TRABAJO DE GRADO

Opción Seminario-Diplomado.

Análisis de Ciberseguridad Organizacional: Caso FERTIBUGA S.A.S.

Informe Técnico Preliminar – Versión para Revisión

Seminario

Corporación Universitaria Remington

Facultad de Ingeniería y Tecnologías de la Información

Ingeniería de Sistemas – Seminario Ciberseguridad Empresarial

Nicolás Zapata– Estudiante

Uriel Esteban Cuadros - Estudiante

Docente Seminario - Jorge Leonardo Ramírez Restrepo

Seminario Ciberseguridad Empresarial

2026

Tabla de Contenidos

Tabla de Contenidos 2

Resumen 4

1. Marco Conceptual y Contextual 5

1.1 Marco Conceptual 5

1.2 Marco Contextual 6

2. Desarrollo e Implementación del Aprendizaje 7

2.1 El Incidente Principal: "La Cadena Rota" 7

2.2 Identificación y Valoración de Activos 7

2.3 Criterios CIA y priorización 7

2.4 Amenazas y Vulnerabilidades 9

2.5 Impacto operativo en FERTIBUGA 10

2.6 Matriz de Riesgos 11

2.7 Políticas y Controles 12

2.8 Incidentes y Respuesta 15

2.9 Valor del plan de continuidad 17

2.10 Cultura Organizacional 18

2.11 Indicadores de evolución cultural 19

3. Impacto del Incidente Global 21

4. Conclusiones 22

5. Referencias 23

Resumen

Este informe aplica los conceptos del Seminario de Ciberseguridad Empresarial al caso hipotético de FERTIBUGA S.A.S., empresa agroindustrial del Valle del Cauca con 140 empleados y facturación simulada de $8.200 millones COP. Se identifican activos críticos, se evalúan riesgos del entorno OT/IT y se proponen controles alineados con la Ley 1273/2009, la Ley 1581/2012 y estándares como ISO/IEC 27001:2022 (ISO, 2022a) e IEC 62443 (IEC, 2018).

El análisis identificó 24 activos en seis categorías, diez con criticidad CIA ≥ 8, y cuatro riesgos máximos independientes entre sí. El incidente principal *"La Cadena Rota"* combinó phishing, sabotaje industrial y ransomware, provocando 7 días de parálisis total. Las tres medidas prioritarias son: segmentación de red OT/IT, autenticación multifactor (MFA) y backup 3-2-1 automatizado.

Nota aclaratoria: *FERTIBUGA S.A.S. es una empresa ficticia de uso académico. Todos los datos, incidentes y sistemas descritos son simulados con fines formativos.*

Palabras clave: *ciberseguridad organizacional, activos de información, gestión de riesgos, ISO 27001, seguridad industrial OT/IT.*

1. Marco Conceptual y Contextual

1.1 Marco Conceptual

La ciberseguridad organizacional protege los sistemas de información, redes y datos de una empresa frente a accesos no autorizados, daños o interrupciones (ISO, 2022a). Para FERTIBUGA, con entornos IT y OT integrados, esto no es solo un asunto técnico: determina si la planta puede producir, si los despachos son exactos y si los datos de los clientes están resguardados.

Marcos normativos aplicados al caso FERTIBUGA

Cada estándar utilizado tiene una consecuencia operativa directa en el caso, no solo una función de referencia bibliográfica:

ISO/IEC 27001:2022 (ISO, 2022a): exige inventario de activos, revisión de riesgos documentada y controles verificables. En FERTIBUGA ninguno existía; por eso el backup manual llevaba 18 días sin ejecutarse sin que nadie lo detectara.

IEC 62443 (IEC, 2018): obliga a separar la red de control industrial (OT) de la red de oficinas (IT). FERTIBUGA los tenía integrados, lo que permitió que un correo malicioso abierto en planta cifrara los servidores de toda la empresa.

ISO/IEC 27005:2022 (ISO, 2022b): guía el análisis de riesgos del informe. Su aplicación significó relacionar cada riesgo con el activo afectado y su impacto operativo concreto: días de producción perdidos, despachos comprometidos, cooperativas sin suministro.

Ley 1273/2009 (Congreso de Colombia, 2009): tipifica el acceso abusivo a sistemas informáticos (art. 269A) y el daño informático (art. 269D), delitos que se materializaron en el incidente principal. FERTIBUGA fue víctima de delitos penales y debió haber notificado a la Fiscalía.

