



TRABAJO DE GRADO

Opción Seminario-Diplomado

Implementación de seguridad informática para la Protección de la Información en ER.
SERVICES

Corporación Universitaria Remington
Facultad de Ingenierías
Programa académico: Ingeniería en sistemas

Estudiante: WILMER ANDRES MOJICA CARDONA
Ing. Esp. ALFONSO VALENCIA MSc
SEMINARIO DE CIBERSEGURIDAD Y CIBERDEFENSA
2026

Dedicatoria

Dedico este trabajo a mi familia, que ha sido un apoyo constante durante mi proceso de formación y me ha motivado a seguir creciendo en el área profesional.

Agradecimientos

Agradezco a la Corporación Universitaria Remington y al Ingeniero Especialista y Magister José Alfonso Valencia Rodríguez por los conocimientos y orientaciones brindados en el Seminario de Ciberseguridad y Ciberdefensa. También agradezco a ER.SERVICES por servir como escenario para relacionar los temas vistos en clase con necesidades reales de una empresa del sector tecnológico. ([carta de autorización, Anexo A.](#))

Tabla de contenido

Dedicatoria.....	2
Agradecimientos	3
Resumen.....	6
Marco conceptual y contextual	7
1. Contexto de ER.SERVICES	7
1.1. Flujo general de información	9
1.2. Alcance del informe	9
1.3. Propósito del informe.....	10
2. Seguridad de la información y ciberseguridad.....	10
2.1. Confidencialidad, integridad y disponibilidad.....	11
2.2. Activos, amenazas, vulnerabilidades, riesgos y controles	12
3. ISO/IEC 27001:2022	12
3.1. Relación de ISO/IEC 27001 con ER.SERVICES.....	13
4. ISO/IEC 27002:2022	14
5. ISO/IEC 31000:2018	14
5. Ciberseguridad y ciberdefensa.....	15
7. Protección de datos y delitos informáticos en Colombia.....	15
8. Relación del marco conceptual con ER.SERVICES	16
2. Planteamiento del problema.....	18
3. Justificación	19
4. Objetivos	20
4.1. Objetivo general.....	20
4.2. Objetivos específicos	20
5.1. Seguridad de la información y ciberseguridad.....	20
5.2. ISO/IEC 27001:2022	21
5.3. ISO/IEC 27002:2022	21
5.4. ISO/IEC 31000:2018	22
5.5. Ciberdefensa	22
5.6. Marco legal colombiano	23
Desarrollo e implementación del aprendizaje.....	23
6. Metodología del diagnóstico.....	23
6.1. Criterios de valoración de riesgos.....	24
7. Inventario y clasificación de activos.....	26
7.1. Tratamiento de equipos de clientes.....	28
8. Diagnóstico de vulnerabilidades y exposición.....	28
9. Estrategia integral de ciberseguridad	30
9.1. Gobierno y responsabilidades	30
9.2. Política de control de acceso.....	31
9.3. Protección de estaciones de trabajo y portátiles	31
9.4. Segmentación y seguridad de red	32
9.5. Política de copias de seguridad y recuperación	32
9.6. Seguridad del sitio web y comercio electrónico	33
9.7. Seguridad en cámaras y dispositivos IoT.....	33
9.8. Gestión de información de clientes.....	34
9.9. Gestión de incidentes	34

9.10. Capacitación y cultura de seguridad	35
11. Plan de implementación de 90 días.....	37
12. Indicadores de seguimiento.....	39
13. Estimación de recursos	40
14. Resultados esperados de la implementación.....	41
15. Limitaciones del ejercicio	41
Conclusiones	42
Recomendaciones	43
Referencias.....	44
Anexos	47
16. Anexo A	47

Resumen

El presente informe técnico aborda la implementación de seguridad informática para la protección de la información en ER.SERVICES, empresa ubicada en Cúcuta y dedicada al servicio técnico y a la comercialización de tecnología. La empresa cuenta con cinco empleados y utiliza un sistema para registrar información de clientes, informes de los servicios realizados, ventas, ingresos y productos. Debido a que buena parte de la operación depende de estos recursos, la pérdida, alteración o exposición de la información puede afectar tanto el trabajo diario como la atención al cliente. En esta primera etapa se presenta el contexto de ER.SERVICES y se relaciona con los conceptos estudiados en el Seminario de Ciberseguridad y Ciberdefensa. Como referentes se toman la seguridad de la información, la gestión de riesgos, ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 31000:2018, la ciberdefensa y la normativa colombiana sobre protección de datos y delitos informáticos. El análisis también considera características propias de la empresa, como el manejo de equipos de clientes, el uso de una plataforma para su gestión interna, el sitio web comercial, los servicios de cámaras de seguridad y la infraestructura de red. A partir de este marco se establecerán posteriormente los riesgos prioritarios y las medidas que puedan aplicarse de forma realista en una organización pequeña. El propósito es que la propuesta no se limite únicamente a la implementación a controles técnicos independiente, sino que ayude a organizar responsabilidades, proteger la información y mantener la continuidad de los procesos más importantes de ER.SERVICES.

Palabras clave: ciberseguridad, seguridad de la información, gestión de riesgos, ISO/IEC 27001,

Marco conceptual y contextual

Marco conceptual

1. Contexto de ER.SERVICES

ER.SERVICES es una empresa pequeña ubicada en Cúcuta, Norte de Santander, que actualmente trabaja con cinco empleados. Su actividad combina el servicio técnico con la venta de productos tecnológicos. Para llevar el control de la operación utiliza un sistema en el que se registran datos de los clientes, informes de los servicios técnicos, ventas, ingresos y productos. Este sistema es importante para el funcionamiento diario porque reúne información que se consulta de manera constante para atender a los clientes y hacer seguimiento a los trabajos realizados. Al ser un equipo de trabajo reducido, algunas funciones pueden quedar concentradas en las mismas personas, por lo que las medidas de seguridad deben ser claras y fáciles de cumplir, sin diseñar procesos que resulten demasiado complejos para el tamaño de la empresa.

Para complementar la descripción de la empresa se consultó su sitio web oficial. Allí ER.Services ofrece mantenimiento y reparación de computadores, tabletas e impresoras; instalación y mantenimiento de cámaras de seguridad; redes y cableado estructurado; instalación de software; asesoría informática y venta de computadores, periféricos, programas y equipos de telecomunicaciones (ER.Services, s. f.-a; ER.Services, s. f.-b). El portal también funciona como vitrina comercial, ya que publica productos, precios, disponibilidad y opciones de carrito. Por esta razón, la página web no es solamente un medio de publicidad: también forma parte de los recursos tecnológicos que deben protegerse, porque una alteración del contenido o la pérdida de acceso administrativo puede afectar la imagen de ER.SERVICES frente a sus clientes.

El sitio web ubica la tienda en el barrio Palmeras Parte Alta, sector Atalaya, en Cúcuta, y presenta canales separados para ventas, soporte e información general. También informa sobre

cotizaciones, métodos de pago, garantías y entregas. En la sección de servicios se indica, además, que la empresa cuenta con certificación HCSA de Hikvision para actividades relacionadas con cámaras de seguridad (ER.Services, s. f.-b). Todo esto muestra que ER.SERVICES no trabaja únicamente con computadores: en su operación también intervienen redes, cámaras, software, dispositivos de almacenamiento y equipos de terceros, elementos que amplían los puntos en los que puede existir información sensible o una posible entrada de amenazas.

Tabla 1

Caracterización de ER. SERVICES para el análisis de ciberseguridad

Aspecto	Descripción
Tamaño	Empresa pequeña con cinco empleados.
Ubicación	Cúcuta, Norte de Santander; el portal ubica la atención física en el sector Atalaya.
Actividad	Servicio técnico, mantenimiento y reparación de equipos; venta de tecnología; cámaras de seguridad; redes; software y asesoría informática.
Canales digitales	Sitio web con catálogo, precios, carrito de compras y correos diferenciados para ventas, soporte e información.
Información crítica	Datos de clientes, informes técnicos, ventas, ingresos, productos, credenciales y respaldos.
Dependencia tecnológica	Importante para el registro de servicios, el control comercial, la atención al cliente y la continuidad del trabajo.

