TRABAJO DE GRADO
Opción Seminario.

Informe técnico de diagnóstico y propuesta de mejora para la gestión agroindustrial de la empresa AgroCampo del Futuro S.A.S.

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Estefany Patricia Martinez Vanegas

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen

Agrocampo del Futuro S.A.S. es una empresa colombiana que se encarga de cultivar, procesar y exportar productos agrícolas. Cuenta aproximadamente con 520 colaboradores entre fincas, centros de acopio, una planta de procesamiento y una oficina administrativa, y depende cada vez más de la tecnología para operar, usa un sistema ERP, plataformas de gestión agrícola, de relación con clientes y de exportaciones, también de servidores propios y en la nube. Este informe nace del diagnóstico inicial el cual presenta debilidades encontradas en el manejo de información de la empresa, entre estas el uso compartido de credenciales, aún registra excolaboradores activos, carece de seguridad en los dispositivos móviles y presenta en su cultura organizacional una creencia de que la seguridad es un tema únicamente del área de tecnología. Estas debilidades ya se han visto reflejadas en la realidad, como el acceso no autorizado a información comercial, un intento de fraude por correo electrónico y la pérdida de un dispositivo móvil en el área de trabajo.

El propósito de este informe es identificar los activos de información más relevantes de la empresa, reconocer amenazas y vulnerabilidades, valorar los riesgos asociados y proponer políticas, controles y recomendaciones que impulsen la protección de la información. Para esto se hizo una revisión en la información estructural de la empresa, su infraestructura tecnológica y los acontecimientos de seguridad registrados en los últimos tres años. Se obtuvo como resultado, la identificación de diez activos críticos relacionados con los sistemas de información, bases de datos y dispositivos que se usan en campo, se realizó la construcción de una matriz con los principales riesgos y se plantearon algunas políticas y controles con el fin de fortalecer el control de acceso, la protección de los dispositivos móviles y capacitación del personal. El informe concluyó que la empresa necesita principalmente fortalecer esos procesos internos y su cultura organizacional más allá de solo invertir en tecnología.

Palabras clave

Seguridad de la información, activos de información, cultura organizacional, vulnerabilidades, amenazas.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

La ciberseguridad se entiende como el conjunto de prácticas que buscan proteger los sistemas, las redes y la información frente a accesos no autorizados, daños o interrupciones (Unión Internacional de Telecomunicaciones [ITU], 2021). Dentro de este campo, la seguridad de la información se centra principalmente en proteger los datos de la organización, sin importar si están en físico, en un computador o en la nube (Whitman & Mattord, 2021). Un activo de información es cualquier elemento que tenga valor para la empresa porque procesa o transmite información: puede ser un sistema, un equipo, un documento o incluso las personas que la manejan (International Organization for Standardization [ISO], 2022). La seguridad de un activo se mide con tres características: la confidencialidad, que consiste únicamente en que la información solo pueda ser accedida por personal autorizado; la integridad, que la información se mantenga completa y sin cambios no autorizados; y la disponibilidad, que esté lista para usarse cuando sea necesaria (Whitman & Mattord, 2021).

Así mismo son importantes la amenaza, que es cualquier situación que pueda causar daño; la vulnerabilidad, que es una debilidad y el riesgo, que es la posibilidad de que una amenaza aproveche una vulnerabilidad y afecte a la organización (ISO, 2022). Frente a esto, los controles de seguridad son las medidas que se implementan para reducir un riesgo, ya sean con técnicas, como el cifrado, o de gestión, como una política interna (National Institute of Standards and Technology [NIST], 2018). En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones promueve que las empresas hagan uso de estos conceptos para gestionar sus riesgos e identificar sus activos de forma ordenada (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2016). Estos conceptos son la base de todo el análisis que se desarrolla en las siguientes secciones de este informe.

Marco normativo

Además de las bases conceptuales, es necesario revisar y tener en cuenta el marco normativo aplicable, ya que la empresa maneja información de trabajadores, clientes y operaciones internacionales.

Tabla 1. Normatividad aplicable.

Norma o estándar	Propósito	Aplicabilidad en la organización
Ley 1273 de 2009	Sanciona delitos informáticos, como el acceso no autorizado a sistemas.	Protege a la empresa frente a los intentos de acceso indebido detectados en sus sistemas.
Ley 1581 de 2012	Establece las reglas para proteger los datos personales.	Aplica a la información de los clientes y de los cerca de 520 colaboradores de la empresa.
Decreto 1377 de 2013	Reglamenta la Ley 1581 y define cómo debe manejarse el consentimiento.	Guía a la empresa sobre cómo debe tratar los datos personales que recolecta.
ISO/IEC 27001:2022	Da los requisitos para implementar un sistema de gestión de seguridad de la información.	Sirve de modelo para que la empresa organice sus políticas y controles de seguridad.
CONPES 3854 de 2016	Define la política nacional de seguridad digital en Colombia.	Orienta a la empresa sobre cómo gestionar los riesgos digitales de su operación.