Ley 1581/2012 (Congreso de Colombia, 2012): obliga a registrar las bases de datos de clientes ante la SIC y publicar una política de privacidad. FERTIBUGA almacena datos de 3.200 clientes sin

cumplir ninguno de los dos requisitos, lo que configura un incumplimiento activo sancionable con hasta 2.000 SMLMV.

ISO 22301:2019 (ISO, 2019): establece cómo mantener la operación durante y después de un incidente. FERTIBUGA no tenía ningún plan de continuidad; los despachos se manejaron en papel durante 7 días de forma improvisada. Con un plan activo, ese tiempo se habría reducido a menos de 48 horas.

1.2 Marco Contextual

FERTIBUGA S.A.S. simula una empresa agroquímica del Valle del Cauca que recibe materias primas (urea, fosfatos, sulfatos), las procesa con control de proporciones y temperatura, y despacha con trazabilidad hacia cooperativas agrícolas. Opera bajo certificaciones ICA (Resolución 150/2003) y NTC 5167.

Su infraestructura combina sistemas de distintas generaciones que representan brechas de seguridad típicas de la industria colombiana. En el entorno IT: SAP Business One 9.3 sin soporte activo, dos servidores Windows Server 2016, un NAS accesible como unidad Z:, correo Microsoft 365 E1 y una aplicación de despachos en PHP 7.2 sin auditorías desde 2018. En el entorno OT: un SCADA conectado directamente a la red corporativa sin segmentación, que constituye la vulnerabilidad central del caso.

Esta combinación de sistemas obsoletos, redes sin segmentar y respaldos sin monitoreo configura la superficie de ataque sobre la que se desarrolla el análisis.

2. Desarrollo e Implementación del Aprendizaje

Esta sección aplica los contenidos del seminario al caso FERTIBUGA: se analiza el incidente principal, se valoran los activos, se identifican riesgos, se proponen controles y se examina el papel de la cultura organizacional.

2.1 El Incidente Principal: "La Cadena Rota"

Un operario abrió un correo malicioso desde el PC de control de producción. Dado que la red OT no tenía separación de la red corporativa, el atacante modificó silenciosamente las básculas del SCADA (1.847 sacos con 8% menos de peso durante cuatro días), encontró contraseñas en texto plano en el mismo escritorio y con ellas accedió al servidor SAP. Finalmente cifró en 90 minutos todos los archivos, incluidas las copias de seguridad conectadas a la misma red.

El resultado fue 7 días de parálisis total, un rescate de $85.000 USD, fraude a 23 cooperativas y exposición simultánea ante las leyes 1273, 1581 y 1480 (Congreso de Colombia, 2009, 2011, 2012). La empresa no detectó el ataque por sus propios medios: fueron las cooperativas quienes reportaron el problema del peso varios días después.

2.2 Identificación y Valoración de Activos

Se identificaron 24 activos en seis categorías (datos, software, hardware, servicios, personas y procesos), siguiendo la taxonomía de ISO/IEC 27001:2022 (ISO, 2022a).

2.3 Criterios CIA y priorización

Cada activo se valoró con el modelo CIA (Confidencialidad, Integridad, Disponibilidad), escala 1–3 por dimensión. Puntaje total 7–9: ALTO/CRÍTICO; 5–6: MEDIO; 3–4: BAJO.

Confidencialidad (C): gravedad si alguien no autorizado accede al activo. Las fórmulas de producción, si se filtran a un competidor, generan pérdida irreversible (C=3); la lista de proveedores tiene un impacto menor (C=2).

Integridad (I): gravedad si el activo es modificado sin autorización. El SCADA alterado en el incidente generó fraude en 1.847 despachos (I=3); el firmware de cámaras tiene menor riesgo de integridad (I=2).

Disponibilidad (D): gravedad si el activo deja de funcionar. Sin SAP no es posible facturar ni comprometer despachos (D=3); sin tablets de logística, el proceso puede hacerse en papel temporalmente (D=2).

La priorización usó tres criterios: participación directa en el incidente documentado, consecuencias legales ante su compromiso (Ley 1581/2012 o Ley 1273/2009) y capacidad de generar daño físico o fraude al consumidor (SCADA y PLCs). La tabla siguiente presenta los 24 activos con su valoración.