Nota: Esta tabla muestra información de la empresa ER:SERVICES y las actividades que realiza.

Marco contextual

1.1. Flujo general de información

El manejo de la información comienza desde el momento en que un cliente solicita un servicio o lleva un equipo para revisión. Se registran sus datos de contacto, la descripción de la falla, las características del equipo y, después del diagnóstico, el trabajo realizado. Cuando se genera una venta o un cobro, también se actualizan los registros comerciales. En el área de ventas se manejan productos, existencias, precios e ingresos. En la práctica, parte importante de estos datos termina registrada en el sistema que utiliza la empresa para hacer seguimiento a su operación.

La protección de esta información se puede entender a partir de tres principios básicos. La confidencialidad busca que los datos de clientes, claves y documentos internos solo sean consultados por quienes realmente los necesitan. La integridad se relaciona con mantener correctos los informes técnicos, precios, inventarios y movimientos registrados. La disponibilidad significa que el sistema, los equipos y los respaldos deben poder utilizarse cuando sean necesarios. Estos tres principios serán la base para analizar posteriormente los riesgos de ER.SERVICES.

1.2. Alcance del informe

El informe se concentra en la información de clientes, reportes de servicio técnico, registros de ventas e inventario, computadores utilizados por los empleados, cuentas de usuario, correo electrónico, red local, conexiones inalámbricas, dispositivos de almacenamiento, copias de seguridad, cámaras, credenciales administrativas y el sitio web de ER.SERVICES. También se tendrán en cuenta los equipos que los clientes dejan para diagnóstico o reparación, ya que estos dispositivos pueden contener archivos personales y, al mismo tiempo, pueden llegar con virus, programas no confiables o configuraciones que no dependen de la empresa.

En esta primera etapa no se realizaron pruebas de penetración ni intentos de acceso a sistemas internos. El avance se construye con el conocimiento del funcionamiento de ER.SERVICES y con la información que se puede observar públicamente en su sitio web. Las verificaciones técnicas, como la revisión de configuraciones, respaldos, usuarios, equipos y vulnerabilidades, se plantearán dentro de la etapa de desarrollo e implementación. Esto permite diferenciar desde el comienzo lo que ya se conoce de la empresa de lo que todavía debe comprobarse técnicamente.

1.3. Propósito del informe

El objetivo general del trabajo es crear un plan de seguridad informática para ER. SERVICES. El plan de seguridad proteger la información, los sistemas, los dispositivos y recursos tecnológicos de la empresa contra a amenazas cibernéticas, mediante la identificación de vulnerabilidades aplicando medidas de seguridad.

El alcance del objetivo se define según las condiciones y necesidades reales de la empresa. No se requiere crear una estructura de seguridad propia de una organización grande, sino establecer controles que puedan mantenerse con cinco empleados y que se integren a las actividades que ya se hacen. En este sentido se dará prioridad a medidas de seguridad como el control de accesos, los respaldos, la actualización de equipos, la separación de la red de trabajo, la protección del sitio web y el establecimiento de procedimiento y atención de incidentes de seguridad.

2. Seguridad de la información y ciberseguridad

La seguridad de la información y la ciberseguridad a menudo se usan como si fueran lo mismo, pero no lo son. La seguridad de la información se encarga de proteger los datos, sin importar su formato. Esto incluye archivos digitales, documentos físicos, contraseñas, copias de

seguridad, correos electrónicos y cualquier otro elemento que sea importante para la empresa. Por otro lado, la ciberseguridad se enfoca en proteger la información, los sistemas y los dispositivos que funcionan o se comunican a través de medios digitales y están conectados entre sí.

En ER. SERVICES los dos conceptos están muy relacionados. Un informe técnico puede estar en el sistema, enviado por correo, impreso o guardado temporalmente en una memoria USB. De la misma manera, la información de un cliente puede estar en una orden de servicio y también estar en una base de datos. Por eso no basta con proteger solo las computadoras. También es necesario tener reglas claras sobre quién puede acceder a la información, cómo se almacena, cómo se comparte y qué hacer cuando ya no es necesaria.

2.1. Confidencialidad, integridad y disponibilidad

La confidencialidad, la integridad y la disponibilidad son tres propiedades fundamentales de la seguridad de la información y permiten organizar de manera sencilla lo que se quiere proteger. En el caso de ER.SERVICES, la confidencialidad se relaciona con evitar que una persona no autorizada pueda consultar datos de clientes, contraseñas, reportes técnicos o información comercial. Un ejemplo sería impedir que las credenciales del sistema sean compartidas entre varias personas o queden guardadas en un equipo al que cualquiera pueda acceder.

La integridad busca que la información se mantenga correcta y que cualquier cambio pueda ser identificado. Para la empresa esto es importante en los registros de ventas, inventarios, precios e informes de servicio, porque una modificación accidental o realizada sin autorización puede producir cobros equivocados, pérdida de trazabilidad o confusión sobre el trabajo que se hizo a un equipo. La disponibilidad, por su parte, significa que la información y los sistemas puedan utilizarse cuando se necesitan. Una falla del computador principal, un ataque de ransomware o un

respaldo que nunca se haya probado pueden dejar a la empresa sin acceso a información necesaria para seguir trabajando.

2.2. Activos, amenazas, vulnerabilidades, riesgos y controles

Para estudiar la seguridad de una empresa primero es necesario saber qué tiene valor y qué situaciones pueden afectarlo. Un activo de información puede ser un dato, un sistema, un equipo, una cuenta, una copia de seguridad, una red o incluso una persona que cumple una función importante. En ER.SERVICES, algunos activos claros son el sistema donde se registran los servicios, los datos de clientes, los computadores de trabajo, el correo, el sitio web, la red, las cámaras y las credenciales de administración.

Una amenaza es una situación que puede causar daño, mientras que una vulnerabilidad es una debilidad que facilita que ese daño ocurra. Por ejemplo, un archivo malicioso en el computador de un cliente puede representar una amenaza y conectar ese equipo directamente a la misma red donde funciona el sistema administrativo puede aumentar la exposición. De igual forma, una contraseña débil es una vulnerabilidad que puede facilitar el acceso no autorizado. El riesgo aparece al relacionar la posibilidad de que ocurra una situación con el impacto que tendría sobre la empresa. Los controles son las medidas utilizadas para reducir ese riesgo, como la autenticación en dos pasos, los respaldos, el antivirus, la segmentación de red o una política para crear y retirar usuarios.

3. ISO/IEC 27001:2022

ISO/IEC 27001:2022 es una de las normas analizadas en el seminario. Esta norma ofrece requisitos para diseñar, aplicar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Su enfoque no es instalar herramientas de seguridad por separado, sino entender el

entorno de la organización, identificar los riesgos, definir roles, aplicar controles y revisar regularmente si las medidas tomadas realmente funcionan (International Organization for Standardization [ISO], 2022)

Para ER.SERVICES este enfoque resulta útil porque permite organizar la seguridad alrededor de sus procesos reales. Antes de decidir qué herramienta comprar, se debe saber qué información es crítica, quién la utiliza, cuáles son los riesgos más probables y qué impacto tendría una interrupción. En una empresa de cinco empleados esto puede llevarse de forma sencilla mediante un inventario de activos, una matriz de riesgos, políticas cortas, responsables definidos y evidencias básicas de seguimiento.

3.1. Relación de ISO/IEC 27001 con ER.SERVICES

Aplicar el enfoque de ISO/IEC 27001 a ER.SERVICES no significa que la empresa deba iniciar un proceso de certificación. Para este trabajo se toma la norma como una guía para ordenar la gestión. El contexto corresponde al tamaño de la empresa, sus servicios y la información que utiliza; el liderazgo se refleja en la necesidad de que una persona tenga responsabilidad sobre las decisiones de seguridad; la planificación parte de los riesgos; la operación corresponde a la aplicación de controles; y la evaluación y mejora permiten revisar lo que funciona y corregir lo que falle.