Se resaltan estas normas porque le dan un marco legal a la protección de la información empresarial. La ley 1273 y la ley 1581, junto con su decreto reglamentario, exigen proteger tanto los sistemas como los datos personales, mientras que la norma ISO 27001 y la política nacional de seguridad digital ofrecen unas pautas para seguir procesos internos y reducir esos riesgos evidenciados en el informe.

Marco contextual

Descripción de la organización

Agrocampo del Futuro S.A.S. es una empresa colombiana con más de 20 años de experiencia en el sector agrícola. Se encarga de cultivar, procesar, exportar frutas y otros productos de alto valor y cuenta con cuatro fincas, dos centros de acopio, una planta de procesamiento y una oficina, tiene cerca de 520 colaboradores entre personal de campo, ingenieros agrónomos, personal administrativo y directivos, distribuidos en áreas como producción, comercial y exportaciones, logística, tecnología y sistemas, finanzas y talento humano.

En su parte tecnológica la empresa hace uso de un sistema ERP, un sistema de gestión agrícola, un sistema de monitoreo de cultivos, plataformas de exportaciones, CRM y respaldo, correo corporativo, servidores propios y en la nube, de computadores, dispositivos móviles y sensores en el campo. El área de tecnología y sistemas es pequeña frente al tamaño de la empresa, con apenas un coordinador, un administrador de infraestructura, dos analistas de soporte, un desarrollador y un analista de datos.

Problemática identificada

Un diagnóstico inicial y algunos eventos ocurridos en los últimos tres años muestran que la empresa tiene debilidades importantes en el manejo de su información. Hay supervisores que comparten sus credenciales, usuarios con más permisos de los necesarios, cuentas de excolaboradores aún activas, lo que ya terminó en un caso real de acceso no autorizado a información comercial.

Falta organización interna; no existe una política de clasificación de la información, no hay unos pasos definidos para atender incidentes, además las copias de respaldo no se han probado recientemente y algunos dispositivos móviles no tienen protección adecuada “uno se perdió en campo con información de producción” y la cultura de seguridad aún es débil, pues muchos colaboradores creen que este tema es solo del área de tecnología, otro acontecimiento alarmante que ocurrió fue que un colaborador cayó en un correo

fraudulento lo que casi lleva a un acceso indebido al sistema, un tema más común de lo que parece e incluso muestra que el riesgo no es solo teórico, se evidenció que hay un problema de actitud y conectividad en las fincas dicho problema parte de la resistencia de las personas a los controles y atraso de las actualizaciones en equipos. Esta situación justifica el desarrollo de este informe, ya que la empresa necesita entender mejor sus riesgos antes de que un incidente mayor afecte su operación o su reputación.

Identificación y análisis de activos

Inventario de activos

Partiendo de la infraestructura tecnológica de la empresa y del diagnóstico inicial, se identificaron los principales activos de información para la operación de Agrocampo del Futuro.

Tabla 2. Inventario de activos

Activo	Tipo	Descripción	Criticidad
Sistema ERP empresarial	Software	Prioriza la información administrativa, financiera y operativa de la empresa.	Alta
Sistema de gestión agrícola	Software	Se usa para planear y controlar la siembra, la cosecha y el manejo de los cultivos.	Alta
Sistema de monitoreo de cultivos	Software	Recibe los datos de los sensores instalados en las fincas.	Alta
Plataforma de seguimiento de exportaciones	Software	Administra los documentos y trámites necesarios para exportar los productos.	Alta
Correo electrónico corporativo	Software / Servicio	Es el canal oficial de comunicación con clientes, proveedores y entidades externas.	Alta
Infraestructura de servidores	Hardware / Servicio	Almacena los sistemas y las bases de datos de la empresa, tanto local como en la nube.	Alta
Base de datos de clientes	Información	Guarda los datos de contacto, contratos y transacciones comerciales.	Alta
Base de datos de colaboradores	Información	Contiene la información personal y laboral de los empleados.	Alta
Dispositivos móviles corporativos	Hardware	Celulares y tabletas usados en las labores de supervisión en campo.	Alta
Información financiera y contable	Información	Registros de presupuestos, pagos y estados financieros de la empresa.	Alta

De estos activos el sistema ERP, la infraestructura de servidores y las bases de datos de clientes y colaboradores son los más importantes porque de ellos depende gran parte de la operación diaria y porque contienen información sensible. El correo corporativo y los dispositivos móviles también son críticos ya que ambos han estado involucrados en situaciones de riesgo real dentro de la empresa, como el intento de fraude por correo y la pérdida de un equipo en campo.

