Diagnóstico de ciberseguridad en un taller de maquinaria agrícola: identificación de activos, amenazas, vulnerabilidades y evaluación de riesgos

Corporación Universitaria Remington
Facultad de Ingenierías
Tecnología en desarrollo de software

Yerson Danian Morales Rivera
Jorge Leonardo Ramírez Restrepo
Seminario de Grado — Gestión de Ciberseguridad en Organizaciones
2026

Tabla de Contenidos

Resumen

El presente informe técnico analiza la situación de seguridad de la información de un taller de maquinaria agrícola de tamaño mediano, presentado como caso hipotético con base en un contexto organizacional verosímil y representativo de empresas medianas del sector agropecuario colombiano. La organización hipotética gestiona cotidianamente información sensible de clientes, proveedores, inventarios y transacciones financieras a través de medios completamente informales: hojas de cálculo en computadores personales, mensajes de WhatsApp y documentos físicos sin ningún control de acceso ni respaldo.

El trabajo se enmarca en el Seminario de Grado en Gestión de Ciberseguridad en Organizaciones y aplica los contenidos de las 8 primeras sesiones a un caso hipotético. El informe desarrolla cuatro componentes: el marco conceptual (conceptos de ciberseguridad, activos, amenazas, vulnerabilidades, riesgo y normativa aplicable); el marco contextual (descripción de la organización y su situación actual); la identificación de activos (nueve activos clasificados por tipo y criticidad); y el análisis de amenazas, vulnerabilidades y evaluación de riesgos (seis escenarios analizados mediante matriz de probabilidad e impacto).

El resultado principal es que el taller presenta tres riesgos críticos, todos con probabilidad alta: borrado accidental de datos sin posibilidad de recuperación, acceso vigente de ex-empleados desvinculados y fuga de datos personales por canales no cifrados. Ninguno requiere un atacante externo para materializarse; son consecuencias directas de operar sin los controles más básicos de seguridad de la información.

Palabras clave:

Ciberseguridad organizacional, activos de información, amenazas, vulnerabilidades, gestión de riesgos.

Marco conceptual y contextual

Desde el marco normativo, la Ley 1581 de 2012 regula el tratamiento de datos personales en Colombia y aplica a cualquier organización independientemente de su tamaño, incluyendo el taller hipotético analizado. El incumplimiento puede derivar en sanciones de la Superintendencia de Industria y Comercio. El estándar ISO/IEC 27001 estructura el Sistema de Gestión de Seguridad de la Información, mientras que el marco NIST orienta las acciones operativas en cinco funciones: identificar, proteger, detectar, responder y recuperar.

El taller es una empresa mediana del sector agropecuario colombiano dedicada al mantenimiento, reparación y comercialización de maquinaria agrícola y repuestos. Atiende principalmente a agricultores, cooperativas y empresas del campo, con varios años de operación y buena reputación en su zona de influencia. Cuenta con entre doce y quince colaboradores: técnicos especializados en distintos tipos de maquinaria, personal administrativo encargado de la atención al cliente y gestión de pedidos, y una persona responsable de la contabilidad. Por solicitud del propietario, la organización no se identifica con su nombre real en este documento.

El caso hipotético fue diseñado para representar con precisión un tipo de empresa muy común en Colombia: operativa, consolidada en su sector, pero que nunca ha considerado la ciberseguridad como una necesidad porque nunca ha tenido un incidente visible. Esta característica es intencionada: la ausencia de incidentes no es evidencia de seguridad, sino evidencia de que los riesgos aún no se han materializado.

En cuanto a su situación hipotética frente a la seguridad de la información, el panorama es uniforme: no existe ningún control formal. Toda la información operativa vive en hojas de cálculo en computadores personales, las comunicaciones internas y con clientes se hacen por WhatsApp sin protocolo, las contraseñas son compartidas entre empleados y ningún proceso está documentado. La organización opera bajo la suposición implícita de que "nunca ha pasado nada", que es precisamente la vulnerabilidad más difícil de gestionar: la que no se percibe como tal.