Este punto es importante porque una política escrita por sí sola no protege la información. Si se define, por ejemplo, que deben existir copias de seguridad, también debe quedar claro quién las realiza, con qué frecuencia, dónde se guardan y cómo se comprueba que pueden restaurarse. El mismo criterio se aplica a contraseñas, actualizaciones, acceso al sistema, sitio web y red interna. La norma aporta precisamente esa idea de mantener la seguridad como un proceso y no como una actividad de una sola vez.

4. ISO/IEC 27002:2022

ISO/IEC 27002:2022 complementa el enfoque de gestión de ISO/IEC 27001. Proporciona orientación para elegir y usar controles de seguridad de la información. La norma cubre controles organizacionales, relacionados con las personas, con instalaciones y con tecnología. Ayuda a manejar riesgos según las necesidades de cada empresa (ISO, 2022b). No todos los controles se aplican igual. La selección depende del entorno y de los riesgos que se hayan encontrado

En ER.SERVICES los controles más útiles son aquellos que pueden mantenerse sin requerir personal especializado de tiempo completo. Entre ellos se encuentran la asignación de cuentas individuales, la autenticación segura, el retiro de accesos cuando una persona deja de necesitarlos, las copias de seguridad, la protección contra software malicioso, la actualización de equipos, el registro de eventos importantes, la seguridad de la red, el control de dispositivos externos, la protección física de equipos y la preparación para responder a incidentes. Estos controles tienen relación directa con la forma en que la empresa presta soporte técnico y administra su información.

5. ISO/IEC 31000:2018

Esta norma da principios y directrices. Nos ayuda a crear un proceso ordenado para identificar amenazas y vulnerabilidades. Tiene un enfoque completo para identificar, evaluar y analizar riesgos en una organización (International Organization for Standardization [ISO], 2018)

Para ER. SERVICES, la gestión del riesgo se ajusta a las características y recursos de la organización. Por eso, se sugiere identificar los activos de información más importantes, definir los escenarios de riesgo posibles, evaluar cada riesgo con criterios de probabilidad e impacto, y establecer controles de seguridad que se ajusten a las necesidades de la empresa.

5. Ciberseguridad y ciberdefensa

Dentro del seminario también se estudia la ciberdefensa. En Colombia, el concepto está relacionado con la capacidad del Estado para prevenir y contrarrestar amenazas o incidentes cibernéticos que puedan afectar la sociedad, la soberanía, la integridad territorial, el orden constitucional y los intereses nacionales.

Por esta razón, en el caso de ER.SERVICES no sería correcto hablar de ciberdefensa como si la empresa fuera a realizar acciones militares u ofensivas. La relación con este tema se encuentra en la capacidad de protegerse y responder: reconocer incidentes, contener un equipo comprometido, conservar información que pueda servir como evidencia, recuperar el servicio y acudir a los canales institucionales cuando la situación lo requiera. Este enfoque defensivo sí tiene sentido dentro de una empresa privada y se relaciona con la continuidad de la operación.

7. Protección de datos y delitos informáticos en Colombia

ER.SERVICES recopila datos de clientes para poder ofrecer sus servicios y llevar un registro de los trabajos realizados. Por eso, la protección de datos personales también es parte fundamental del proyecto. La Ley 1581 de 2012 establece las normas generales para proteger los datos personales en Colombia y reconoce los derechos de las personas que tienen información almacenada en bases de datos. Entre otras cosas, esta ley exige que los datos se usen solo para las finalidades que se informan y que se tomen medidas para evitar que se acceda, consulte o utilice sin autorización. Esto lo menciona el (Congreso de Colombia en 2012).

Para la empresa, esto implica acciones simples pero muy importantes. Es necesario saber qué datos se piden al cliente, evitar recoger información que no sea necesaria, controlar quién tiene acceso al sistema, proteger las copias de seguridad y decidir qué hacer con los registros cuando ya no se necesiten. También hay que prestar atención especial a los equipos que llegan al taller, ya

que pueden contener archivos personales del cliente. El servicio técnico no debe revisar información privada que no sea esencial para diagnosticar o arreglar el dispositivo.

La Ley 1273 de 2009 complementa este marco legal al incluir en el Código Penal colombiano ciertas conductas relacionadas con la protección de la información y los datos. Entre estas conductas se encuentran el acceso indebido a sistemas, el daño informático, el uso de software malicioso y la violación de datos personales. Esto indica que una mala práctica de seguridad no solo puede provocar pérdida de información o dañar la imagen de la empresa; en algunos casos, también puede traer consecuencias legales.

8. Relación del marco conceptual con ER.SERVICES

Los puntos anteriores ayudan a entender cómo aplicar el proyecto en la situación de ER.SERVICES. El sistema que se usa para clientes, servicios, ventas e inventario es un elemento importante, ya que contiene datos esenciales para el trabajo. Los equipos y las cuentas de los empleados son formas de acceder a esa información. La red conecta equipos propios con otros dispositivos, y el taller recibe computadoras de clientes cuyo nivel de seguridad no se conoce con anticipación. Además, el sitio web muestra la imagen de la empresa y necesita cuentas de administración, actualizaciones y copias de seguridad.

Basado en esta situación, la estrategia de ciberseguridad debe enfocarse en los riesgos que realmente pueden ocurrir en la empresa: pérdida de datos, virus, robo de contraseñas, acceso no autorizado, fallos en las copias de seguridad, conexión insegura de equipos de clientes, problemas en el sitio web y filtrado de información personal. Usar las normas ISO/IEC 27001, ISO/IEC 27002 y ISO/IEC 31000 no es solo para cumplir con estándares, sino para apoyar controles que tengan sentido en el trabajo diario.

Con este marco, se establece la base para la siguiente parte del informe, donde se hará un análisis de los activos y riesgos y se propondrán políticas y medidas de seguridad para ER.SERVICES. Las decisiones que se tomen deben ser prácticas: deben poderse aplicar, comprobar y mantener en una empresa con cinco empleados.

Tabla 2

Relación de los principales referentes con ER.SERVICES

Referente	Aporte al trabajo	Aplicación en ER.SERVICES
ISO/IEC 27001:2022	Organiza la gestión de la seguridad a partir del contexto, los riesgos, responsabilidades y mejora continua.	Sirve para estructurar el diagnóstico, las políticas y el seguimiento del proyecto.
ISO/IEC 27002:2022	Orienta la selección e implementación de controles de seguridad.	Apoya controles de acceso, respaldos, malware, red, equipos, sitio web e incidentes.
ISO/IEC 31000:2018/	Proporciona principios y directrices para la gestión de riesgo	Se utiliza como referencia metodología para identificar y valorar amenaza de seguridad de la información de ER.SERVICES
Ciberdefensa	Ubica la seguridad digital dentro de la capacidad de protección del Estado.	Se toma el enfoque de preparación, respuesta, recuperación y conservación de evidencias.
Ley 1581 de 2012	Regula la protección y el tratamiento de datos personales.	Aplica a los datos de clientes que ER.SERVICES registra y administra.
Ley 1273 de 2009	Protege la información y los sistemas frente a conductas informáticas ilícitas.	Da contexto legal a riesgos como accesos abusivos, daño informático y software malicioso.

Nota. La tabla resume la función de cada referente dentro del informe. No representa una declaración de certificación ni de cumplimiento integral.

2. Planteamiento del problema

ER.SERVICES presta servicios relacionados con tecnología y, al mismo tiempo, depende de sus propios recursos informáticos para registrar clientes, documentar servicios técnicos y controlar ventas y productos. Esta combinación crea una situación particular: la empresa no solo protege sus datos administrativos, sino que también interactúa con dispositivos de terceros que pueden estar infectados, desactualizados o configurados de manera insegura. Si esos equipos se conectan a la misma red utilizada por el sistema de gestión, aumenta la posibilidad de propagación de malware o acceso no previsto a recursos internos.