#	Activo	Categoría	C	I	D	Total	Nivel
1	Base de datos de clientes	Datos	3	2	3	8	CRÍTICO
2	Fórmulas de fertilizantes	Datos	3	3	2	8	CRÍTICO
3	Registros de pesaje y trazabilidad	Datos	2	3	3	8	CRÍTICO
4	Registros financieros y DIAN	Datos	2	3	2	7	ALTO
5	Información de proveedores	Datos	2	2	2	6	MEDIO
6	SAP Business One 9.3	Software	2	3	3	8	CRÍTICO
7	Sistema SCADA	Software	2	3	3	8	CRÍTICO
8	App despachos PHP 7.2	Software	2	3	3	8	CRÍTICO
9	Microsoft 365 E1 (correo)	Software	2	2	3	7	ALTO
10	Servidores físicos (×2)	Hardware	2	3	3	8	CRÍTICO
11	NAS de backup (unidad Z:)	Hardware	2	2	3	7	ALTO
12	PLCs mezcladoras Allen-Bradley	Hardware	2	3	3	8	CRÍTICO
13	Cámaras IP (×22)	Hardware	2	2	2	6	MEDIO
14	Tablets de logística (×8)	Hardware	2	1	2	5	MEDIO

#	Activo	Categoría	C	I	D	Total	Nivel
15	PCs de planta (red OT)	Hardware	1	3	3	7	ALTO
16	VPN proveedor SAP	Servicios	3	2	2	7	ALTO
17	Facturación electrónica DIAN	Servicios	2	3	2	7	ALTO
18	Red Wi-Fi visitantes	Servicios	1	1	2	4	BAJO
19	Conexión a internet principal	Servicios	1	1	3	5	MEDIO
20	Jefe de Sistemas	Personas	3	3	3	9	CRÍTICO
21	Operarios de planta	Personas	2	3	2	7	ALTO
22	Vendedores (equipo comercial)	Personas	3	2	2	7	ALTO
23	Proveedor externo SAP	Personas	3	2	2	7	ALTO
24	Gestión de backups	Procesos	2	3	3	8	CRÍTICO

2.4 Amenazas y Vulnerabilidades

Una amenaza es cualquier agente externo con potencial de daño; una vulnerabilidad, la debilidad interna que lo hace posible (ISO, 2022b). La tabla siguiente relaciona ambas con los activos del caso, partiendo de situaciones concretas de FERTIBUGA.

Activo	Amenaza	Vulnerabilidad	Prob.	Impacto	Nivel
Servidor + NAS	Ransomware vía phishing en PC de control industrial	NAS montado como unidad Z: sin aislamiento; macros Office habilitadas; red OT/IT sin segmentar	Alta	Alta	CRÍTICO
BD clientes (SAP)	SQL Injection por app PHP 7.2	Consultas sin parametrización; sin auditoría desde 2018; sin WAF; 3.200 registros expuestos	Media	Alta	ALTO

Activo	Amenaza	Vulnerabilidad	Prob.	Impacto	Nivel
VPN / Servidor / SCADA	Acceso con credenciales comprometidas	VPN compartida entre 3 técnicos sin MFA; contraseñas en texto plano; sin revocación al terminar contratos	Alta	Alta	CRÍTICO
SCADA / PLCs	Manipulación de parámetros OT por pivoting	Red OT sin segmentar; sesión SCADA siempre abierta; alarmas desactivadas sin protocolo formal	Media	Alta	CRÍTICO
Fórmulas / contratos	Exfiltración interna por USB	Sin restricciones DLP; acceso total a fórmulas sin mínimo privilegio; sin clasificación de información	Media	Alta	ALTO
Infraestructura global	Pérdida total por backup deficiente	Backup manual sin monitoreo; NAS en misma red; sin verificación de integridad	Alta	Alta	CRÍTICO
Cámaras IP (×22)	Espionaje por dispositivos IoT expuestos	Credenciales admin/admin de fábrica; 4 CVEs críticos sin parchear desde 2021; sin VLAN dedicada	Media	Alta	ALTO

2.5 Impacto operativo en FERTIBUGA

Caída del SCADA: sin control de mezcla y pesaje, la planta no cumple las especificaciones exigidas por el ICA. En el incidente, 1.847 sacos salieron con 8% menos de peso, generando sanciones por Ley 1480/2011 y riesgo de cancelación del registro ICA.

Caída del SAP: sin ERP no es posible emitir facturas electrónicas válidas ante la DIAN ni controlar el inventario de materias primas. En el incidente, la empresa operó en papel durante 7 días con riesgo de doble facturación al normalizar.

