciones	Medio
Microsoft 365 Amenaza: Compromiso de cuenta	Monitoreo insuficiente y contraseñas reutilizadas	Suplantación y fuga de información	4 × 4 = 16 (Alto)	MFA, acceso condicional, alertas, revisión de reenvíos y auditoría	Medio
Copias de seguridad Amenaza: Ransomware	Backups sin inmutabilidad o sin pruebas de restauración	Imposibilidad de recuperación ante incidente	3 × 5 = 15 (Alto)	Regla 3-2-1-1-0, repositorio segregado, inmutabilidad y pruebas de restauración	Bajo/Medio
Administrador de tecnología Amenaza: Ingeniería social o abuso interno	Uso compartido o almacenamiento inseguro de credenciales	Acceso privilegiado no autorizado	3 × 5 = 15 (Alto)	Cuentas nominativas, bóveda de contraseñas, mínimo privilegio y revisión periódica	Medio
Firewall corporativo y VPN Amenaza:	Reglas permisivas o VPN sin	Acceso no autorizado a red interna	3 × 4 = 12 (Medio-alto)	Revisión de reglas, VPN con MFA, registro de eventos y segmentación	Bajo/Medio

Acceso remoto indebido	controles robustos				
Gestión de inventarios Amenaza: Manipulación o error humano	Permisos excesivos y ausencia de segregación	Alteración de entradas, salidas o existencias	4 × 4 = 16 (Alto)	RBAC, segregación de funciones, bitácoras y revisión de cambios	Medio
Proceso de entrega Amenaza: Falla operativa	Procedimiento manual no documentado	Retrasos, errores de despacho o pérdida de trazabilidad	3 × 4 = 12 (Medio-alto)	Procedimiento de contingencia, responsables y conciliación posterior	Bajo/Medio

El impacto de los riesgos técnicos identificados no debe leerse como fallos aislados de sistemas, sino como interrupciones críticas a la cadena de valor de la organización. Por ejemplo, un compromiso del Active Directory o la VPN no solo representaría un fallo de acceso; significaría que el personal comercial y logístico quedaría incapacitado para registrar pedidos y coordinar despachos en tiempo real, generando cuellos de botella en la salida de productos perecederos. De igual forma, la ausencia de respaldos inmutables ante un ataque de ransomware detendría la trazabilidad operativa y contable, impidiendo que la gerencia administrativa valide pagos a proveedores y nómina, lo que derivaría en parálisis operativa y posibles sanciones por incumplimiento de contratos de exportación o distribución.

Políticas y controles de seguridad

Las políticas definen el lineamiento obligatorio y los controles indican la forma concreta de aplicación. Para mantener trazabilidad, cada control se relaciona con un activo o riesgo de la matriz anterior. Este enfoque responde al principio de tratamiento del riesgo planteado por ISO/IEC 27005:2022 y al ciclo de mejora esperado en ISO/IEC 27001:2022 (ISO/IEC, 2022a, 2022b).

Tabla 4

Políticas y controles propuestos

Tipo de política	Política redactada	Justificación
Gestión de accesos	Todo acceso a sistemas críticos debe ser individual, autorizado, trazable y revisado periódicamente.	Reduce accesos indebidos, cuentas compartidas, permisos acumulados y usuarios activos sin necesidad operativa.
Autenticación multifactor	Todo servicio que procese información sensible o permita acceso remoto debe exigir autenticación multifactor.	Disminuye la probabilidad de compromiso por robo de credenciales, phishing o reutilización de contraseñas.
Protección de datos personales	La información personal debe tratarse con acceso restringido, finalidad definida y controles proporcionales a su sensibilidad.	Alinea el tratamiento de datos con la Ley 1581 de 2012 y reduce exposición legal, reputacional y operativa.
Respaldo y recuperación	Las copias de seguridad deben ser íntegras, segregadas, protegidas contra modificación no autorizada y probadas periódicamente.	Permite recuperar información crítica ante ransomware, error humano, corrupción de datos o fallas de infraestructura.
Endurecimiento y actualización	Los servidores, estaciones y aplicaciones deben mantenerse actualizados y configurados bajo criterios mínimos de seguridad.	Reduce la superficie de ataque explotable por malware, ransomware y vulnerabilidades conocidas.
Control de pagos	Toda modificación de cuenta bancaria, instrucción de pago o cambio de condición financiera debe validarse por un canal alterno.	Mitiga fraude por suplantación, correos comprometidos y cambios no autorizados en instrucciones financieras.
Acceso de terceros	Los proveedores solo deben acceder con autorización previa, tiempo definido, cuenta individual y registro de actividad.	Limita accesos permanentes, acciones no trazables y exposición de sistemas internos por terceros.
Segregación de funciones	Los permisos asignados deben corresponder al rol del usuario y evitar combinaciones incompatibles en ventas, inventarios, pagos y administración.	Disminuye el riesgo de fraude, manipulación interna y errores no detectados en procesos críticos.
Gestión de incidentes	Todo evento de seguridad debe registrarse, clasificarse, contenerse, analizarse y cerrarse con acciones correctivas documentadas.	Reduce improvisación, facilita la preservación de evidencia y mejora la recuperación y prevención de recurrencias.