A lo anterior se suma que una organización de cinco personas suele disponer de poco tiempo para separar funciones, documentar procedimientos o mantener controles especializados. Las cuentas compartidas, contraseñas conocidas por varios empleados, copias de seguridad sin pruebas de restauración, actualizaciones aplazadas o el uso de una sola red para todos los equipos pueden convertirse en amenaza, aunque la infraestructura sea pequeña. La ausencia de políticas escritas también dificulta responder de manera uniforme cuando ocurre un incidente.

El problema central consiste, entonces, en que ER.SERVICES maneja información y recursos tecnológicos necesarios para su operación, pero requiere formalizar una estrategia que defina qué debe protegerse, quién puede acceder, cómo se realizan los respaldos, cómo se aíslan los equipos de clientes, qué hacer ante un incidente y cómo se verifica que las medidas siguen funcionando.

3. Justificación

La información que almacena ER.SERVICES tiene un valor importante para las operaciones y, en algunos casos, contiene datos personales. Si se pierde la base de clientes, los reportes de servicio o el registro de ventas, se pueden detener procesos, generar trabajo adicional y afectar la relación con los usuarios. Si los inventarios o los ingresos se ven alterados, se pueden tomar decisiones erróneas. Además, si se revelan nombres, números de contacto, datos de equipos o credenciales, se puede afectar la privacidad de las personas y la imagen de la empresa.

En Colombia, la Ley 1581 de 2012 establece las reglas para proteger los datos personales y exige que quienes manejan esa información tomen medidas para gestionarla correctamente (Congreso de Colombia, 2012). Por otro lado, la Ley 1273 de 2009 incluyó en el Código Penal actos como acceso no autorizado, daño a sistemas, uso de software malicioso y filtración de datos personales (Congreso de Colombia, 2009). Estas leyes muestran que la seguridad no es solo un tema técnico, sino también legal y de responsabilidad empresarial.

La propuesta también tiene sentido porque se puede adaptar al tamaño de la empresa. No se requiere una infraestructura cara ni un centro de seguridad grande. Se enfocan en controles básicos pero muy importantes: inventario de activos, usuarios individuales, autenticación segura, respaldo, actualizaciones, segmentación de red, protección de dispositivos, revisión del sitio web, capacitación y un plan para manejar incidentes. El objetivo es que la seguridad forme parte de la operación diaria, sin convertirse en una carga difícil de mantener.

4. Objetivos

4.1. Objetivo general

Implementar un plan de seguridad informática para ER. SERVICES, orientada a proteger la información y recursos tecnológicos de la empresa frente a amenazas cibernéticas, mediante la identificación de vulnerabilidades.

4.2. Objetivos específicos

- Identificar los activos de información y recursos tecnológicos que soportan los procesos de servicio técnico, atención al cliente, ventas e inventario.
- Analizar amenazas, vulnerabilidades y escenarios de riesgo que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Proponer un plan de implementación, responsables e indicadores que permitan verificar el cumplimiento y mejorar la estrategia de forma continua.

5.1. Seguridad de la información y ciberseguridad

La seguridad de la información protege los datos, sin importar en qué tipo de medio estén. La seguridad de la información incluye archivos digitales, documentos impresos, credenciales, copias de seguridad, conversaciones y cualquier información que sea importante para la empresa. La ciberseguridad se enfoca en los riesgos que ocurren en sistemas, redes, servicios en línea y dispositivos conectados. En ER.SERVICES, estos dos conceptos trabajan juntos, porque un informe técnico puede estar en el sistema, puede enviarse por correo, puede imprimirse o puede copiarse en un dispositivo de almacenamiento.

La gestión de seguridad se basa en analizar activos, amenazas, vulnerabilidades, riesgos y controles. Un activo es algo que la empresa debe proteger. Una amenaza es algo que puede causar daño. Una vulnerabilidad es una debilidad que podría ser explotada. El riesgo combina la posibilidad de que algo suceda y el daño que causaría. Un control es una medida que reduce la probabilidad de que suceda algo o el daño que causaría.

5.2. ISO/IEC 27001:2022

ISO/IEC 27001:2022 establece requisitos para crear, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información. Esto incluye la evaluación y el manejo de riesgos según el contexto de cada organización. (International Organization for Standardization [ISO], 2022).

5.3. ISO/IEC 27002:2022

ISO/IEC 27002:2022 da una guía para elegir e instalar controles de seguridad de la información. La norma ayuda a las organizaciones a gestionar los riesgos y a reforzar su SGSI, la norma incluye controles de acceso, criptografía, seguridad de personas, respuesta a incidentes y protección tecnológica (ISO, 2022b). Su enfoque facilita adaptar los controles al tamaño y a las necesidades reales de una empresa.

Para ER.SERVICES se priorizan controles organizacionales, humanos, físicos y tecnológicos que puedan sostenerse con cinco empleados. La selección se concentra en inventario de activos, responsabilidades, gestión de identidades, autenticación, copias de seguridad, registro de eventos, protección contra malware, gestión de vulnerabilidades, configuración segura, seguridad de redes, seguridad física, relaciones con proveedores y preparación para incidentes.

5.4. ISO/IEC 31000:2018

ISO/IEC 31000:2018 es un estándar que ofrece principios y directrices para gestionar el riesgo en una organización. Este enfoque permite desarrollar un proceso claro para identificar, analizar, evaluar, tratar, comunicar, monitorear y revisar los riesgos. El objetivo es ayudar a tomar mejores decisiones y fortalecer la capacidad de la organización.

Para ER. SERVICES, la aplicación de este enfoque se adapta a su estructura organizacional, que cuenta con solo cinco empleados. Por lo tanto, las medidas que proponemos son prácticas, proporcionales y sostenibles. Nos enfocamos en los riesgos que puedan afectar la confidencialidad, la integridad y la disponibilidad de la información. De esta forma, la gestión del riesgo se convierte en una herramienta clave para guiar las acciones de seguridad informática y establecer un proceso continuo de seguimiento y mejora.

5.5. Ciberdefensa

En Colombia es la capacidad del Estado para evitar y enfrentar amenazas o incidentes en el mundo digital que puedan dañar a la sociedad, la soberanía, la independencia, la integridad territorial, el orden constitucional y los intereses del país. Esta capacidad puede incluir el uso de medios militares para defenderse contra amenazas cibernéticas (Presidencia de la República de Colombia, 2022). Por eso, no es adecuado que una empresa privada realice funciones militares u ofensivas y las llame ciberdefensa.

La relación de ER. SERVICES con este concepto es de defensa: proteger sus activos, registrar los incidentes, guardar pruebas, recuperar servicios y notificar situaciones graves a los canales correspondientes.

5.6. Marco legal colombiano

La estrategia debe incluir al menos la Ley 1581 de 2012 sobre protección de datos personales. También debe incluir el Decreto 1074 de 2015 y la Ley 1273 de 2009, que regulan la protección de la información y los datos frente a conductas ilegales en el ámbito informático (Congreso de Colombia, 2009, 2012; Presidencia de la República de Colombia, 2015). La empresa debe conocer qué datos recoge, para qué los usa, quién puede acceder a ellos, cuánto tiempo los guarda y cómo responde a las solicitudes de los dueños de los datos. En ciberseguridad, estos puntos se convierten en controles que evitan accesos no autorizados, pérdidas, alteraciones o divulgaciones no deseadas.

Desarrollo e implementación del aprendizaje

6. Metodología del diagnóstico

El trabajo se desarrolló bajo un enfoque aplicado y descriptivo. Primero se caracterizó la empresa con la información suministrada para el ejercicio y con una revisión de fuentes abiertas. Después se identificaron activos y flujos de información. Con esa base se construyeron escenarios de amenaza, se priorizaron controles y se formuló un conjunto de políticas que pueden ser implementadas por una empresa de cinco personas sin requerir una estructura especializada.

