Gestión de ciberseguridad en servicios tercerizados

Corporación Universitaria Remington.

Facultad de Ingenierías

Ingeniería de sistemas

Presentado por:

Jesús Alberto Arias Castrillón

Michael Alejandro Hernández Diaz

Mario Alberto Cera Moreno

Tutor del trabajo de grado: Jorge Mauricio Sepúlveda Castaño

Opción de Trabajo de grado Seminario

Octubre 2025

Tabla de Contenidos

Tabla de contenido

1. Resumen

El presente trabajo de grado titulado “Gestión de ciberseguridad en servicios tercerizados” tiene como objetivo analizar, estructurar e implementar estrategias de seguridad informática aplicadas a entornos donde las organizaciones delegan parte de su infraestructura tecnológica a proveedores externos2. Se propone un modelo integral que garantice la protección de los activos digitales, el cumplimiento normativo y la continuidad operativa mediante políticas, controles y acuerdos de servicio claramente definidos.

El estudio aborda la importancia del descubrimiento y mapeo de la infraestructura crítica, identificando activos, flujos de información y niveles de privilegios para establecer una línea base segura3. Asimismo, se detalla la gestión de seguridad en endpoints, donde se enfatiza la automatización de parches, la clasificación de vulnerabilidades y la migración hacia soluciones avanzadas como XDR (Extended Detection and Response), que permiten una detección y respuesta proactiva ante amenazas **(Sophos, 2025)**.

Otro componente esencial es la protección del correo electrónico, principal vector de ataque actual, que se fortalece mediante autenticación de dominios (SPF, DKIM, DMARC), cifrado de comunicaciones y análisis dinámico de archivos mediante sandboxing. De igual manera, se desarrolla la gestión de incidentes bajo metodologías reconocidas (ISO 27035, NIST SP 800-61), asegurando una respuesta oportuna y documentada ante eventos de seguridad.

El trabajo incluye la formulación de acuerdos de nivel de servicio (ANS) **(Raza, 2024)**, donde se definen responsabilidades, niveles de soporte y tiempos de respuesta, garantizando la transparencia y calidad del servicio tercerizado. Además, se incorporan políticas de protección de datos personales, en cumplimiento con la **Ley 1581 de 2012 (Gobierno de Colombia, 2012)**56, el Decreto 1377 de 2013 y estándares internacionales como **ISO/IEC 27001:2022 (International Organization for Standardization [ISO], 2021)**57 y GDPR.

Finalmente, se establecen exclusiones del servicio y mecanismos de control que delimitan responsabilidades entre proveedor y cliente. Este modelo demuestra cómo una gestión integral de ciberseguridad en esquemas de outsourcing puede fortalecer la confianza digital, mitigar riesgos operativos y asegurar la sostenibilidad tecnológica de las organizaciones.

Palabras clave

Ciberseguridad – Outsourcing – Gestión de riesgos – ISO 27001 – Protección de datos.

2. Marco conceptual y contextual

En la actualidad, las organizaciones dependen de la tecnología para desarrollar sus operaciones, almacenar información crítica y comunicarse de manera eficiente. Este entorno digital, aunque indispensable, ha incrementado a la exposición a amenazas informáticas, por lo que la ciberseguridad se ha convertido en un componente estratégico para garantizar la continuidad del negocio, la protección de los datos y la confianza de los usuarios (**ISO, 2021; MinTIC, 2024**).

La tercerización de servicios tecnológicos (outsourcing) ha surgido como una alternativa eficaz para que las empresas optimicen recursos, accedan a conocimientos especializados y fortalezcan sus infraestructuras sin aumentar su carga operativa interna (**Navarro, 2024; ITSM.tools, 2025**). Sin embargo, delegar funciones críticas de seguridad a proveedores externos implica nuevos desafíos relacionados con la confidencialidad, integridad y disponibilidad de la información.

En este contexto, el presente trabajo desarrolla un modelo de gestión integral de ciberseguridad aplicado a empresas que externalizan sus servicios tecnológicos, tomando como referencia la empresa ficticia Security Tech Solutions S.A.S. Esta compañía se especializa en la prestación de servicios de seguridad informática, monitoreo de redes, protección de endpoints, respuesta a incidentes y asesorías en cumplimiento normativo (**ISO, 2021; MinTIC, 2024**).