Caída del sistema de trazabilidad: sin registro de lotes, ante un problema de calidad no es posible identificar qué cooperativas recibieron el producto afectado. Esto expone a FERTIBUGA a responsabilidad por pérdidas de cosecha, que pueden superar ampliamente el valor del fertilizante vendido.

2.6 Matriz de Riesgos

La matriz usa escala P×I (1–3 c/u). El hallazgo más relevante es que los cuatro riesgos con índice máximo son independientes entre sí: cualquiera puede ocurrir sin que los demás estén activos. Esto confirma una vulnerabilidad estructural que requiere atención simultánea en varios frentes.

Activo	Amenaza	Vulnerabilidad principal	Prob.	Impacto	Nivel
Servidor + NAS	Ransomware (phishing)	Red OT/IT sin segmentar; NAS en misma red	Alta (3)	Alta (3)	CRÍTICO (9)
BD clientes (SAP)	SQL Injection	PHP 7.2 sin soporte; sin parametrización	Alta (3)	Alta (3)	CRÍTICO (9)
VPN / Servidor / SCADA	Acceso con credenciales comprometidas	Sin MFA; credenciales compartidas; sin revocación	Alta (3)	Alta (3)	CRÍTICO (9)
Infraestructura global	Pérdida total por backup deficiente	Backup manual; NAS sin aislamiento; sin verificación de integridad	Alta (3)	Alta (3)	CRÍTICO (9)
SCADA / PLCs	Sabotaje OT por pivoting	Red OT sin segmentar; sesión	Media (2)	Alta (3)	ALTO (6)

Activo	Amenaza	Vulnerabilidad principal	Prob.	Impacto	Nivel
		SCADA siempre abierta			
Fórmulas / contratos	Exfiltración interna USB	Sin DLP; sin mínimo privilegio	Media (2)	Alta (3)	ALTO (6)
Cámaras IP	Espionaje IoT	Credenciales de fábrica; firmware sin actualizar	Alta (3)	Media (2)	ALTO (6)
VPN proveedor SAP	Acceso persistente exproveedor	Sin revocación; logs desactivados; sin SIEM	Media (2)	Alta (3)	ALTO (6)

2.7 Políticas y Controles

Cada medida responde a un problema concreto del caso. La columna de justificación indica quién es responsable, cómo se verifica y con qué periodicidad, conectando el control con el incidente que lo origina.

#	Control / Política	Marco de referencia	Plazo	Justificación operativa	Tipo
1	Segmentar red OT/IT con firewall industrial y VLAN dedicada para planta	IEC 62443, ISO 27001 A.13	0–30 días	Sin esta separación, cualquier equipo de oficina o planta es una puerta de entrada al SCADA y a los servidores. Responsable: Jefe de Sistemas con soporte del proveedor de red. Verificación: prueba de aislamiento donde desde un PC de oficina no sea posible acceder a la IP del SCADA.	Técnico
2	MFA en VPN del proveedor SAP; revocar accesos al terminar contratos	ISO 27001 A.8.2, NIST CSF	0–15 días	Cada técnico del proveedor debe tener credenciales individuales con doble verificación. Al terminar el contrato, el Jefe de Sistemas ejecuta la revocación el mismo día y deja registro firmado. Auditoría trimestral:	Técnico

#	Control / Política	Marco de referencia	Plazo	Justificación operativa	Tipo
				listar todas las cuentas VPN activas y validar que correspondan a contratos vigentes.	
3	Backup 3-2-1 automatizado con verificación semanal de integridad	ISO 22301, ISO 27001 A.8.13	0–30 días	Tres copias, en dos medios distintos, una fuera de la red local (nube o disco físico desconectado). El sistema envía un reporte automático cada lunes confirmando que el backup del fin de semana fue exitoso. Responsable de revisión del reporte: Jefe de Sistemas. Sin confirmación, se escala a gerencia ese mismo día.	Técnico
4	Migrar aplicación de despachos: reemplazar PHP 7.2 por framework moderno con consultas parametrizadas	Ley 1273, ISO 27002 A.8.28	30–60 días	Responsable: Jefe de Sistemas con el desarrollador de la app. Antes de la migración, contratar una auditoría de seguridad básica (prueba de penetración). Después de la migración, auditoría anual. Mientras tanto, limitar el acceso a la app solo desde la red interna.	Técnico
5	DLP: bloquear puertos USB en producción, laboratorio y área comercial	Ley 256/1996, ISO 27002 A.8.12	15–45 días	Configuración desde el directorio activo o software de endpoint. Responsable: Jefe de Sistemas. Excepción documentada y firmada por gerencia para casos de necesidad. Verificación semestral: intento controlado de transferencia USB para confirmar que el bloqueo funciona.	Técnico
6	SIEM con monitoreo de logs de VPN, servidor y SCADA	NIST CSF DE.CM, ISO 27001 A.8.15	30–60 días	Administrador del SIEM: responsable de seguridad alterno (designado en Control 10). Revisión de alertas:	Técnico