La revisión de información pública comprendió aspecto como el nombre comercial, el dominio de la empresa, la ubicación y la actividad visible en el sitio web. Las búsquedas se realizaron sobre páginas indexadas y no incluyeron técnicas intrusivas. La información pública se utilizó únicamente para comprender el contexto y detectar elementos que justifican revisiones defensivas, como el contenido anómalo identificado en la página principal.

6.1. Criterios de valoración de riesgos

Los riesgos se califican con una escala de probabilidad e impacto de 1 a 5. La probabilidad representa qué tan factible es que el escenario ocurra dadas las condiciones de la empresa y la exposición del activo. El impacto representa el efecto posible sobre operación, información, clientes, finanzas o reputación. El nivel se obtiene multiplicando ambos valores. Los resultados de 1 a 4 se consideran bajos, de 5 a 9 moderados, de 10 a 14 altos y de 15 a 25 críticos. La escala no reemplaza una medición con datos históricos; funciona como herramienta de priorización inicial.

Tabla 3
Matriz inicial de riesgos de ciberseguridad

ID	Escenario de riesgo	P	I	Nivel	Tratamiento prioritario
R1	Acceso no autorizado al sistema por credenciales débiles, compartidas o robadas.	4	5	20 - Crítico	Usuarios individuales, MFA y mínimo privilegio.
R2	Ransomware o malware en equipos internos.	4	5	20 - Crítico	EDR/antimalware, parches, backups y restricciones.
R3	Ingreso de malware desde equipos de clientes al entorno corporativo.	4	4	16 - Crítico	Red de taller aislada y estación de análisis.
R4	Alteración o pérdida de datos sin respaldo restaurable.	3	5	15 - Crítico	Esquema 3-2-1 y pruebas trimestrales.
R5	Compromiso o	4	4	16 - Crítico	Revisión de integridad,

ID	Escenario de riesgo	P	I	Nivel	Tratamiento prioritario
	modificación no autorizada del sitio web.				MFA, actualización, WAF/hosting y backups.
R6	Phishing y robo de cuentas de correo o administración.	4	4	16 - Crítico	MFA, capacitación y verificación de enlaces/solicitudes.
R7	Exposición de datos personales de clientes.	3	5	15 - Crítico	Control de acceso, cifrado, retención y registro.
R8	Red Wi-Fi o cámaras con configuraciones inseguras.	3	4	12 - Alto	Segmentación, WPA2/WPA3, firmware y claves únicas.
R9	Robo o pérdida de un equipo con información empresarial.	3	4	12 - Alto	Cifrado de disco, bloqueo y respaldo.
R10	Falla del sistema o dependencia de una sola persona/proveedor.	3	4	12 - Alto	Documentación, respaldo de configuración y procedimiento de continuidad.
R11	Cambios no autorizados en inventario, precios o ventas.	3	4	12 - Alto	Roles, trazabilidad y revisión periódica.
R12	Uso de memorias	3	3	9 - Moderado	Restricción, análisis previo

ID	Escenario de riesgo	P	I	Nivel	Tratamiento prioritario
	USB no controladas.				y medios autorizados.

Nota. P = probabilidad; I = impacto. La valoración es inicial y debe revisarse con evidencia interna, historial de incidentes y pruebas autorizadas.

7. Inventario y clasificación de activos

El inventario de activos permite saber qué debe protegerse y quién es responsable. En una empresa pequeña el inventario no necesita ser complejo. Puede mantenerse en una hoja controlada con identificador, propietario, ubicación, clasificación, sistema operativo, fecha de actualización y estado del respaldo. La clasificación propuesta utiliza tres niveles: pública, interna y confidencial.

Tabla 4
Inventario inicial de activos de información y tecnología

ID	Activo	Información o función	Clasificación	Criticidad
A1	Sistema de gestión	Clientes, informes técnicos, ventas, ingresos e inventario.	Confidencial	Crítica
A2	Base de datos / archivos del sistema	Registros estructurados y soportes asociados.	Confidencial	Crítica
A3	Cuentas y credenciales	Usuarios del sistema, correo, web, red y servicios.	Confidencial	Crítica

ID	Activo	Información o función	Clasificación	Criticidad
A4	Equipos de trabajo	Computadores y portátiles usados por empleados.	Interna	Alta
A5	Sitio web y tienda	Catálogo, precios, contenido, formularios y administración web.	Pública/Interna	Alta
A6	Correo corporativo	Comunicaciones con clientes y proveedores.	Confidencial	Alta
A7	Red local y Wi-Fi	Conectividad del sistema, empleados, cámaras y dispositivos.	Interna	Alta
A8	Equipos de clientes	Dispositivos recibidos para diagnóstico o reparación.	Terceros/Confidencial	Alta
A9	Copias de respaldo	Respaldo de base de datos, informes y configuraciones.	Confidencial	Crítica
A10	Cámaras y grabador	Videovigilancia, cuentas remotas y grabaciones.	Confidencial	Alta
A11	Documentos comerciales	Cotizaciones, facturas, garantías y registros de proveedores.	Interna/Confidencial	Media-Alta

Nota. La criticidad propuesta debe validarse con el responsable de la empresa durante la implementación.

7.1. Tratamiento de equipos de clientes

Los computadores, discos, memorias y otros equipos recibidos para servicio técnico requieren un tratamiento diferenciado. El técnico puede necesitar acceso temporal a archivos o credenciales para probar el funcionamiento, pero esto no significa que la empresa deba conservar copias innecesarias. Se recomienda registrar la autorización del cliente, limitar el acceso al personal asignado, evitar copiar información que no sea necesaria para el diagnóstico y eliminar de forma segura cualquier archivo temporal cuando finalice el servicio.

Desde el punto de vista de red, los equipos de clientes no deben conectarse directamente a la misma red donde opera el sistema administrativo. La medida recomendada es una red o segmento de taller aislado. Si el presupuesto no permite VLAN, puede utilizarse un router independiente conectado a Internet sin acceso a la red interna. Esta separación reduce el riesgo de que malware presente en un equipo reparado alcance computadores administrativos, cámaras o respaldos.

8. Diagnóstico de vulnerabilidades y exposición

El diagnóstico inicial no busca afirmar vulnerabilidades que no han sido comprobadas con acceso técnico. Se identifican condiciones de exposición y puntos que deben verificarse. La prioridad se establece por la consecuencia que tendría cada escenario sobre los activos críticos.

- Sistema central de información: concentra datos de clientes, servicios y ventas; requiere cuentas individuales, respaldos y registro de cambios.
- Correo y credenciales: el tamaño del equipo favorece el uso informal de contraseñas; debe verificarse que no existan cuentas compartidas y que las cuentas críticas usen autenticación multifactor.

- Equipos de clientes: constituyen una fuente frecuente de archivos maliciosos, software no confiable o configuraciones inseguras; deben permanecer aislados de la red corporativa.
- Red local: debe comprobarse si oficina, taller, visitantes y cámaras comparten el mismo segmento. Si comparten, la segmentación es una prioridad.
- Copias de seguridad: no basta con crear copias. Debe existir al menos una copia desconectada o fuera del sitio y deben realizarse pruebas de restauración.
- Sitio web: el portal funciona como vitrina comercial y tienda. El contenido ajeno al negocio observado en la página principal requiere revisión de integridad, administración, complementos, temas, registros y alojamiento.
- Videovigilancia: las cámaras y grabadores deben operar con credenciales únicas, firmware actualizado y sin exposición directa mediante puertos abiertos cuando exista una alternativa más segura.
- Protección de datos personales: el sistema almacena información de clientes, por lo que se requiere control de acceso, finalidad definida, retención y eliminación segura.