Desarrollo e implementación del aprendizaje

1. Identificación de activos de información

El primer paso para analizar la seguridad de cualquier organización es entender qué tiene valor dentro de ella. En el taller, ese ejercicio reveló que varios de los activos más críticos no son tecnológicos sino humanos y organizacionales: el conocimiento de los técnicos y los procesos operativos no documentados son, en muchos casos, más valiosos que los equipos físicos. La tabla 1 presenta los activos identificados, clasificados por tipo y con una valoración de criticidad basada en el impacto que tendría su pérdida, alteración o indisponibilidad.

Tabla 1.

Inventario de activos de información del taller de maquinaria agrícola.

Tipo	Activo	Descripción	Ubicación actual	Responsable	Criticidad
Datos	Base de clientes	Nombres, teléfonos, correos, historial de equipos y pagos.	Hoja de cálculo en PC personal del administrador, sin contraseña.	Administrador	Alta
Datos	Información financiera	Facturas, pagos, créditos a clientes y pagos a proveedores.	Hojas de cálculo y documentos físicos sin archivar.	Contador / Admin.	Alta
Datos	Órdenes de trabajo	Servicios prestados, repuestos usados, tiempos y costos por equipo.	WhatsApp y hojas sueltas sin sistema de archivo.	Técnicos / Admin.	Media-Alta
Datos	Inventario de repuestos	Stock, precios de compra, proveedores y referencias técnicas.	Hojas de cálculo sin control de versiones ni acceso diferenciado.	Bodeguero / Admin.	Media
Personas	Técnicos especializados	Conocimiento técnico sobre equipos y procesos, sin documentar en ningún sistema.	Exclusivamente en la memoria del personal técnico.	Propietario	Alta
Personas	Personal administrativo	Acceso sin restricciones a toda la	Sin controles de acceso diferenciados por rol.	Propietario	Alta

		información del taller.			
Procesos	Atención al cliente	Recepción, diagnóstico, cotización, reparación, entrega y cobro.	No documentado. Cada técnico lo ejecuta según su criterio.	Sin asignado	Alta
Procesos	Facturación y cobro	Registro de servicios, generación de factura y gestión de pagos.	Informal, sin validaciones ni protocolo.	Contador / Admin.	Alta
Tecnología	Computadores personales	Dispositivos donde vive toda la información digital del taller.	En escritorios de empleados. Sin cifrado, sin respaldo.	Sin asignado	Alta

Nota. Elaboración propia con base en el análisis del caso hipotético y los criterios de clasificación del seminario (Ramírez, 2026).

En el caso hipotético, la base de clientes —representada como una hoja de cálculo sin contraseña— sería el activo más crítico del negocio. Su pérdida implicaría no poder identificar a qué clientes se les deben piezas o servicios pendientes, no tener historial de equipos atendidos para diagnósticos futuros y perder el registro de cuentas por cobrar. En la práctica, el taller quedaría sin su principal herramienta comercial de un momento a otro, lo que podría paralizar la facturación durante semanas. El segundo activo crítico es el conocimiento técnico del personal especializado: si el técnico principal se desvincula sin transferir ese saber, trabajos complejos quedarían inconclusos, clientes esperando y reputación afectada, porque nadie más en el taller sabría cómo resolverlos.

2. Análisis de amenazas y vulnerabilidades

Con los activos identificados, el siguiente paso es entender qué los amenaza y qué condiciones internas hacen posible que esas amenazas se materialicen. Una amenaza por sí sola no genera el incidente, ni tampoco la vulnerabilidad aislada: el problema ocurre cuando las dos se encuentran (Ramírez, 2026). La tabla 2 relaciona explícitamente cada amenaza con la vulnerabilidad que la permite y el impacto potencial sobre la organización, limitándose a las situaciones más realistas para este tipo de empresa.

Tabla 2.

Relación de amenazas y vulnerabilidades identificadas en el taller.

Amenaza	**Vulnerabilidad que la permite**	**Impacto potencial en el taller**	**Activo(s) afectado(s)**
Borrado o modificación accidental de datos	Sin copias de seguridad. Sin control de versiones. Credenciales compartidas sin trazabilidad.	Pérdida irreversible de información crítica. Sin posibilidad de identificar al responsable del cambio.	Base de clientes, información financiera
Acceso de ex-empleado desvinculado	Sin procedimiento de revocación de accesos. Contraseñas no se cambian al desvincularse alguien.	Fuga o modificación de información de clientes, precios y proveedores por alguien externo a la organización.	Base de clientes, información financiera