Análisis de amenazas y vulnerabilidades

Para cada uno de los activos identificados se encontró una amenaza principal, una situación que podría afectarlo, y una vulnerabilidad, que es la debilidad que facilita que esa amenaza se pueda aprovechar.

Tabla 3. Amenazas y vulnerabilidades

Activo	Amenaza	Vulnerabilidad
Sistema ERP empresarial	Acceso no autorizado o falla del sistema.	Usuarios con más permisos de los que necesitan para su trabajo.
Sistema de gestión agrícola	Manipulación o pérdida de datos de siembra y cosecha.	Uso de credenciales compartidas entre varios supervisores.
Sistema de monitoreo de cultivos	Interrupción del servicio o ingreso indebido.	Accesos administrativos sin autenticación multifactor.
Plataforma de exportaciones	Manipulación de documentos o trámites.	Falta de una política clara de acceso a la información.
Correo electrónico corporativo	Suplantación de identidad y correos fraudulentos.	Poca capacitación del personal y exceso de confianza en remitentes externos.
Infraestructura de servidores	Caída de servidores o ataque externo.	Falta de monitoreo continuo y actualizaciones de seguridad en los servidores.
Base de datos de clientes	Acceso no autorizado a información comercial (ya ocurrió).	Controles de acceso débiles y credenciales compartidas.
Base de datos de colaboradores	Filtración de datos personales de los empleados.	No existe una política de clasificación de la información.
Dispositivos móviles corporativos	Pérdida o robo del equipo en campo (ya ocurrió un caso).	Varios dispositivos no cuentan con protección adecuada.
Información financiera y contable	Fraude o manipulación de registros contables.	Controles de acceso insuficientes a la información financiera.

Las situaciones más críticas son las relacionadas con el acceso a las bases de datos y al correo corporativo, ya que ambos activos ya sufrieron intentos reales de acceso no autorizado, y las vulnerabilidades que los rodean, como las credenciales compartidas y la falta de capacitación del personal, siguen presentes en la empresa. La pérdida de dispositivos móviles también representa un riesgo alto, porque estos equipos se usan fuera de campo y contienen información de producción y logística.

Análisis y gestión de riesgos

Metodología de análisis

Para valorar los riesgos se usó una escala simple de tres niveles alto, medio y bajo. Esta escala se aplicó a dos aspectos de cada riesgo: el impacto, que mide qué tan grave sería para la empresa si el riesgo se llegara a realizar y la probabilidad, que mide qué tan posible es que eso ocurra teniendo en cuenta las vulnerabilidades ya identificadas. Al combinar estos dos puntos se obtiene el nivel final del riesgo.

Esta forma de valorar los riesgos sigue la lógica que normalmente proponen estándares como la ISO 31000, que recomienda identificar, evaluar y analizar los riesgos antes de decidir cómo tratarlos (International Organization for Standardization [ISO], 2018), y las guías del NIST para la evaluación de riesgos de seguridad de la información (Ross, 2012). Incluso se tuvo en cuenta que cuando el impacto y la probabilidad son altos, la organización debe atender ese riesgo de manera prioritaria (Whitman & Mattord, 2021).

Para determinar el nivel de riesgo se estableció que cuando el nivel es alto, es decir cuando las consecuencias de este riesgo son graves para la empresa incluso si su probabilidad no es alta, su nivel es automáticamente alto, esto basado en darle prioridad a la gravedad de la consecuencia sobre la frecuencia esperada, como lo sugiere la ISO 31000.