Para asegurar que los controles propuestos no sean meras declaraciones de intención, se establece que el Coordinador de Tecnología será el responsable directo de supervisar la efectividad de la Autenticación Multifactor (MFA) y el mínimo privilegio, mediante una revisión técnica quincenal. La evidencia del cumplimiento real se consolidará en un Log de Auditoría de Accesos, el cual deberá ser refrendado por la Gerencia Administrativa mensualmente. Por otro lado, la integridad de los respaldos inmutables será verificada mediante pruebas de restauración

trimestrales, cuya bitácora servirá como evidencia de control para auditorías bajo el estándar ISO/IEC 27001:2022.

Gestión de incidentes

Para la organización simulada, un incidente de seguridad es cualquier evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad del ERP, nómina, correo, identidad, VPN, respaldos o información financiera. El procedimiento se estructura en seis fases, alineadas con la función de respuesta y recuperación del NIST Cybersecurity Framework 2.0 (NIST, 2024).

Tabla 5

Procedimiento de respuesta ante incidentes

Fase	Aplicación en la organización simulada
Preparación	Definir responsables, contactos, inventario de activos críticos, canales de reporte, criterios de severidad, formatos y procedimientos mínimos.
Identificación	Detectar anomalías en ERP, Microsoft 365, Active Directory, firewall, endpoints, VPN y copias de seguridad. Registrar hora, usuario, sistema afectado y evidencia inicial.
Contención	Aislar equipos afectados, bloquear cuentas comprometidas, suspender accesos de terceros, limitar tráfico y proteger respaldos antes de restaurar.
Erradicación	Eliminar malware, corregir configuraciones débiles, cerrar vulnerabilidades, aplicar parches y retirar credenciales comprometidas.
Recuperación	Restaurar servicios desde copias verificadas, validar integridad de datos y monitorear recurrencia antes de declarar cierre operativo.
Lecciones aprendidas	Documentar causa raíz, impacto, controles fallidos, tiempos, decisiones adoptadas y acciones de mejora con responsable y fecha.

Ante ransomware sobre el ERP, la restauración no debe ejecutarse sin contención previa. Primero se debe aislar el alcance, preservar evidencia mínima, verificar que las copias no estén comprometidas, cerrar el vector probable y restaurar desde respaldos limpios. Restaurar sin erradicar la causa puede repetir el incidente.

Continuidad del negocio

La continuidad se orienta a mantener o recuperar los servicios que soportan la operación. Los RTO y RPO propuestos son una línea base técnica; deben validarse mediante un análisis formal de impacto al negocio antes de convertirse en compromiso institucional.

Tabla 6

Objetivos iniciales de recuperación

Servicio / activo	Impacto de indisponibilidad	RTO sugerido	RPO sugerido	Medida de continuidad
ERP	Detención de inventarios, ventas, facturación y trazabilidad operativa.	4 horas	1 hora	Restauración desde respaldo verificado y operación manual temporal.
Active Directory	Fallas de autenticación y acceso a servicios internos.	4 horas	2 horas	Controlador redundante, respaldo de estado del sistema y cuenta de emergencia.
Microsoft 365	Afectación de comunicaciones, coordinación y trazabilidad de aprobaciones.	8 horas	4 horas	Canal alterno de comunicación y monitoreo de cuentas comprometidas.
Nómina	Afectación de pagos, reportes y tratamiento de datos personales.	24 horas	4 horas	Restauración priorizada, validación de integridad y acceso restringido.
Copias de seguridad	Pérdida de capacidad de recuperación ante incidentes mayores.	Crítico	Según política	Inmutabilidad, segregación, pruebas de restauración y monitoreo de fallos.
VPN / firewall	Interrupción de acceso remoto seguro y soporte externo.	8 horas	4 horas	Configuración respaldada, reglas documentadas y acceso alterno autorizado.
Proceso de entrega	Retrasos, errores de despacho o pérdida de confirmación.	8 horas	4 horas	Formato manual de contingencia y conciliación posterior contra ERP.

Durante una interrupción del ERP, la organización debe usar un procedimiento manual temporal para ventas, inventario y entregas. Ese procedimiento debe tener responsable, formato único, hora de inicio, hora de cierre y conciliación posterior. Sin conciliación, la contingencia puede resolver la disponibilidad inmediata, pero crear problemas de integridad de datos.

La estrategia de continuidad operativa prioriza el Proceso de Despachos e Inventarios con un RTO de 4 horas, reconociendo que la supervivencia financiera de la empresa depende de su capacidad de entrega física. Ante una crisis de ciberseguridad, la Gerencia General asumirá el liderazgo del Comité de Crisis, estableciendo canales de comunicación transparentes con los clientes para mitigar el daño reputacional. Se estima que una interrupción prolongada del ERP superior a las 12 horas generaría una pérdida operativa por penalizaciones logísticas y lucro cesante de aproximadamente el 15% del margen neto mensual, lo que justifica la inversión en infraestructuras de alta disponibilidad y contingencias manuales documentadas.