Phishing o engaño por WhatsApp / correo	Personal sin formación en seguridad digital. Canales no verificados usados para comunicación operativa.	Entrega de información sensible o credenciales a un tercero que suplanta un cliente o proveedor conocido.	Datos de clientes, información financiera
Pérdida o daño físico del equipo	Toda la información digital en computadores personales sin respaldo en ningún otro medio.	Pérdida total de la información operativa. Paralización inmediata del negocio sin posibilidad de recuperación.	Todos los activos digitales
Fuga de datos personales de clientes	Sin política de tratamiento de datos. Información enviada por WhatsApp sin cifrado. Sin acuerdos de confidencialidad.	Incumplimiento de la Ley 1581. Sanciones de la SIC. Daño reputacional ante los clientes del taller.	Base de clientes, datos personales
Interrupción de la operación por incidente	Sin plan de contingencia. Sin procesos documentados. Conocimiento concentrado en pocas personas.	Paralización parcial o total del taller ante cualquier incidente, sin saber cómo continuar la operación.	Todos los procesos operativos

Nota. Elaboración propia con base en el análisis del caso hipotético y los conceptos trabajados en el seminario (Ramírez, 2026).

El elemento más relevante de este análisis no es el número de amenazas sino su origen. Ninguna de las seis situaciones identificadas requiere un atacante externo sofisticado: todas son consecuencias directas de operar sin controles básicos. Eso no es un fallo del personal; es un fallo de la organización que nunca definió cómo se debe manejar la información. Como señala Ramírez (2026), el factor humano no es el eslabón más débil de la cadena de seguridad: es el más determinante, y la diferencia la hace la cultura organizacional.

3. Evaluación del nivel de riesgo

Identificar amenazas y vulnerabilidades no es suficiente. El análisis de riesgos requiere evaluar cada situación en dos dimensiones: probabilidad de ocurrencia e impacto potencial si llegara a materializarse. Esa combinación, trabajada en la clase 5 del seminario, permite pasar de una lista de problemas a un análisis priorizado que oriente las decisiones de gestión (Ramírez, 2026; ISO/IEC 27005, 2022). El riesgo se define como la posibilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto; no es el ataque en sí ni la vulnerabilidad aislada, sino la combinación de ambos.

Para valorar cada riesgo se utilizó una escala cualitativa de tres niveles (Alto, Medio y Bajo) en cada dimensión. La probabilidad se calificó como Alta cuando la situación puede ocurrir en el transcurso normal de la operación sin requerir ningún factor externo; Media cuando depende de alguna condición adicional; y Baja cuando el escenario es poco probable en este contexto. El impacto se valoró como Alto cuando el incidente afecta directamente la continuidad operativa o financiera del negocio; Medio cuando genera perturbaciones gestionables; y Bajo cuando el efecto es menor y recuperable con rapidez. El nivel de riesgo resultante combina ambas dimensiones: probabilidad Alta con impacto Alto equivale a riesgo Crítico que exige atención inmediata.

Tabla 3.

Matriz de evaluación de riesgos del taller de maquinaria agrícola.

Riesgo identificado	Probabilidad	Impacto	Nivel de riesgo	Justificación
Borrado o modificación accidental de datos	Alta	Alto	Crítico	Sin controles ni respaldos, la pérdida es irreversible y puede ocurrir en cualquier jornada normal de trabajo.
Acceso de ex-empleado desvinculado	Alta	Alto	Crítico	Cada desvinculación deja el acceso activo de forma indefinida sobre toda la información del taller.
Fuga de datos personales de clientes	Alta	Alto	Crítico	Un mensaje de WhatsApp enviado al contacto equivocado puede ocurrir en cualquier momento del día.
Pérdida o daño físico del equipo	Media	Alto	Alto	Sin respaldos, el daño o pérdida de un equipo implica la pérdida total de la información que contenía.
Phishing o engaño por WhatsApp / correo	Media	Alto	Alto	El personal usa a diario los mismos canales por los que podría llegar un engaño sin poder identificarlo.
Interrupción de la operación por incidente	Media	Alto	Alto	Sin plan de contingencia ni procesos documentados, cualquier incidente puede paralizar el negocio.

Nota. Elaboración propia. Escala: Alto / Medio / Bajo en probabilidad e impacto. Nivel crítico = probabilidad alta + impacto alto. Referencia: ISO/IEC 27005 (2022) y Ramírez (2026).