El marco conceptual del proyecto se fundamenta en estándares internacionales como **ISO/IEC 27001:2022 (**International Organization for Standardization **[ISO], 2021)**710, ISO/IEC 20000-1:2018, y NIST SP 800-53, que proporcionan lineamientos para la implementación de sistemas de gestión de seguridad y calidad en servicios TI. Además, se consideran las leyes colombianas que regulan la protección de datos personales, como la Ley 1581 de 2012 **(Gobierno de Colombia, 2012)** y el Decreto 1377 de 2013, junto con las disposiciones del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) (Ministerio de Tecnologías de la Información y las Comunicaciones **– MinTIC, 2024)**.

Este marco permite contextualizar la necesidad de establecer políticas, procedimientos y acuerdos de servicio que definan las responsabilidades tanto del proveedor como del cliente, asegurando que la ciberseguridad tercerizada se ejecute de forma controlada, confiable y alineada con los objetivos estratégicos de cada organización

3. Desarrollo e implementación del aprendizaje

En esta etapa se aplicaron los conocimientos adquiridos en el seminario sobre transformación digital y outsourcing inteligente en TI, enfocándolos en la Gestión de ciberseguridad y protección de infraestructuras tercerizadas a través de la empresa ficticia Security Tech Solutions S.A.S.

Primero, se realizó el mapeo de la infraestructura crítica, identificando activos, segmentos de red y flujos de información para establecer una línea base segura. Luego, se definieron políticas de acceso y control de privilegios, limitando los permisos de acuerdo con el rol de cada usuario.

Se implementaron medidas de seguridad en endpoints, como la automatización de parches, la gestión de vulnerabilidades y el uso de plataformas XDR, que fortalecen la detección y respuesta ante amenazas **(Sophos, 2025)**. Asimismo, se diseñó un sistema de protección de correo electrónico con autenticación (SPF, DKIM, DMARC) y cifrado de datos, complementado con programas de capacitación y concienciación para reducir riesgos humanos.

Finalmente, se establecieron acuerdos de nivel de servicio (ANS) **(Raza, 2024)** que definen responsabilidades, tiempos de respuesta y niveles de soporte, junto con políticas de protección de datos personales **(Gobierno de Colombia, 2012)** y un plan de respuesta a incidentes alineado con las normas ISO 27035 y NIST SP 800-61.

En conjunto, estas acciones reflejan la aplicación práctica de los conceptos del seminario, integrando tecnología, gestión y cumplimiento normativo para fortalecer la ciberseguridad en servicios tercerizados.

4. Seguridad perimetral

4.1 Descubrimiento y Mapeo de la Infraestructura Crítica

Antes de implementar cualquier política, el equipo de ciberseguridad debe obtener una visibilidad total de lo que vamos a proteger.

Se requiere un conocimiento detallado de la topología de Red:

- Identificación de Segmentos de Red: mapear no solo las redes principales (LAN, WAN), sino también la micro segmentación existente, esto incluye redes de invitados, redes operacionales, redes de servidores y cualquier zona desmilitarizada (DMZ) que aloje servicios de cara al público.
- Inventario de Activos: registrar todos los dispositivos que interactúan con el perímetro; un activo desconocido es una vulnerabilidad potencial.
- Flujo de Tráfico: entender qué información fluye entre segmentos, qué protocolos se utilizan y cuáles son las direcciones de origen y destino más frecuentes, esto permite una gestión de excepciones más segura.

4.2 Análisis del Modelo de Control de Acceso y Privilegios.

La seguridad perimetral debe adaptarse a la forma en que está organizada la empresa, aplicando controles que limiten los accesos únicamente a lo estrictamente necesario para cada usuario o área.

- Evaluación del acceso por Rol, es crucial determinar los niveles de permisos basados en la función o el área de trabajo (Finanzas, Recursos Humanos, Desarrollo). Por ejemplo, los usuarios de contabilidad no deberían tener acceso directo a los servidores de desarrollo.
- Políticas de Usuarios Internos: se debe documentar qué usuarios o grupos de usuarios (áreas) tienen la necesidad de acceder a servicios externos a través del perímetro (VPN, servicios en la nube, servicios de terceros), y con qué restricciones de tiempo y protocolo.
- Gestión de Acceso Remoto (VPN): es vital establecer políticas rigurosas sobre quién puede acceder a la red interna desde el exterior, qué recursos específicos pueden alcanzar y mediante qué métodos de autenticación multifactor (MFA).