Análisis organizacional y cultura de seguridad

La cultura de seguridad debe enfocarse en conductas observables. No basta con decir que los usuarios deben estar capacitados; la organización debe medir reportes de phishing, permisos revisados, accesos cerrados, restauraciones probadas y cambios aprobados. Este enfoque es coherente con la necesidad de evidencias de control y mejora continua (ISO/IEC, 2022a; NIST, 2024).

Tabla 7

Plan de cultura y medición

Tema	Acción propuesta	Indicador de seguimiento
Phishing y vishing	Simulaciones trimestrales, microcapacitaciones y protocolo de verificación por canal alterno.	Tasa de clics, tasa de reporte, reincidencia por área.
Uso de privilegios	Capacitación al personal de tecnología sobre mínimo privilegio, cuentas nominativas y registro de cambios.	Número de cuentas privilegiadas revisadas y hallazgos corregidos.
Acceso remoto	Instrucción obligatoria sobre VPN, MFA y prohibición de herramientas remotas no autorizadas.	Accesos remotos revisados, cuentas temporales cerradas y eventos anómalos.
Manejo de datos personales	Sensibilización sobre Ley 1581, clasificación de información y acceso por rol.	Incidentes de exposición, permisos corregidos y evidencias de capacitación.

Continuidad	Simulacros semestrales de restauración y operación manual controlada.	Tiempo real de recuperación y porcentaje de restauraciones exitosas.

Lograr un cambio cultural profundo requiere trascender la capacitación teórica y fomentar un compromiso genuino desde las áreas no técnicas (bodega y ventas). Para reducir la resistencia al cambio frente a controles como la VPN o el MFA, se implementará un programa de 'Seguridad por Empatía', donde se explique el beneficio personal de proteger la información. En casos de incumplimiento reiterado de las políticas, la organización aplicará el régimen disciplinario interno, vinculando la seguridad con el desempeño profesional. No obstante, se promoverá una cultura de 'Cero Culpa' ante el reporte temprano de incidentes, asegurando que el factor humano sea la primera línea de detección y no el eslabón más débil por temor a represalias.

Conclusiones

El análisis demuestra que la organización simulada agroindustrial y comercializadora necesita gestionar la ciberseguridad con trazabilidad entre activos, amenazas, vulnerabilidades, riesgos y controles. Los activos más críticos son el ERP, la nómina, la información financiera, Microsoft 365, Active Directory, las copias de seguridad, el firewall/VPN, la gestión de accesos y el proceso de inventarios.

Los riesgos con mayor prioridad son ransomware sobre ERP y respaldos, phishing contra usuarios con acceso a nómina o correo, suplantación para fraude financiero, compromiso de cuentas en Microsoft 365, abuso de privilegios, acceso remoto indebido y manipulación de inventarios. Estos riesgos requieren controles técnicos, pero también políticas, responsables, evidencia y revisión periódica.

La reducción del riesgo residual depende de controles concretos: MFA, mínimo privilegio, revisión de accesos, respaldo inmutable, pruebas de restauración, EDR, segmentación,

validación de pagos por canal alterno, control de proveedores, capacitación focalizada y respuesta documentada ante incidentes. La propuesta no elimina el riesgo; lo reduce a niveles más gestionables y verificables.

El ejercicio permitió evidenciar que la seguridad de la información no puede tratarse como un asunto exclusivamente tecnológico. En el caso analizado, los riesgos relevantes aparecen cuando los procesos de ventas, pagos, inventarios y entregas dependen de datos confiables y de accesos bien administrados. La principal lección es que cada control debe responder a un riesgo concreto; de lo contrario, la organización puede invertir en herramientas sin reducir de forma clara su exposición operativa.

Desde el componente técnico, el informe confirma que la continuidad del negocio depende de controles verificables y no solo de tener infraestructura disponible. La protección del ERP, Microsoft 365, Active Directory, credenciales administrativas, VPN y copias de seguridad debe gestionarse con responsables, frecuencia de revisión, evidencia de restauración, monitoreo y riesgo residual esperado. Esa trazabilidad permite priorizar recursos y reduce la improvisación durante incidentes de seguridad.

Referencias

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

Corporación Universitaria Remington. (2026). *Seminario en Gestión de Ciberseguridad en las Organizaciones. Material académico del seminario*.

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. ENISA.

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

International Organization for Standardization. (2022b). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.

Instituto Colombiano de Normas Técnicas y Certificación. (2013). *NTC-ISO/IEC 27001:2013 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos*. Icontec.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Modelo de seguridad y privacidad de la información (MSPI) — Guía 2: Elaboración de la política general de seguridad y privacidad de la información*. MinTIC.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.