Los tres riesgos clasificados como críticos comparten una característica: todos tienen probabilidad alta, lo que los convierte en la prioridad inmediata de la propuesta de controles que se desarrollará en la siguiente entrega. No son escenarios hipotéticos ni remotos; son situaciones que pueden ocurrir en cualquier jornada normal sin que ningún factor externo intervenga. La matriz también deja ver que ninguno de los seis riesgos identificados tiene impacto bajo: el taller no tiene riesgos menores, tiene riesgos que aún no se han materializado.

4. Diseño de políticas de seguridad y controles

Una vez identificados los riesgos y construida la matriz de evaluación, el paso siguiente es definir qué debe hacer la organización para controlarlos. Para eso existen las políticas de seguridad: lineamientos formales que establecen el deber ser frente a situaciones específicas. Como señala Ramírez (2026), una política no es una recomendación ni una sugerencia; es una directriz que orienta el comportamiento de toda la organización y que nace directamente del análisis de riesgo previo.

Una distinción clave que trabajó el seminario en la clase 6 es que la política define el qué, no el cómo. Establecer que "los accesos deben ser controlados y autorizados" es una política. Explicar cómo se configura ese sistema de acceso paso a paso ya es un procedimiento. En el informe, cada política va acompañada de su control correspondiente, que es el mecanismo concreto que permite que el lineamiento se cumpla en la práctica. Sin control, la política queda en papel; sin política, el control carece de respaldo formal.

Tabla 4.

Políticas de seguridad y controles propuestos para el taller de maquinaria agrícola.

Riesgo que origina	Tipo de política	Política (el qué)	Control asociado (el cómo)	Justificación
Borrado accidental de datos / pérdida por daño físico del equipo	Política de respaldo de información	La organización deberá garantizar la existencia de copias de seguridad periódicas de toda la información crítica, asegurando su disponibilidad ante cualquier incidente que afecte los equipos o los datos.	Copia de seguridad automática semanal en servicio en la nube (Google Drive o similar). Verificación mensual de que el respaldo sea accesible y esté completo.	Sin respaldos, la pérdida de un equipo implica la pérdida total e irreversible de la información operativa del taller. Esta política reduce el impacto del riesgo crítico más probable.
Acceso de ex-empleado desvinculado	Política de control de accesos	El acceso a los sistemas e información del taller deberá ser controlado, autorizado y diferenciado por rol, garantizando que cada colaborador acceda únicamente a la información necesaria para sus funciones.	Asignación de contraseñas individuales por empleado. Procedimiento de revocación inmediata de accesos al momento de cualquier desvinculación. Revisión semestral de quién tiene acceso a qué.	Las credenciales compartidas impiden identificar responsables de cambios y mantienen activos los accesos de personas desvinculadas, generando un riesgo crítico de fuga o modificación de información.
Fuga de datos personales de clientes (Ley 1581)	Política de tratamiento de datos personales	La organización deberá garantizar que la información personal de sus clientes sea recolectada, almacenada y utilizada de forma segura, con propósito definido y bajo	Almacenamiento de datos de clientes en sistema centralizado con acceso restringido. Prohibición de compartir datos personales por canales no cifrados como WhatsApp.	El taller almacena datos personales sin política alguna y los comparte por canales no seguros, incumpliendo la Ley 1581. Una fuga puede derivar en sanciones de la SIC y pérdida

		consentimiento, en cumplimiento de la Ley 1581 de 2012.	Firma de acuerdo de confidencialidad con todos los colaboradores.	de confianza de los clientes.
Phishing o engaño por WhatsApp / correo	Política de uso de canales digitales	Los colaboradores deberán hacer uso responsable de los canales digitales corporativos, verificando la autenticidad de los mensajes recibidos y evitando la interacción con contenidos sospechosos que puedan comprometer la seguridad de la información.	Capacitación básica anual en identificación de mensajes fraudulentos. Lista de verificación simple para solicitudes de información por canales digitales. Definición de canal oficial para solicitudes de datos de clientes o proveedores.	El personal utiliza WhatsApp y correo electrónico para comunicación operativa sin ningún lineamiento de seguridad, haciéndolos vulnerables a engaños que ya han afectado a organizaciones similares.
Interrupción de la operación por incidente	Política de continuidad operativa	La organización deberá contar con lineamientos básicos que permitan mantener o retomar la operación ante la ocurrencia de incidentes que afecten sus sistemas, información o personal clave.	Documentación de los procesos críticos (atención al cliente, facturación) en formato escrito accesible. Identificación de al menos una persona alternativa capaz de asumir cada función crítica. Definición de un protocolo mínimo de respuesta ante pérdida de información.	El conocimiento operativo del taller vive exclusivamente en la memoria del personal. Si alguien falta o un sistema falla, no hay manera de continuar con normalidad. Esta política mitiga la vulnerabilidad más estructural del negocio.