4.3 Documentación, Conformidad y Riesgos.

La información recopilada es la base para el servicio continuo y la mitigación de riesgos:

- El conocimiento de la infraestructura y los privilegios permite crear una línea base de las configuraciones correctas, cualquier desviación de esta línea es una alerta de seguridad o un error de configuración.

- Al conocer la división de la red, se puede asignar un valor de riesgo específico a cada segmento; por ejemplo, la DMZ y la red de administración del Firewall tienen un riesgo mucho más alto que la red de invitados.

- Con el fin de garantizar el Cumplimiento se debe hacer un mapeo interno asegurando que las políticas perimetrales cumplan con las regulaciones aplicables al cliente o usuario final, evitando la transferencia no autorizada de datos sensibles fuera de la red.

5. Seguridad Endpoint

La gestión de la seguridad del endpoints (servidores, estaciones de trabajo, dispositivos móviles) es crítica, ya que estos dispositivos representan la mayor superficie de ataque de una organización; una administración efectiva requiere un enfoque metódico que va desde el conocimiento del activo hasta la capacidad de respuesta inmediata.

5.1 Inventario, Clasificación y Gestión de Vulnerabilidades.

El punto de partida de cualquier estrategia de seguridad es el conocimiento exhaustivo de los activos.

- Es fundamental mantener un inventario de equipos en tiempo real, que no solo enumere los dispositivos, sino que los clasifique según su criticidad para el negocio, no se puede proteger lo que no se conoce.
- Se debe registrar y monitorizar activamente los sistemas operativos (SO) instalados en cada equipo, esta información es vital para identificar sistemas obsoletos o sin soporte, que son un foco de vulnerabilidades.
- El servicio debe incluir la detección, priorización y gestión de vulnerabilidades, asegurando que los parches y actualizaciones se apliquen de forma periódica y diligente para mitigar el riesgo antes de que sea explotado.

5.2 Fortalecimiento a través de políticas de uso y control.

Una vez conocido el inventario, se definen las políticas que limitan el riesgo de exposición a través del comportamiento del usuario y la configuración del dispositivo.

- Las políticas de seguridad en el Endpoint deben ajustarse a la tolerancia al riesgo y a las normativas internas de la empresa, evitando la interrupción del negocio mientras se garantiza la protección.

- **Control Granular de acciones del usuario:**

  - Restringir el acceso a sitios web maliciosos y bloquear la ejecución de aplicaciones no autorizadas o de alto riesgo, minimizando la posibilidad de infección por malware.

  - Implementar políticas para restringir o monitorizar el uso de dispositivos externos (memorias USB, discos duros), que a menudo son vectores de malware o puntos de fuga de información.

  - Se debe establecer una periodicidad clara y automatizada para la actualización del agente de seguridad, garantizando que las firmas y capacidades de detección se mantengan al día.

5.3 Evolución Tecnológica: Del Antivirus a la Respuesta (XDR)

El riesgo moderno exige ir más allá de la simple detección de *malware* conocida, antivirus tradicional.

- Migración a XDR (Extended Detection and Response), es imperativo utilizar una solución con capacidad de respuesta (Detection and Response), idealmente XDR (Sophos, 2025). A diferencia del Antivirus tradicional que solo detecta y aísla, el XDR:
  - Detecta Comportamientos Anómalos utilizando técnicas avanzadas apoyadas de IA para identificar movimientos sospechosos, ataques o amenazas de día cero.
  -
  - Con la visibilidad extendida puede correlacionar eventos no solo en el Endpoint, sino también en la red, correo electrónico y seguridad perimetral, ofreciendo un contexto completo del ataque.
  -
  - Capacidad de remediación proactiva permitiendo la acción inmediata como aislar el equipo comprometido de la red, finalizar procesos maliciosos y deshacer los cambios realizados por el atacante, garantizando la contención rápida del incidente y de manera desatendida.

Figura 1. https://www.sophos.com/es-es/products/next-gen-firewall/ecosystem

6. Protección de correo electrónico

Si bien la seguridad perimetral tradicional (firewall) y la protección del Endpoint (XDR) son cruciales, el correo electrónico se ha convertido en el principal vector de ataque; por lo tanto, es indispensable implementar una solución avanzada de seguridad de correo electrónico que actúe como una defensa en profundidad contra el malware, el phishing y la suplantación.