Matriz de riesgos

Tabla 4. Matriz de riesgos

Riesgo	Impacto	Probabilidad	Nivel
Acceso no autorizado a las bases de datos por uso de credenciales compartidas	Alto	Alta	Alto
Pérdida de información por fallas en las copias de respaldo	Alto	Media	Alto
Ataques de phishing a través del correo corporativo	Alto	Alta	Alto
Pérdida o robo de dispositivos móviles en actividades de campo	Medio	Alta	Alto
Interrupción del sistema ERP por una falla técnica o un ataque	Alto	Media	Alto

Riesgo	Impacto	Probabilidad	Nivel
Manipulación de los datos del sistema de monitoreo de cultivos	Medio	Media	Medio
Retraso en las actualizaciones de seguridad de los equipos rurales	Medio	Media	Medio
Conexión de personas no autorizadas a la red WiFi corporativa	Bajo	Media	Bajo

Los riesgos de alto nivel son los que la empresa debería atender primero, el acceso no autorizado a las bases de datos, la pérdida de información por falencias en el respaldo, los ataques de phishing y la pérdida de dispositivos móviles. Estos cuatro riesgos comparten una característica, ya se relacionan con hechos que ocurrieron en la empresa, lo que confirma que no son solo una posibilidad teórica, sino una situación que ya se vivió y que puede repetirse si no se atienden.

Para riesgos como “pérdida de información por fallas en las copias de respaldo”, aunque su probabilidad es media ya que no hay evidencia de fallas frecuentes, el impacto es alto ya que la empresa depende de esta información para su operación diaria y no tiene un proceso de pruebas de restauración verificado, lo que empeora las consecuencias si dicho respaldo fallara. Para la “interrupción del sistema ERP”, este concentra la información administrativa, financiera y operativa de la empresa, una interrupción así no sea frecuente entorpecería procesos importantes de los 520 colaboradores, esto justifica el riesgo alto aunque su probabilidad sea media.

Políticas y controles de seguridad

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	Objetivo	Riesgo asociado
Política de control de acceso	Garantizar que cada persona tenga solo los permisos que necesita para su trabajo.	Acceso no autorizado a las bases de datos.
Política de uso de contraseñas y autenticación	Evitar el uso de credenciales compartidas y exigir un segundo factor de verificación.	Acceso no autorizado a los sistemas.
Política de copias de seguridad	Asegurar que la información se pueda recuperar ante cualquier suceso.	Pérdida de información.
Política de uso de dispositivos móviles	Proteger la información que se usa fuera de las instalaciones de la empresa.	Pérdida o robo de dispositivos móviles.
Política de seguridad en el correo electrónico	Reducir el riesgo de fraudes y de correos maliciosos.	Ataques de phishing.

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	Control	Justificación
Acceso no autorizado a las bases de datos	Autenticación multifactor y eliminación de cuentas de excolaboradores.	Reduce la posibilidad de que alguien entre sin permiso.
Pérdida de información por fallas en el respaldo	Pruebas periódicas de restauración de las copias de seguridad.	Garantiza que la información realmente se pueda recuperar.
Ataques de phishing en el correo	Capacitaciones regulares y filtros de seguridad en el correo.	Disminuye la probabilidad de que un colaborador caiga en un engaño.
Pérdida de dispositivos móviles	Cifrado de la información y bloqueo remoto de los equipos.	Protege los datos aunque el dispositivo se pierda o sea robado.
Falla del sistema ERP	Mantenimiento preventivo y monitoreo constante de los servidores.	Permite detectar fallas antes de que afecten la operación.

Dichas políticas y controles tienen como fin mitigar los riesgos con el nivel más alto identificados en la matriz anterior. El control de acceso y la autenticación multifactor

reducen la posibilidad de accesos no autorizados a las bases de datos, las pruebas de restauración garantizan que la información realmente se pueda recuperar, y las capacitaciones y el cifrado de los dispositivos móviles atienden los riesgos relacionados con el correo electrónico y la pérdida de equipos en campo.

Gestión de incidentes y continuidad del negocio

La empresa debe estar preparada para reaccionar si un incidente llega a ocurrir.

Tabla 7. Incidentes potenciales

Incidente	Descripción	Impacto
Acceso no autorizado a la base de datos de clientes	Alguien ingresa al sistema usando credenciales de otra persona.	Exposición de información comercial y pérdida de confianza de los clientes.
Pérdida de un dispositivo móvil con información sensible	Un equipo se extravía durante una actividad de supervisión en campo.	Posible filtración de datos de producción y logística.
Ataque de phishing exitoso	Un colaborador da clic en un enlace fraudulento recibido por correo.	Acceso indebido a los sistemas corporativos.
Falla en los servidores principales	Los servidores dejan de funcionar por una falla técnica o un ataque.	Interrupción de la operación y de los procesos administrativos.

Para responder a este tipo de situaciones se propone un plan básico organizado en cuatro fases, que permite actuar de forma ordenada desde el momento en que se detecta un problema hasta que se resuelve por completo.