Nota. Elaboración propia con base en el análisis de riesgos de la sección 3 y los lineamientos de diseño de políticas trabajados en la clase 6 del seminario (Ramírez, 2026). Las políticas siguen el principio de definir el qué; los controles especifican el cómo de implementación.

Cada política responde directamente a un riesgo identificado: no son lineamientos genéricos sino respuestas al caso hipotético analizado. En términos de implementación, el responsable de verificar los respaldos sería el administrador, quien confirmaría una vez por semana que la copia en la nube se completó correctamente. El control de WhatsApp se implementaría definiendo qué información puede circular por ese canal (coordinación operativa) y cuál no (datos personales, información financiera), comunicándolo en una reunión breve. El cumplimiento de contraseñas individuales se verificaría mensualmente: el administrador confirma que cada equipo requiere credencial propia para iniciarse. La revisión general de políticas correspondería al propietario, con frecuencia semestral mínima.

5. Gestión de incidentes y respuesta

A pesar de los controles y las políticas implementadas, ninguna organización está completamente a salvo de que un incidente ocurra. Como señala Ramírez (2026), un

incidente de seguridad es el momento en que el riesgo deja de ser una posibilidad y se convierte en realidad: cualquier evento que compromete la confidencialidad, la integridad o la disponibilidad de la información. La diferencia entre una organización que colapsa y una que supera una crisis no está en si sufrió o no el incidente, sino en cómo respondió ante él.

Para el taller, los escenarios de incidente más probables son aquellos que se derivan directamente de los riesgos críticos identificados en la sección 3: pérdida de información por daño o robo de un equipo, acceso de un ex-empleado desvinculado a los sistemas, y fuga de datos de clientes por un error en WhatsApp. Ninguno de estos requiere un atacante sofisticado; todos pueden ocurrir en el transcurso de un día normal de trabajo.

Tabla 5.

Escenarios de incidente y fases de respuesta para el taller de maquinaria agrícola.

Fase	Descripción de la fase	Aplicación al taller
1. Preparación	Ocurre antes del incidente. Se definen roles, responsabilidades y protocolos de respuesta.	El propietario designa un responsable de gestionar incidentes. Se establece un protocolo básico documentado: a quién llamar, qué hacer primero, dónde están los respaldos y cómo revocar accesos.
2. Identificación	Se detecta que algo inusual está ocurriendo y se evalúa si constituye un incidente real.	Señales de alerta: un equipo que no enciende, accesos a información desde cuentas de empleados desvinculados, mensajes de clientes que no reconocen comunicaciones enviadas desde el taller.
3. Contención	Se evita que el incidente se propague o genere daños adicionales.	Desconectar el equipo afectado de la red. Bloquear las credenciales comprometidas de forma inmediata. Suspender temporalmente el uso del canal de WhatsApp si hay sospecha de fuga de información.
4. Erradicación	Se elimina la causa raíz del incidente.	Cambiar todas las contraseñas de acceso. Verificar qué información fue afectada y por quién. Si el equipo fue comprometido, restaurarlo desde el respaldo más reciente.
5. Recuperación	La organización retoma la operación normal de manera controlada.	Restaurar la información desde los respaldos. Validar que los datos estén completos e íntegros antes de reanudar operaciones. Comunicar a los clientes afectados de forma transparente y controlada.
6. Lecciones aprendidas	Se analiza qué ocurrió, por qué fue posible y qué se debe mejorar.	Documentar el incidente: qué pasó, qué lo permitió, cómo se respondió y qué cambios se implementarán para que no vuelva a ocurrir. Actualizar las políticas y controles según lo aprendido.