8.1. Hallazgo público sobre el sitio web

El primer hallazgo corresponde al contenido externo no relacionado con la empresa que aparece incrustado en la página principal. Desde una perspectiva de gestión de seguridad, el tratamiento recomendado es abrir una revisión controlada del portal. El responsable web debe confirmar si el texto fue incorporado intencionalmente, revisar usuarios administradores, cambios recientes, complementos instalados, archivos modificados, temas, permisos, registros del alojamiento y copias de seguridad. También debe comprobar que no existan redirecciones, cuentas desconocidas o código agregado sin autorización.

La revisión debe realizarse sobre una copia o entorno de mantenimiento y con respaldo previo. Si se confirma una modificación no autorizada, la empresa debe cambiar credenciales administrativas, invalidar sesiones, actualizar componentes, restaurar desde una versión confiable cuando sea necesario y documentar el incidente. Si no se confirma un ataque, el hallazgo sigue siendo útil para mejorar el control de cambios y la supervisión de integridad del portal.

9. Estrategia integral de ciberseguridad

La estrategia propuesta se organiza en diferentes líneas de acción, donde cada uno responde a un riesgo identificado y puede verificarse mediante evidencia sencilla. La implementación documental queda definida en este informe; la implementación técnica debe ejecutarse sobre los sistemas reales por personal autorizado y quedar registrada con fecha, responsable y resultado.

9.1. Gobierno y responsabilidades

ER.SERVICES debe designar un responsable de seguridad de la información. Por el tamaño de la empresa, este rol puede ser asumido por la gerencia o por la persona que tenga autoridad para aprobar cambios, siempre que reciba apoyo técnico cuando sea necesario. El responsable conserva el inventario de activos, aprueba accesos, revisa incidentes y verifica los indicadores. Cada empleado es responsable de proteger sus credenciales y reportar comportamientos inusuales.

Los permisos deben responder a la función. El personal técnico necesita acceso a órdenes de servicio y a información necesaria para la reparación; el área comercial requiere funciones de ventas, inventario y clientes; la administración puede requerir reportes globales. Un usuario no debe recibir privilegios administrativos solo por comodidad. Las cuentas de administración del sistema, correo, hosting, router y cámaras deben separarse de las cuentas de uso cotidiano.

9.2. Política de control de acceso

- Cada empleado utilizará una cuenta personal e identificable; se prohíbe compartir usuarios para el sistema, correo o servicios críticos.
- Las contraseñas tendrán al menos 14 caracteres o se utilizarán frases largas; no deben reutilizarse entre servicios.
- Las cuentas de correo, sitio web, almacenamiento y administración habilitarán autenticación multifactor cuando el servicio lo permita.
- Las credenciales empresariales se almacenarán en un gestor de contraseñas, no en archivos de texto, chats o notas visibles.
- Los accesos se asignarán por función y se revisarán cada tres meses. Cuando una persona deje de trabajar en la empresa, sus accesos se deshabilitarán el mismo día.
- Las cuentas administrativas se usarán únicamente para tareas de administración y no para navegación o correo cotidiano.

9.3. Protección de estaciones de trabajo y portátiles

- Aplicar actualizaciones críticas en un plazo objetivo de 72 horas y el resto en una ventana mensual.
- Mantener protección antimalware/EDR activa, con análisis en tiempo real y actualización automática.
- Cifrar el disco de equipos que almacenen información de clientes o credenciales mediante BitLocker, FileVault o tecnología equivalente.
- Configurar bloqueo automático de pantalla después de un periodo corto de inactividad y exigir autenticación al reanudar.

- Evitar instalar software sin licencia o programas de procedencia desconocida. El software técnico debe mantenerse en un repositorio autorizado.

9.4. Segmentación y seguridad de red

La red se dividirá lógicamente en al menos cuatro zonas: administración, taller, visitantes y videovigilancia. La red administrativa tendrá acceso al sistema de gestión y a los recursos internos. La red de taller permitirá salida a Internet para diagnóstico, pero no acceso a la red administrativa. La red de invitados estará aislada de las demás. Las cámaras y el grabador se ubicarán en un segmento independiente. Cuando el equipo de red no permita VLAN, se puede implementar separación física con routers distintos como medida transitoria.

El Wi-Fi debe utilizar WPA2-AES o WPA3, deshabilitar WPS y mantener una contraseña distinta para cada red. Las credenciales de administración del router no pueden conservar valores predeterminados. La administración remota debe deshabilitarse si no es necesaria; cuando sea indispensable, se recomienda acceso mediante VPN o mediante el mecanismo seguro proporcionado por un equipo administrado.

9.5. Política de copias de seguridad y recuperación

Se propone mantener al menos tres copias de la información, en dos medios diferentes y una copia fuera del equipo principal o fuera del sitio. Para el sistema de gestión, la base de datos y los informes, se recomienda un respaldo diario automático, una copia semanal en un medio independiente y una copia cifrada fuera del sitio. Al menos una copia debe estar protegida contra modificación directa desde los equipos de usuarios para reducir el efecto del ransomware.

La existencia del archivo de respaldo no demuestra que pueda utilizarse. Cada trimestre debe seleccionarse una copia y realizar una restauración de prueba en un entorno controlado. El

resultado se registra con fecha, tamaño, tiempo de recuperación y observaciones. El responsable debe conocer dónde están las copias y cómo acceder a ellas en una emergencia.

9.6. Seguridad del sitio web y comercio electrónico

- Revisar de inmediato el contenido anómalo identificado y documentar la causa.
- Eliminar complementos, cuentas y temas que no se utilicen; reducir la superficie de ataque.
- Usar MFA en cuentas administrativas y limitar el número de administradores.
- Programar copias de seguridad del sitio y de la base de datos antes de cambios importantes y de forma periódica.
- Activar registros de acceso y de cambios, así como alertas de inicio de sesión cuando el proveedor lo permita.
- Usar HTTPS en todo el portal y comprobar periódicamente la vigencia del certificado.
- Revisar formularios, información de clientes y datos de pedidos para minimizar lo recolectado y definir tiempos de retención.
- Considerar un firewall de aplicación web o las funciones equivalentes del proveedor de alojamiento si son compatibles con el presupuesto.

9.7. Seguridad en cámaras y dispositivos IoT

Las cámaras de seguridad forman parte de la actividad comercial de ER.SERVICES y pueden también estar presentes en su propia infraestructura. Deben tratarse como dispositivos de red, no como equipos aislados. Se deben cambiar contraseñas predeterminadas, actualizar firmware, crear usuarios con privilegios limitados para visualización, separar la red de cámaras y evitar exposición directa a Internet mediante reenvío de puertos cuando exista una opción segura.

Las cuentas de administración del grabador o plataforma remota no deben compartirse entre técnicos. Cuando un empleado ya no requiera acceso, la cuenta se elimina o deshabilita. Las grabaciones se consideran información sensible porque pueden identificar personas, horarios y actividades; por ello, su acceso y tiempo de conservación deben definirse de acuerdo con una finalidad legítima y con la política de tratamiento de datos.

9.8. Gestión de información de clientes

- Recolectar únicamente los datos necesarios para prestar el servicio, facturar, contactar al cliente o cumplir obligaciones aplicables.
- No registrar contraseñas personales de clientes en campos abiertos cuando no sean necesarias. Si una credencial temporal es indispensable para una prueba, debe manejarse de forma controlada y eliminarse al finalizar.
- Los informes técnicos enviados por correo deben dirigirse al destinatario verificado y no contener datos adicionales innecesarios.
- Los soportes temporales creados durante la reparación deben eliminarse cuando el servicio finalice, salvo autorización o obligación de conservación.
- Las bases de datos exportadas para trabajo o respaldo deben permanecer cifradas y bajo control del responsable.