Tabla 8. Plan básico de respuesta

Fase	Acción
Detección	Identificar y confirmar que el incidente está ocurriendo, usando alertas del sistema o reportes del personal.
Contención	Aislar el sistema, la cuenta o el equipo afectado para evitar que el problema se extienda.
Erradicación y recuperación	Eliminar la causa del incidente y restaurar la información o el sistema afectado con las copias de seguridad.
Comunicación y aprendizaje	Informar a los responsables y a los afectados, y documentar lo ocurrido para evitar que se repita.

Con este plan la empresa podría responder de manera más rápida y ordenada ante un incidente, reduciendo el tiempo en que un sistema permanece afectado y facilitando que la operación vuelva a la normalidad, así mismo la fase de comunicación y aprendizaje permite que cada incidente deje una enseñanza que ayude a evitar que se repita.

Cultura organizacional en ciberseguridad

Más allá de la tecnología la forma en que las personas de la empresa entienden y aplican la seguridad de la información también influye en el nivel de riesgo.

Tabla 9. Hallazgos organizacionales

Situación observada	Riesgo asociado
Muchos colaboradores creen que la seguridad es responsabilidad solo del área de tecnología.	Baja participación de todo el personal en el cuidado de la información.
Las capacitaciones sobre seguridad son esporádicas.	El personal no está preparado para reconocer amenazas como el phishing.
Existe resistencia a adoptar nuevos controles.	Los controles que se implementen podrían no usarse de forma correcta.
Algunos incidentes menores no se reportan a tiempo.	Los problemas se detectan cuando ya son más graves.

Tabla 10. Recomendaciones de mejora

Hallazgo	Recomendación
Falta de participación general en el cuidado de la información.	Incluir la seguridad de la información como responsabilidad de todas las áreas, no solo de tecnología.
Capacitaciones esporádicas.	Establecer capacitaciones cortas y periódicas sobre buenas prácticas de seguridad.
Resistencia a los nuevos controles.	Explicar al personal el motivo de cada control, usando ejemplos reales de la empresa.
Reporte tardío de incidentes.	Crear un canal sencillo y rápido para que cualquier persona reporte una situación sospechosa.

Estas mejoras buscan que la seguridad de la información deje de verse como una tarea exclusiva del área de tecnología y se convierta en una responsabilidad de todos los colaboradores, capacitar al personal, explicar el por qué de cada control y facilitar el reporte de situaciones extrañas son pasos sencillos que con el tiempo pueden fortalecer la cultura de seguridad de la empresa.

Conclusiones

Agrocampo del Futuro S.A.S. depende cada vez más de la tecnología para operar, pero su forma de proteger la información no ha crecido de la misma forma, lo que la deja expuesta a riesgos que ya se han convertido en hechos reales.

Los activos más críticos de la empresa son los sistemas que sostienen su operación día a día, las bases de datos de clientes y colaboradores, el correo corporativo y los dispositivos móviles usados en campo, ya que todos han estado relacionados con situaciones de riesgo puntuales.

Los riesgos de alto nivel son los que están relacionados con el control de acceso a la información y con el factor humano, especialmente con el manejo del correo electrónico y de los dispositivos móviles, lo que evidencia que las soluciones no son solo en la parte técnica, sino en procesos y en comportamientos del personal.

Las políticas y los controles propuestos en este informe son medidas alcanzables para una empresa de este tamaño, y su implementación no depende solamente de invertir en tecnología, sino de ordenar procesos que hoy no existen, como la clasificación de la información o la rápida atención de incidentes.

Fortalecer la cultura organizacional en seguridad de la información es tan importante como cualquier control técnico, ya que gran parte de los riesgos identificados en este informe se originan en malas prácticas cotidianas del personal que pueden corregirse con capacitación, comunicación y acompañamiento constante por parte de la empresa.

Referencias

Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea el bien jurídico de la protección de la información y de los datos. Diario Oficial. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

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. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Departamento Nacional de Planeación. (2016). CONPES 3854. Política Nacional de Seguridad Digital. DNP. https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx

International Organization for Standardization. (2018). ISO 31000:2018. Gestión del riesgo — Directrices. https://www.iso.org/standard/65694.html

International Organization for Standardization. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/27001

International Telecommunication Union. (2021). Definitions related to cybersecurity. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información.

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/w3-propertyvalue-49984.html

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (versión 1.1). https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Ross, R. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, revisión 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage Learning. https://www.cengage.com/c/principles-of-information-security-7e-whitman-mattord/9780357506431/