Nota. Elaboración propia con base en las fases de respuesta a incidentes trabajadas en la clase 7 del seminario (Ramírez, 2026). Las fases se adaptan al contexto y capacidad real del taller.

Más allá de responder al incidente, el taller necesita garantizar que pueda seguir operando mientras lo resuelve. Esto es lo que Ramírez (2026) denomina continuidad del negocio: la capacidad de mantener la operación activa incluso durante una situación adversa. Para el taller, los elementos mínimos de continuidad son tres. Primero, contar con respaldos periódicos que permitan restaurar la información en caso de pérdida. Segundo, documentar los procesos críticos —especialmente la atención al cliente y la facturación— de manera que más de una persona pueda ejecutarlos si el responsable habitual no está disponible. Tercero, definir un protocolo básico de operación manual para el caso en que los sistemas digitales fallen completamente: cuándo contactar a clientes, cómo registrar pedidos en papel y dónde guardar esos registros de forma segura.

A modo de ejemplo concreto: si el computador del administrador sufriera un daño físico irreparable un lunes en la mañana, la secuencia de respuesta para el taller hipotético sería la siguiente. En la fase de identificación, el administrador confirma que el equipo no enciende y que la información no es accesible. En contención, se suspenden temporalmente los registros digitales y se activa el protocolo de operación manual (libreta de pedidos y facturas físicas). En erradicación, se adquiere un equipo de reemplazo. En recuperación, se restaura la información desde el respaldo en la nube de la semana anterior. En lecciones aprendidas, se documenta que la información perdida corresponde a los movimientos del fin de semana, lo que motiva cambiar los respaldos de semanales a diarios. Sin el respaldo previo, la operación habría quedado paralizada indefinidamente.

6. Cultura organizacional en ciberseguridad

Todos los análisis anteriores —activos, amenazas, vulnerabilidades, riesgos, políticas, controles e incidentes— tienen un denominador común que aparece en cada punto: las personas. Detrás de cada decisión, cada error y cada acción que compromete la seguridad de la información hay un ser humano actuando. La clase 8 del seminario introdujo el concepto que integra todo lo anterior: la cultura organizacional en ciberseguridad, entendida como la forma en que las personas de una organización entienden, valoran y aplican la seguridad en su trabajo diario (Ramírez, 2026).

La cultura no son las normas escritas ni los documentos formales. La cultura es lo que ocurre cuando nadie está supervisando. Es lo que define si una persona valida un correo sospechoso antes de abrirlo o simplemente hace clic. Si alguien protege la información o la comparte por WhatsApp sin pensar. Si una política se cumple porque tiene sentido o se ignora porque nadie la exige. En ese sentido, la cultura organizacional puede ser el mayor riesgo de la organización o su control más efectivo.

Tabla 6.

Diagnóstico de cultura organizacional en ciberseguridad del taller.

Dimensión	Situación actual observada en el taller	Riesgo que genera	Mejora propuesta
Manejo de contraseñas	Las credenciales de acceso a los equipos son compartidas entre empleados. No existen contraseñas individuales.	Imposibilidad de rastrear quién accedió a qué. Acceso indebido sin responsable identificable.	Establecer contraseñas individuales y comunicar por qué es importante. Una sesión corta explicando el riesgo real puede ser suficiente para generar el cambio de hábito.
Comunicación de información	Los datos de clientes, pedidos y pagos se comparten por WhatsApp sin ningún criterio de seguridad.	Fuga de datos personales. Incumplimiento de la Ley 1581. Pérdida de confianza de los clientes.	Definir un canal oficial para comunicaciones que involucren datos sensibles y capacitar al personal sobre qué tipo de información no debe compartirse por mensajería informal.
Validación de solicitudes	El personal no tiene el hábito de verificar la autenticidad de solicitudes de información, sean por correo o por WhatsApp.	Alta vulnerabilidad a ataques de ingeniería social y phishing. Un mensaje fraudulento puede generar una fuga de datos sin que nadie lo detecte.	Socializar con el equipo dos o tres señales básicas de alerta: remitentes desconocidos, solicitudes urgentes de datos, enlaces externos no solicitados. No se necesita tecnología, solo criterio.
Percepción de la seguridad	La seguridad de la información no se percibe como un tema relevante. Nunca ha habido un incidente visible, lo que genera una falsa sensación de que "todo está bien".	La ausencia de cultura hace que los riesgos se normalicen y dejen de percibirse como tal, lo que aumenta la probabilidad de que se materialicen.	Compartir con el propietario y el equipo al menos un caso real de organización similar que sufrió un incidente. El impacto concreto de un caso cercano genera más conciencia que cualquier lista de reglas.
Documentación de procesos	Ningún proceso operativo está documentado. El conocimiento vive exclusivamente en la memoria de quienes lo ejecutan.	Si la persona clave no está disponible, el proceso se detiene. Esto afecta tanto la continuidad como la seguridad de la información.	Documentar al menos tres procesos críticos en una hoja sencilla: quién lo hace, cómo y qué información maneja. No necesita ser técnico; basta con que sea claro y accesible.