#	Control / Política	Marco de referencia	Plazo	Justificación operativa	Tipo
				diaria para eventos críticos, semanal para resumen general. Las VPN se auditan comparando el registro de accesos remotos contra el calendario de mantenimientos programados del proveedor SAP. Cualquier acceso fuera de ventana programada genera alerta inmediata.	
7	Cambiar credenciales de cámaras IP; actualizar firmware; asignar VLAN independiente	ISO 27001 A.7.4	15–30 días	Responsable: Jefe de Sistemas. Lista de las 22 cámaras con firmware actualizado y nueva contraseña: entregada a gerencia como evidencia. Verificación semestral: escaneo con herramienta básica para confirmar que ninguna cámara responde con credenciales de fábrica.	Técnico
8	Capacitación antiphishing mensual; deshabilitar macros Office por defecto	ISO 27001 A.6.3	0–30 días	Responsable: área de RRHH con soporte del Jefe de Sistemas. Cumplimiento verificado con lista de asistencia firmada y resultado del simulacro por empleado. Empleados que no superen el simulacro reciben refuerzo individual. Reporte trimestral a gerencia con tasa de aprobación (meta: 90%).	Factor humano
9	Registrar base de datos en RNBD-SIC; publicar política de privacidad (Decreto 1377)	Ley 1581, Dto. 1377	0–20 días	Responsable: gerencia con apoyo de asesor jurídico. El registro en la SIC es un trámite en línea. La política de privacidad debe estar publicada en la web de la empresa y entregada físicamente a los clientes al momento de firma de contrato. Verificación anual:	Legal

#	Control / Política	Marco de referencia	Plazo	Justificación operativa	Tipo
				confirmar que el registro sigue vigente y que la política está actualizada.	
10	Mínimo privilegio en SAP y SCADA; designar responsable de seguridad alterno documentado	ISO 27001 A.8.2	30–45 días	El alterno recibe capacitación documentada sobre los sistemas críticos y queda registrado formalmente en el organigrama de seguridad. En SAP: perfiles revisados para que cada usuario acceda solo a los módulos que necesita. Verificación semestral de perfiles activos. El alterno también es quien administra el SIEM (Control 6) y revisa el reporte semanal de backups (Control 3).	Proceso

2.8 Incidentes y Respuesta

El análisis sigue las fases del estándar ISO/IEC 27035:2023 (ISO, 2023): identificación, contención, erradicación, recuperación y continuidad. Cada fase se relaciona con los controles propuestos en la sección anterior.

Fase	Descripción en el caso	Análisis / lección aprendida	Control relacionado
Tipo de incidente	Phishing + sabotaje OT + ransomware encadenados (ataque múltiple)	Ninguno de los tres tipos requirió técnicas avanzadas. Su efecto combinado fue posible exclusivamente por la coexistencia de tres capas de falla: tecnológica, de proceso y humana.	Controles 1, 2, 3, 8
¿Qué ocurrió?	Phishing en PC de planta → RAT → SCADA modificado (pesaje −8%) → 1.847 sacos fraudulentos en 4 días → pivoting con contraseñas en	La secuencia completa fue: engaño → acceso silencioso → modificación de producción → pivoting → cifrado total. La red OT/IT sin	Controles 1, 3