6.1 La estrategia de protección debe basarse en los siguientes pilares:

- Autenticación e identificación a nivel de dominio (Protección contra Suplantación) para mitigar los ataques de suplantación de identidad (spoofing y Business Email Compromise - BEC), la solución debe validar la legitimidad de cada remitente.

- Para la implementación de protocolos de autenticación de correo es fundamental configurar y mantener los siguientes registros DNS, que actúan como la cédula de identidad del dominio:

    - SPF (Sender Policy Framework), especifica qué servidores están autorizados para enviar correos en nombre del dominio.
    - DKIM (DomainKeys Identified Mail), utiliza una firma digital criptográfica para verificar que el contenido del correo no fue alterado durante el tránsito.
    - DMARC (Domain-based Message Authentication, Reporting & Conformance), indica a los servidores receptores qué hacer (rechazar, poner en cuarentena, o no hacer nada) con los correos que fallan la validación SPF y DKIM, protegiendo activamente la marca de la empresa.

- Cifrado de correo electrónico, para la comunicación de datos sensibles, la solución debe garantizar el cifrado de extremo a extremo, asegurando la confidencialidad de la información enviada y recibida.

6.2 Detección Avanzada de Amenazas y Sandboxing

La solución de seguridad debe inspeccionar el contenido más allá de las firmas tradicionales, enfrentándose a amenazas sofisticadas:

- Análisis dinámico de contenido, los correos con archivos adjuntos sospechosos o URL desconocidas deben ser detonados y analizados en un entorno aislado y seguro antes de llegar al usuario; esto previene la ejecución de *malware* y la verificación de enlaces maliciosos en tiempo real.

- Filtros de Contenido y Reputación, se deben implementar mecanismos de lista negra y lista blanca, pero de manera inteligente y contextualizada, así como utilizar

bases de datos de reputación global para bloquear remitentes y direcciones IP conocidas por distribuir spam y phishing.

- La solución debe proveer una bandeja de cuarentena centralizada y accesible, que permita a los administradores y, en algunos casos, a los usuarios, revisar y analizar de forma segura los correos que fueron bloqueados por ser sospechosos, minimizando los falsos positivos sin comprometer la seguridad.

6.3 Mitigación del Factor Humano y Concientización

Reconocemos que la seguridad no depende solo de la tecnología, sino también del comportamiento y la atención de los usuarios; por eso, trabajamos en la formación y concientización del personal, promoviendo buenas prácticas que reduzcan los riesgos asociados al error humano y fortalezcan la cultura de ciberseguridad dentro de la organización.

- Reescritura de URL, la solución debe reescribir dinámicamente los enlaces en los correos electrónicos, dirigiéndolos a un servidor de análisis que verifica el destino al momento del clic del usuario, incluso si el enlace era seguro cuando el correo fue recibido.
- Capacitación Continua, complementar la tecnología con programas regulares de concienciación en seguridad, incluyendo simulacros de phishing periódicos, para enseñar a los usuarios a reconocer y reportar correos fraudulentos, convirtiéndolos en una primera línea de defensa.

7. Detección, priorización y remediación de vulnerabilidades de punto final.

La gestión de vulnerabilidades y parches es un pilar esencial en la ciberseguridad corporativa, los atacantes explotan constantemente fallas de seguridad conocidas en sistemas operativos y aplicaciones antiguas o desactualizadas, por lo que la actualización continua no es una opción, sino un requisito.

7.1 El Riesgo de las Versiones Obsoletas y la Superficie de Ataque.

Las versiones antiguas de sistemas operativos y aplicaciones representan una deuda de seguridad significativa por eso:

- Los fabricantes publican constantemente parches para remediar fallas de seguridad que han sido descubiertas y, a menudo, ya están siendo activamente explotadas por atacantes; un sistema desactualizado permanece expuesto a estas amenazas.

- Cuando un sistema operativo o una aplicación llega a su fin de vida útil, el fabricante deja de emitir parches de seguridad, dejando a la empresa indefensa ante cualquier nueva vulnerabilidad.