Nota. Elaboración propia con base en el análisis del caso hipotético y los conceptos de cultura organizacional trabajados en la clase 8 del seminario (Ramírez, 2026).

El diagnóstico hipotético del taller muestra que las personas no estarían fallando con mala intención sino actuando desde el desconocimiento en un contexto que nunca les exigió otra cosa. El cambio cultural requiere que el propietario asuma un rol activo: no basta con comunicar las nuevas políticas, debe modelarlas con su propio comportamiento. Si el propietario usa contraseñas individuales, verifica los respaldos y cuestiona el envío de datos sensibles por WhatsApp, el equipo lo incorpora como norma natural. Si los ignora, nadie más las tomará en serio. Para medir si las prácticas se están adoptando, el taller podría hacer tres verificaciones simples cada trimestre: confirmar que cada equipo tiene contraseña individual activa, revisar que los respaldos de la última semana existan y sean accesibles, y preguntarle a dos o tres colaboradores qué harían si

recibieran un mensaje pidiendo datos de un cliente por WhatsApp. Las respuestas revelan más sobre la cultura real que cualquier política escrita.

Conclusiones

Desarrollar este informe permitió recorrer, aplicado a un caso hipotético, el ciclo completo de la gestión de ciberseguridad organizacional que el seminario construyó clase a clase: identificación de activos, análisis de amenazas y vulnerabilidades, evaluación de riesgos, diseño de políticas y controles, preparación para la gestión de incidentes y diagnóstico de cultura organizacional. Cada sección no existe de manera aislada; todas están conectadas por una lógica que el docente repitió a lo largo del seminario: un problema de seguridad no es técnico, es organizacional.

El taller de maquinaria agrícola, aunque es un caso hipotético, representa con precisión a miles de organizaciones colombianas: opera bien, tiene clientes, genera ingresos, y sin embargo ninguno de sus activos más valiosos está protegido. La base de clientes vive en una hoja de cálculo sin contraseña. El conocimiento técnico de sus especialistas no está documentado en ningún lugar. Sus procesos críticos dependen de la memoria de quienes los ejecutan. Y sus datos circulan por WhatsApp sin ningún criterio de seguridad.

La matriz de riesgos evidenció que los tres riesgos más críticos del taller tienen probabilidad alta. No requieren un atacante externo para materializarse. Las políticas y controles propuestos responden directamente a esos riesgos, son aplicables a la realidad del negocio y no requieren inversiones tecnológicas complejas. El plan de respuesta a incidentes y los lineamientos de continuidad operativa aseguran que el taller pueda actuar con estructura si algo falla. Y el análisis de cultura organizacional deja claro que el cambio más importante no es tecnológico sino de comportamiento: las personas necesitan entender por qué la seguridad importa antes de que puedan aplicarla.

La ciberseguridad no se instala. Se gestiona. Y ese es el aprendizaje central de este proceso.

Referencias

Instituto Colombiano de Normas Técnicas y Certificación. (2022). NTC-ISO/IEC 27001: Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Requisitos. ICONTEC.

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

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

Ramírez Restrepo, J. L. (2026). Seminario de grado: Gestión de ciberseguridad en organizaciones [Material de clases, sesiones 1–5]. Corporación Universitaria Remington.

República de Colombia. (2012). Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial n.° 48.587. https://www.funcionpublica.gov.co

Superintendencia de Industria y Comercio. (2021). Guía para la implementación del principio de responsabilidad demostrada. SIC. https://www.sic.gov.co