Fase	Descripción en el caso	Análisis / lección aprendida	Control relacionado
	texto plano → LockBit cifra servidor y NAS en 90 min → 7 días de parálisis total	segmentar y el NAS sin aislamiento convirtieron un ataque de alcance limitado en un evento de impacto máximo.	
¿Qué lo permitió?	(1) Red OT/IT sin segmentar. (2) Sesión SCADA siempre abierta. (3) Contraseñas en texto plano en el escritorio. (4) NAS montado como unidad Z:. (5) Jefe de Sistemas de incapacidad sin reemplazo documentado. (6) Alarmas SCADA desactivadas.	Ninguna falla era catastrófica de forma individual. Su coexistencia simultánea fue la condición que transformó el incidente. Esto subraya la necesidad de un enfoque sistémico, no de correcciones puntuales.	Controles 1, 3, 6, 8, 10
Identificación	Detección tardía: el operario notó la anomalía en el SCADA 90 min después del compromiso. Las cooperativas reportaron el peso incorrecto entre los días 2 y 4.	Sin SIEM y con alarmas desactivadas, la detección dependió de quejas externas. Evidencia clara de falla en el componente 'Detectar' del NIST CSF 2.0.	Control 6
Contención	Desconexión manual del servidor (vie. 09:30). Revocación de acceso VPN del proveedor SAP. Aislamiento físico del PC de planta y del NAS. Comunicación de emergencia a comercial y logística.	Contención reactiva e improvisada por ausencia de protocolo documentado. Se evitó propagación adicional, pero el tiempo de reacción ya había permitido el impacto multidimensional.	Controles 2, 6
Erradicación	Formateo y reinstalación de servidores. Cambio forzado de todas las credenciales. Análisis forense externo para identificar y eliminar el RAT. Cierre permanente de la sesión VPN comprometida.	Se eliminó la causa raíz. La ausencia de backups limpios y verificados obligó a reinstalar parcialmente desde cero, alargando el tiempo de recuperación de forma significativa.	Controles 2, 3
Recuperación	Restauración parcial desde backup del martes anterior	Sin backup 3-2-1 ni verificación de integridad, la	Control 3

Fase	Descripción en el caso	Análisis / lección aprendida	Control relacionado
	(pérdida de 3 días de transacciones). Operaciones manuales de despacho en papel durante 7 días. Reconfiguración supervisada del SCADA.	recuperación fue inevitable con pérdida de datos. Los 7 días de operación manual representan el impacto financiero más cuantificable del incidente.	
Continuidad del negocio	Despacho manual en papel durante 7 días. Contacto directo con las 23 cooperativas para acordar re-despacho. Notificación hipotética a la SIC por violación de datos de clientes.	Sin plan de continuidad documentado, la improvisación multiplicó el costo operativo, reputacional y legal. Con un plan activo, el tiempo de recuperación estimado se reduce de 7 días a menos de 48 horas según estándar ISO 22301.	Controles 3, 9, 10

2.9 Valor del plan de continuidad

Un plan documentado basado en ISO 22301 (ISO, 2019) habría reducido el impacto en tres dimensiones:

Operativa: con procedimientos alternativos de despacho y facturación, los 7 días de operación manual se habrían reducido a 24–48 horas, con efecto directo sobre los $320 millones de ventas no realizadas.

Reputacional: las 23 cooperativas no recibieron comunicación oficial hasta varios días después del incidente. Un plan incluye protocolos de crisis que permiten notificar el mismo día y ofrecer un plan de re-despacho, preservando la confianza comercial.

Legal: la Ley 1581/2012 (Congreso de Colombia, 2012) exige notificar a la SIC en un plazo razonable tras una filtración de datos. Sin plan documentado, esa notificación no se realizó a tiempo, agravando la exposición regulatoria.

2.10 Cultura Organizacional

Los incidentes de FERTIBUGA no fueron causados por ataques sofisticados, sino por hábitos cotidianos del personal. La siguiente tabla analiza esos comportamientos y propone mejoras concretas, incluyendo el rol de la dirección y los indicadores de seguimiento.

Comportamiento identificado	Impacto en seguridad	Riesgo / incidente	Mejora propuesta	Rol de la dirección y medición
Operario revisa correo personal (Gmail) en el PC de control del SCADA	Convierte el equipo de control industrial en el vector de entrada; la red sin segmentar extiende inmediatamente el alcance al servidor principal	RAT instalado → SCADA modificado → ransomware (Riesgo CRÍTICO P×I=9)	Política de uso aceptable: PC de planta exclusivo para control industrial, sin internet ni cuentas personales. Capacitación mensual antiphishing con simulacros en contexto agroindustrial.	La gerencia debe firmar y comunicar la política formalmente. Indicador: % de empleados con simulacro completado y aprobado (meta: 100% en 60 días).
Empleado guarda contraseñas en texto plano en archivo del escritorio	Elimina toda barrera de acceso al servidor una vez el atacante controla el PC; el pivoting al SAP no requirió ningún ataque adicional de credenciales	Pivoting al servidor SAP y fórmulas maestras (Riesgo CRÍTICO P×I=9)	Prohibición documentada de contraseñas en texto plano. Implementar gestor de contraseñas corporativo. Sesión formativa obligatoria con evidencia firmada.	La gerencia debe aprobar el presupuesto del gestor de contraseñas y asistir a la primera sesión formativa como señal visible de compromiso. Indicador: auditoría trimestral de cumplimiento.
Coordinador desactiva alarmas del SCADA para 'reducir el ruido' en arranques de turno	Elimina el único mecanismo de detección temprana; la modificación fraudulenta del pesaje operó sin alarma durante 4 días completos	Fraude silencioso días 2–4, 1.847 sacos con peso incorrecto (Riesgo ALTO, sabotaje OT)	Protocolo formal documentado para desactivar alarmas: requiere autorización del Jefe de Planta, registro escrito y reactivación obligatoria al finalizar. Auditoría quincenal de estado de alarmas.	El Jefe de Planta reporta directamente el estado de alarmas al comité de seguridad TI trimestral. Indicador: número de desactivaciones no autorizadas