- Cada aplicación desactualizada o sistema sin parchear aumenta la superficie de ataque de la compañía, creando múltiples puntos de entrada para malware, ransomware y actores maliciosos.

7.2 La Necesidad de la Automatización y la Centralización

La gestión manual de parches es insostenible en entornos corporativos modernos, la cantidad de aplicaciones, la frecuencia de las actualizaciones y la diversidad de sistemas hacen que la tarea sea agotadora, propensa a errores e ineficaz, por tal manera:

- Los fabricantes lanzan parches de seguridad de manera constante (mensual, semanal e incluso diaria) en ciclos conocidos como "Patch Tuesday" y fuera de banda.

- El tiempo entre el descubrimiento público de una vulnerabilidad crítica y su explotación activa por atacantes es cada vez más corto, exigiendo una remediación rápida.

Por lo tanto, es indispensable migrar a una Plataforma de Gestión de Parches y Vulnerabilidades (Patch Management).

7.3 Solución clave plataformas de gestión automatizada

La solución radica en implementar plataformas que centralicen y automaticen el ciclo de gestión de vulnerabilidades, como herramientas de gestión unificada de endpoints o soluciones especializadas (similares a Vicarius, que permiten la orquestación) (**Sophos, 2025**).

Funcionalidades Críticas de la Plataforma:

- Inventario y descubrimiento constante, la plataforma debe escanear los puntos finales de forma constante para identificar todas las actualizaciones disponibles de la lista de aplicaciones instaladas y sistemas operativos.

- No todos los parches tienen la misma urgencia, la herramienta debe priorizar automáticamente las actualizaciones según el nivel de criticidad de la vulnerabilidad y el impacto potencial en el negocio **(Navarro, 2024).**

- La gestión de parches debe automatizarse mediante tareas programadas que permitan:
    - Pruebas para desplegar primero los parches en un pequeño grupo de equipos para validar su compatibilidad y evitar fallos operativos en producción **(ISO, 2021).**
    - Una vez probados, el despliegue a la red completa debe ser automático, sin requerir intervención manual en cada dispositivo.

- Informes y Auditoría: la plataforma debe generar reportes claros que demuestren el estado de cumplimiento de parches y vulnerabilidades, lo cual es esencial para auditorías internas, normativas (como ISO 27001) (**International Organization for Standardization [ISO], 2021**) y la gestión de riesgos.

Al automatizar este proceso, la compañía pasa de una gestión reactiva y manual a una estrategia de seguridad proactiva y escalable.

8. Acuerdos de nivel de servicio (ANS)

En nuestra empresa Security Tech Solutions S.A.S asumimos nuestros acuerdos de nivel de servicio (**ANS**) como un compromiso directo con cada uno de nuestros clientes **(Raza, 2024)**; a través de estos acuerdos, definimos de manera clara los estándares de calidad, disponibilidad y tiempos de atención que orientan nuestra operación3.

Nuestro objetivo es garantizar que cada servicio prestado cumpla con los niveles de desempeño esperados, manteniendo siempre la transparencia en los procesos y la eficiencia en la gestión de incidentes; estos acuerdos reflejan nuestra responsabilidad por ofrecer soluciones alineadas con las necesidades del negocio de cada cliente, fortaleciendo la confianza y asegurando la continuidad de sus operaciones tecnológicas.

Figura.2 https://blog.qservus.com/que-es-un-acuerdo-de-nivel-de-servicio-ans-y-como-escribir-uno/

8.1 Descripción del servicio

Nuestro servicio abarca la monitorización, gestión y la protección de la infraestructura tecnológica, el análisis y mitigación de vulnerabilidades, respuestas ante incidentes de seguridad, administración de redes, soporte técnico especializado y asesorías continuas en seguridad informática (**ISO, 2021; MinTIC, 2024**).

8.2 Alcance del servicio

- Soporte remoto 7x2436.
- Acceso a mesa de ayuda (Help Desk) en la nube (**Navarro, 2024**).
- Monitoreo permanente de los sistemas de seguridad perimetral que se emplearan endpoints y correo electrónico.
- Generación de reportes mensuales (KPI), según acuerdos con el cliente; informes de incidentes y cumplimiento de métricas de servicio (**Raza, 2024**).
- Gestiones de actualizaciones automáticas a niveles de aplicaciones y sistemas operativo (**Ambit, 2020; Ministerio TIC, 2022**).