9.9. Gestión de incidentes

Todo empleado debe conocer una ruta única de reporte. Un incidente puede ser un archivo sospechoso, una cuenta bloqueada, un inicio de sesión desconocido, una pérdida de equipo, una modificación inesperada del sitio web, un cifrado de archivos, una filtración de datos o cualquier

evento que afecte la operación. La primera acción es informar; no se recomienda ocultar o borrar evidencias para “arreglar” el problema rápidamente.

El procedimiento se organiza en seis pasos: identificar, contener, preservar evidencias, erradicar la causa, recuperar el servicio y registrar las lecciones aprendidas. La contención puede incluir desconectar un equipo de la red, bloquear una cuenta o aislar un servicio. Después de recuperar, se deben cambiar credenciales afectadas, aplicar parches y revisar si el mismo problema puede repetirse.

9.10. Capacitación y cultura de seguridad

Con cinco empleados, la capacitación puede ser breve y frecuente. Se propone una sesión inicial de 60 a 90 minutos y refuerzos trimestrales de 20 minutos. Los temas prioritarios son phishing, contraseñas, MFA, manejo de equipos de clientes, archivos adjuntos, copias de seguridad, protección de datos y reporte de incidentes. Cada sesión debe dejar una lista de asistencia y una actividad corta de verificación.

Tabla 5
Conjunto de políticas propuesto para ER.SERVICES

Código	Política	Contenido principal	Responsable	Revisión
P-01	Política general de seguridad	Define alcance, principios, responsabilidades y cumplimiento.	Gerencia	Anual
P-02	Control de acceso y contraseñas	Usuarios individuales, MFA, mínimo privilegio y retiro de accesos.	Responsable de seguridad	Trimestral
P-03	Copias de seguridad	Frecuencia, medios, cifrado y	Responsable de sistema	Mensual/Trimestral

Código	Política	Contenido principal	Responsable	Revisión
		pruebas de restauración.		
P-04	Actualización y protección de endpoints	Parches, antimalware, cifrado y configuración segura.	Soporte técnico	Mensual
P-05	Red y Wi-Fi	Segmentación, redes de taller, invitados y cámaras.	Soporte técnico	Semestral
P-06	Sitio web	Cambios, cuentas, actualizaciones, respaldo e integridad.	Administrador web	Mensual
P-07	Tratamiento de datos	Acceso, finalidad, retención y eliminación.	Gerencia	Anual
P-08	Gestión de incidentes	Reporte, contención, recuperación y registro.	Responsable de seguridad	Después de cada incidente
P-09	Uso de medios y equipos de clientes	Aislamiento, USB, copias temporales y autorización.	Soporte técnico	Semestral
P-10	Continuidad	Prioridades, restauración, contactos y operación mínima.	Gerencia	Semestral

Nota. Los responsables corresponden a roles, no necesariamente a cargos exclusivos; una misma persona puede asumir varios roles en una empresa de cinco empleados.

11. Plan de implementación de 90 días

El plan prioriza acciones de bajo costo y alto impacto. La secuencia evita iniciar por controles avanzados mientras siguen abiertos problemas básicos como cuentas compartidas o respaldos no probados. Las fechas exactas se definen cuando la empresa apruebe el inicio, pero la distribución propuesta permite completar la fase inicial en tres meses.

Tabla 6
Plan inicial de implementación

Periodo	Frente	Acciones	Evidencia esperada
Días 1-15	Gobierno e inventario	Aprobar política general; designar responsable; inventariar activos; identificar usuarios; registrar respaldos actuales.	Política firmada e inventario base.
Días 1-15	Contención web	Revisar contenido anómalo; respaldar portal; verificar usuarios administradores; actualizar componentes prioritarios.	Acta de revisión web y evidencia de cambios.
Días 16-30	Identidades	Eliminar cuentas compartidas; activar MFA; usar gestor de contraseñas; retirar accesos innecesarios.	Listado de cuentas y prueba de MFA.
Días 16-30	Backups	Configurar esquema 3-2-1 para sistema y archivos críticos; documentar ubicación y cifrado.	Registro de respaldos automáticos.
Días 31-45	Endpoints	Actualizar sistemas; activar antimalware/EDR; cifrar equipos con	Checklist por equipo.

Periodo	Frente	Acciones	Evidencia esperada
Días 31-60	Red	datos; restringir software no autorizado. Separar administración, taller, invitados y cámaras; cambiar claves predeterminadas; deshabilitar WPS.	Diagrama y prueba de aislamiento.
Días 46-60	Datos personales	Revisar datos recolectados, permisos, retención y política de tratamiento.	Matriz de datos y ajustes de acceso.
Días 61-75	Incidentes y continuidad	Probar procedimiento de incidente; realizar restauración de prueba; documentar contactos y prioridades.	Acta de simulacro y prueba de restauración.
Días 76-90	Capacitación	Capacitar a los cinco empleados en phishing, contraseñas, datos y equipos de clientes.	Registro de asistencia y evaluación.
Días 76-90	Medición	Calcular indicadores; revisar riesgos; aprobar acciones pendientes.	Informe de cierre de fase inicial.

Nota. La ejecución técnica debe realizarse con acceso autorizado a la infraestructura real de ER.SERVICES.

12. Indicadores de seguimiento

Los indicadores permiten saber si los controles se mantienen en el tiempo. En una empresa pequeña deben ser pocos y fáciles de medir. Se propone revisar el tablero una vez al mes y presentar un resumen trimestral a la gerencia.

Tabla 7
Indicadores mínimos para el seguimiento de la estrategia

ID	Indicador	Cálculo	Meta
KPI-1	Cobertura MFA	Cuentas críticas con MFA / cuentas críticas totales $\times 100$	100 %
KPI-2	Actualización	Equipos con parches del mes / equipos inventariados $\times 100$	≥ 95 %
KPI-3	Protección endpoint	Equipos con antimalware/EDR activo / equipos inventariados $\times 100$	100 %
KPI-4	Éxito de respaldos	Respaldos exitosos / respaldos programados $\times 100$	≥ 98 %
KPI-5	Restauración	Pruebas de restauración exitosas / pruebas programadas	100 % trimestral
KPI-6	Accesos vigentes	Cuentas revisadas / cuentas totales	100 % trimestral
KPI-7	Capacitación	Empleados capacitados / 5 $\times 100$	100 %
KPI-8	Incidentes	Incidentes con registro y cierre documentado / incidentes reportados	100 %

Nota. Las metas pueden ajustarse después de tres meses de medición real.

13. Estimación de recursos

La propuesta prioriza configuraciones y hábitos antes que compras. No obstante, algunos controles pueden requerir licencias, almacenamiento o equipo de red. La siguiente estimación es orientativa y debe cotizarse con proveedores antes de aprobar un presupuesto. Los valores dependen de marcas, capacidades y servicios ya contratados.

Tabla 8

Estimación orientativa de recursos para el primer año

Recurso	Alcance	Rango estimado (COP)	Observación
Gestor de contraseñas	5 usuarios, versión empresarial o equivalente.	0 - 600.000/año	Puede iniciar con solución de bajo costo y MFA.
Protección de endpoints	Licencia para aproximadamente 5 equipos.	600.000 - 1.500.000/año	Depende de funciones EDR y consola.
Respaldo externo/nube	1 TB aproximado y copia local cifrada.	500.000 - 1.500.000/año	Ajustar a volumen real.
Router/firewall administrable	Equipo con segmentación/VLAN y VPN.	500.000 - 1.500.000	Compra única si el actual no cumple.
Disco externo cifrable/UPS	Medio de respaldo y continuidad eléctrica básica.	500.000 - 1.200.000	Compra única; no debe quedar siempre conectado.
Capacitación	Sesiones internas y material de sensibilización.	0 - 500.000/año	Puede ejecutarse internamente.

Nota. Valores académicos de referencia, no cotización comercial. El costo final depende de los productos y servicios seleccionados por la empresa.