Comportamiento identificado	Impacto en seguridad	Riesgo / incidente	Mejora propuesta	Rol de la dirección y medición
				detectadas (meta: cero).
Técnicos del proveedor SAP comparten credenciales; ex-técnico mantiene acceso activo 2 meses después del cese	Imposibilita la trazabilidad de acciones remotas; la cuenta del ex-técnico fue el vector de exfiltración durante 6 meses consecutivos sin detección interna	Exfiltración de 2,3 GB durante 6 meses (Riesgo CRÍTICO P×I=9)	Política de identidades de terceros: accesos individuales e intransferibles; revocación inmediata y documentada al terminar la relación comercial. Auditoría trimestral de cuentas VPN activas.	La gerencia incluye la revocación de accesos en el checklist de cierre de contratos. Indicador: tiempo máximo de revocación tras terminación de contrato (meta: 24 horas).
Gerencia delega la totalidad de la responsabilidad de seguridad al único Jefe de Sistemas	Crea el punto único de fallo humano más crítico del caso (CIA 9/9); su incapacidad durante el incidente impidió una respuesta oportuna	Parálisis total ante incapacidad del Jefe de Sistemas (condición previa al incidente principal)	La gerencia general lidera visiblemente las políticas de seguridad. Designar responsable alterno con capacitación documentada. Comité de seguridad TI trimestral con presencia gerencial.	La gerencia preside el primer comité de seguridad TI y aprueba el plan de formación del alterno. Indicador: % de reuniones de comité con representación gerencial (meta: 100%).
Logs de VPN desactivados por 'rendimiento del servidor'; nadie revisa los existentes	Hace imposible detectar conexiones nocturnas del exproveedor; los logs existentes del firewall nunca se revisaron en 5 meses de exfiltración silenciosa	Detección tardía en mes 5 por accidente —actualización de rutina—, no por monitoreo activo	Activar y conservar logs de VPN, SCADA y servidor de forma permanente. Asignar responsable de revisión semanal. Implementar SIEM con alertas automáticas.	La gerencia aprueba el presupuesto del SIEM y designa formalmente al responsable. Indicador: % de semanas con revisión de logs completada y documentada (meta: 100%).

2.11 Indicadores de evolución cultural

El cambio cultural requiere medición continua. Se proponen cuatro indicadores trimestrales para la gerencia:

Tasa de detección en simulacros antiphishing: meta inicial 60%, meta a 12 meses 90%. Solo mejora con capacitaciones continuas, no con eventos únicos.

Desactivaciones de alarmas SCADA no autorizadas: meta cero por trimestre. Si no baja a cero en el primer período, el protocolo no se está cumpliendo.

Tiempo de revocación de accesos de terceros: meta menos de 24 horas desde el cierre del contrato. Depende de que la gerencia lo incluya en el checklist de finalización de contratos.

Participación gerencial en el comité de seguridad TI: meta 100% de reuniones trimestrales con representación de la dirección. Es el indicador más revelador: sin presencia gerencial, la organización interpreta que la seguridad no es prioridad.

El cambio cultural no se decreta: se construye con consistencia entre lo que la dirección dice y lo que hace.

3. Impacto del Incidente Global

La tabla resume el impacto del incidente en cuatro dimensiones (operativa, legal, financiera y reputacional) e indica cómo los controles propuestos habrían reducido cada uno.