14. Resultados esperados de la implementación

Al finalizar la fase inicial, ER.SERVICES debe contar con un inventario actualizado de activos, una política aprobada, responsables definidos, usuarios individuales, MFA en cuentas críticas, esquema de copias de seguridad con prueba de restauración, equipos actualizados, red de taller separada, controles básicos para cámaras, un sitio web revisado y un procedimiento sencillo de respuesta a incidentes. Estos resultados son verificables mediante evidencias y no dependen de una percepción general de que “los equipos están protegidos”.

El principal cambio esperado es pasar de decisiones reactivas a una gestión organizada. Un archivo malicioso seguirá siendo posible y un empleado todavía puede recibir un correo de phishing; la diferencia es que la empresa tendrá barreras, respaldos y una ruta de respuesta. La seguridad se convierte en un proceso continuo, no en una instalación única de antivirus.

15. Limitaciones del ejercicio

El informe no tuvo acceso directo al sistema interno, base de datos, computadores, router, grabador de cámaras, consola de correo, panel de hosting ni registros de incidentes. Tampoco se realizaron pruebas de penetración ni escaneos. Por esta razón, la matriz de riesgos se considera una línea base para validación. Antes de cerrar la implementación técnica, el responsable debe confirmar versiones, configuraciones, topología, usuarios, frecuencia real de copias y dependencia de proveedores.

La información pública de redes sociales no pudo validarse de manera suficiente para ser incorporada como fuente. La investigación se concentra en el portal oficial y en referencias normativas y técnicas. Esta limitación se deja explícita para mantener trazabilidad de la evidencia utilizada y evitar atribuir a ER.SERVICES información de terceros.

Conclusiones

1. ER.SERVICES depende de información digital para procesos esenciales como atención de clientes, informes de servicio técnico, ventas e inventario. Aunque se trata de una empresa pequeña, el impacto de perder o alterar esos datos es alto porque varias actividades se concentran en un mismo sistema y en un equipo humano reducido.
2. La aplicación de ISO/IEC 31000:2018 como referencia de gestión permite estructurar el trabajo alrededor del contexto, la identificación, análisis, la evaluación y el tratamiento de los riesgos. Para la selección de controles.
3. La amenaza de mayor prioridad son el acceso no autorizado al sistema, ransomware, equipos de clientes conectados al entorno interno, respaldos no restaurables, robo de cuentas, exposición de datos personales y compromiso del sitio web. El contenido externo observado en la página principal justifica una revisión inmediata de integridad, sin que por sí solo pueda considerarse prueba definitiva de una intrusión.
4. La estrategia propuesta es viable para cinco empleados porque concentra el esfuerzo en controles básicos: cuentas personales, MFA, gestor de contraseñas, respaldo 3-2-1, actualización, antimalware, cifrado, segmentación, protección del portal, procedimiento de incidentes y capacitación. Su valor está en que cada control genera una evidencia que puede revisarse.
5. La ciberdefensa, entendida en el marco colombiano como una capacidad del Estado, no implica que ER.SERVICES deba desarrollar acciones ofensivas. La empresa debe fortalecer su defensa, preservar evidencias, recuperar su operación y utilizar los canales institucionales correspondientes cuando un incidente lo requiera.

Recomendaciones

- Validar si existen cuentas compartidas en el sistema, correo, router, hosting o cámaras y reemplazarlas por cuentas individuales.
- Implementar y probar el respaldo de la información crítica antes de realizar cambios mayores en infraestructura o aplicaciones.
- Separar físicamente o mediante VLAN la red utilizada para equipos de clientes de la red administrativa.
- Crear una política de tratamiento de datos personales o revisar la existente, asegurando coherencia entre lo que se informa a los clientes y la operación real.
- Solicitar una evaluación técnica autorizada cuando la empresa haya implementado los controles básicos, con el fin de validar configuraciones y vulnerabilidades internas sin afectar la operación.
- Revisar anualmente la estrategia y actualizarla cuando cambie el sistema, el proveedor de hosting, la red, el número de empleados o los servicios prestados.

Referencias

- Congreso de Colombia. (2009). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. SUIN-Juriscol. <https://www.suin-juriscol.gov.co/clp/contenidos.dll/Leyes/1676699>
- Congreso de Colombia. (2012). *Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*. Función Pública. <https://www1.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Departamento Nacional de Planeación. (2011). *CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa*. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>
- Departamento Nacional de Planeación. (2020). *CONPES 3995: Política Nacional de Confianza y Seguridad Digital*. <https://dnp.gov.co/LaEntidad/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-confianza-y-seguridad-digital.aspx>
- ER.Services. (s. f.-a). *Inicio*. Recuperado el 5 de septiembre de 2026, de <https://www.erservices.com.co/>
- ER.Services. (s. f.-b). *Servicios*. Recuperado el 5 de septiembre de 2026, de <https://www.erservices.com.co/index.php/servicios/>

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

International Organization for Standardization. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls*. <https://www.iso.org/standard/75652.html>

International Organization for Standardization. (2018). *ISO 31000:2018*

Risk management — Guidelines <https://www.iso.org/standard/65694.html>

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información*. https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_min_tic_0500_2021.htm

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025a). *Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), versión 5.0*. https://www.mintic.gov.co/portal/715/articles-403045_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025b). *Resolución 2277 de 2025, por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia*. https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_2277_2025.htm

Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.). *Modelo de Seguridad y Privacidad de la Información (MSPI)*. Recuperado el 5 de septiembre de 2026,

de <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/>

Presidencia de la República de Colombia. (2015). *Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo*. SUIN-

Juriscol. [https://www.suin-](https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos%2F30019935)

[juriscol.gov.co/viewDocument.asp?ruta=Decretos%2F30019935](https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos%2F30019935)

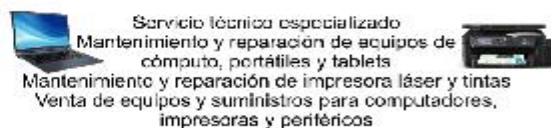
Presidencia de la República de Colombia. (2022). *Decreto 338 de 2022, por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015 para fortalecer la gobernanza de la seguridad digital*. Función

Pública. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>

Anexos

16. Anexo A

Carta de autorización de datos de ER. SERVICES, autorizado por representante legal ELIONARDO RUEDA PEREZ



San José de Cúcuta, 24 de septiembre del 2026

AUTORIZACION DE DATOS DE LA EMPRESA

Yo, **ELIONARDO RUEDA PEREZ**, identificado con cédula de ciudadanía No. **1090401643**, en calidad de representante legal y propietario de la empresa **ER. SERVICES**, identificada con NIT No. 1090401643-5, por medio de la presente:

AUTORIZO

A **WILMER ANDRES MOJICA CARDONA**, identificado con cédula de ciudadanía **1233488059** de la institución educativa **CORPORACION UNIVERSITARIA REMINGTON**, para utilizar el nombre, información y datos relacionados con la empresa **ER.SERVICES**, exclusivamente con fines académicos de investigación, dentro del desarrollo del proyecto o trabajo académico.

La información de la empresa podrá ser utilizada para la elaboración de informes, trabajos escritos, presentaciones, análisis, diagnósticos y demás actividades relacionadas directamente con el proyecto académico.

La presente autorización se autoriza bajo las siguientes condiciones:

1. La información de la empresa deberá ser utilizada exclusivamente para fines académicos y educativos.
2. No se permitirá utilizar la información para fines comerciales, publicitarios o diferentes a los establecidos en esta autorización.
3. El estudiante se compromete a manejar la información de manera responsable y a mantener la confidencialidad de aquella información que la empresa considere reservada.
4. La utilización del nombre de la empresa deberá estar relacionada únicamente con el desarrollo del proyecto académico autorizado.
5. Cuando sea necesario, se podrán omitir o modificar datos que puedan comprometer información confidencial, financiera, personal, técnica o estratégica de la empresa.

La presente autorización se expide a solicitud del interesado, para los fines académicos correspondientes.

Atentamente,

ELIONARDO RUEDA PEREZ.

Representante legal y propietario de ER. SERVICES