Dimensión	Métricas del caso	Descripción del impacto simulado	Cómo los controles propuestos lo habrían reducido
Operacional	Parálisis total 7 días; pérdida $320M en ventas; 1.847 sacos con peso incorrecto	Detención completa de producción y despacho. 23 cooperativas afectadas por fraude en peso (Ley 1480/2011 y NTC 5167).	Con segmentación OT/IT (Control 1) y backup 3-2-1 (Control 3), el tiempo de recuperación estimado se reduce de 7 días a menos de 48 horas.
Legal / Regulatorio	Leyes 1273, 1581 y 1480 infringidas simultáneamente; posible cancelación registro ICA	Acceso abusivo (art. 269A), daño informático (art. 269D), datos filtrados, productos defectuosos. Posible cancelación del registro ICA por incumplimiento NTC 5167.	Los controles 9 (registro RNBD-SIC) y 4 (migración PHP 7.2) habrían eliminado las exposiciones ante Ley 1581 y Ley 1273, respectivamente.
Financiero	Rescate $85.000 USD + recuperación infraestructura $180M + multa SIC ~$1.200M + indemnizaciones cooperativas	Costo total hipotético superior a la facturación mensual de la empresa. Sin contar pérdida de contratos de largo plazo.	Los 10 controles propuestos tienen un costo de implementación estimado entre el 3% y el 7% de la facturación mensual, frente al 100%+ del impacto del incidente.
Reputacional	23 cooperativas afectadas; publicación en medios agrícolas regionales; pérdida de contratos exclusivos	Daño de imagen en el sector agrícola del Valle del Cauca, con riesgo de pérdida definitiva de contratos exclusivos y migración de clientes.	La capacitación antiphishing (Control 8) y la política de continuidad (Control 3) habrían preservado la confianza de las cooperativas al mantener la operación y comunicar el incidente de forma proactiva.

4. Conclusiones

El caso de FERTIBUGA muestra que los incidentes más destructivos no requieren atacantes sofisticados: son posibles por debilidades estructurales básicas. Se identificaron 10 activos CRÍTICOS, 4 riesgos con índice máximo y tres capas de falla tecnológica, de proceso y humana que coexistían de forma simultánea.

Las tres medidas prioritarias segmentación OT/IT, MFA y backup 3-2-1 tienen un costo estimado entre el 3% y el 7% de la facturación mensual (ISO, 2022a; IEC, 2018), frente a pérdidas hipotéticas que superaron el 100% de ese mismo valor.

El análisis de cultura organizacional confirma que detrás de cada falla técnica hubo una decisión humana o una omisión gerencial. La ciberseguridad es, en última instancia, un problema de gestión integral: solo se resuelve cuando tecnología, procesos y cultura se abordan de forma simultánea y la dirección lo asume como compromiso estratégico.

5. Referencias

Congreso de la República de Colombia. (1996). Ley 256 de 1996, por la cual se dictan normas sobre competencia desleal. Diario Oficial.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, creando el bien jurídico tutelado de la protección de la información y de los datos. Diario Oficial.

Congreso de la República de Colombia. (2011). Ley 1480 de 2011 – Estatuto del Consumidor. Diario Oficial.

Congreso de la República de Colombia. (2012). Ley 1581 de 2012, disposiciones generales para la protección de datos personales. Diario Oficial.

Consejo Nacional de Política Económica y Social. (2020). Documento CONPES 3995: Política Nacional de Confianza y Seguridad Digital. Departamento Nacional de Planeación.

International Electrotechnical Commission. (2018). IEC 62443: Security for industrial automation and control systems. IEC.

International Organization for Standardization. (2012). ISO/IEC 27037:2012: Guidelines for identification, collection and preservation of digital evidence. ISO.

International Organization for Standardization. (2019). ISO 22301:2019: Business continuity management systems – Requirements. ISO.

International Organization for Standardization. (2022a). ISO/IEC 27001:2022: Information security management systems – Requirements. ISO.

International Organization for Standardization. (2022b). ISO/IEC 27005:2022: Guidance on managing information security risks. ISO.

International Organization for Standardization. (2022c). ISO/IEC 27002:2022: Information security controls. ISO.

International Organization for Standardization. (2023). ISO/IEC 27035:2023: Information security incident management. ISO.

National Institute of Standards and Technology. (2024). Cybersecurity Framework 2.0. https://www.nist.gov/cyberframework

Open Web Application Security Project. (2021). OWASP Top 10:2021 – Top 10 web application security risks. https://owasp.org/Top10

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013, reglamentación parcial de la Ley 1581 de 2012. Diario Oficial.