8.3 Definición de responsabilidades

- En Security Tech Solutions S.A.S, asumimos la responsabilidad de garantizar la continuidad operativa de los servicios que ofrecemos, cumpliendo con los tiempos de respuesta acordados y asegurando en todo momento la confidencialidad de la información que gestionamos (**ISO, 2021**).
- Por parte del cliente, es fundamental la notificación oportuna de cualquier incidente que pueda afectar la seguridad, como la pérdida de equipos o el uso indebido de credenciales (**MinTIC, 2024)**.
- Asimismo, hemos establecido mecanismos claros de escalamiento para asegurar una atención prioritaria en casos críticos, permitiendo una respuesta rápida y coordinada ante cualquier situación que comprometa la integridad de los sistemas o la información (**Navarro, 2024; Ministerio TIC, 2022**).
- . Es responsabilidad del cliente informar la adquisición de nuevos equipos, buzones de correo, configuraciones de segmentos de red, con el fin de que estos sean ingresados al sistema de protección y monitoreo.

8.4 Nivel de soporte

- **Nivel 1:** Atención de incidencias básicas, registro y canalización de solicitudes.
- **Nivel 2**: Soporte técnico especializado para la solución de fallas intermedias o configuraciones específicas.
- **Nivel 3:** Intervención avanzada, análisis forense digital y coordinación con fabricantes o aliados estratégicos.

8.5 Tiempos de respuesta y resolución

- **Nivel alto:** Respuesta en menos de 1 hora, resolución estimada en 4 horas.
- **Nivel medio:** Respuesta en 2 horas, resolución estimada en 8 horas.
- **Nivel bajo:** Respuesta en 4 horas, resolución en 24 horas.

9. Personal calificado y certificado

En Security Tech Solutions S.A.S, contamos con un equipo técnico altamente calificado, con certificaciones reconocidas y amplia experiencia en la gestión de riesgos informáticos y la protección de activos digitales; sabemos que la calidad de nuestros servicios depende directamente del conocimiento y la preparación de nuestro personal, por eso promovemos la capacitación continua y el desarrollo profesional de nuestros colaboradores; además nuestro compromiso con el cliente es garantizarle que cada proyecto sea atendido por especialistas competentes, capaces de ofrecer soluciones seguras, eficientes y adaptadas a las necesidades de cada cliente (**Navarro, 2024; Ambit, 2020**).

9.1 Perfil profesional

Nuestro personal encargado ha de poseer formación académica en ingeniería o en tecnología de sistemas, redes o seguridad informática, con una experiencia mínima de tres años en administración de infraestructuras tecnológicas, gestión de incidentes y auditoria de seguridad

9.2 Certificaciones recomendadas

Para garantizar la calidad del servicio prestado y el cumplimiento de los estándares internacionales, el personal técnico y de gestión cuenta con certificación:

- **CompTIA Security+**: Fundamentos de seguridad informática.
- **CEH (Certified Ethical Hacker)**: Pruebas de penetración y análisis de vulnerabilidades.
- **CISM (Certified Information Security Manager)** o **CISSP**: Gestión avanzada de la seguridad de la información.
- **ISO/IEC 27001 Lead Implementer**: Implementación de Sistemas de Gestión de Seguridad de la Información.
- **Fortinet NSE / Cisco CCNA Security**: Seguridad en redes y dispositivos perimetrales.

Como también, se promueve la formación continua del personal mediante capacitaciones, actualizaciones tecnológicas y participación en seminarios o talleres especializados.

10. Gestión de respuesta a incidentes

En Security Tech Solutions S.A.S consideramos la gestión de respuesta a incidentes como un pilar fundamental dentro de nuestros servicios de ciberseguridad; este proceso nos permite identificar, analizar, contener y mitigar cualquier evento que pueda afectar la seguridad de la información.

Nuestro objetivo es actuar de manera rápida y coordinada para minimizar el impacto de los incidentes (**ISO, 2021; MinTIC, 2022**). En la operación de cada cliente, garantizando la continuidad de sus servicios y la protección de sus activos digitales; contamos con procedimientos definidos y personal especializado que supervisa cada fase del proceso, asegurando una respuesta eficiente ante cualquier amenaza o vulnerabilidad detectada **(ITSM.tools, 2025; Raza, 2024**).

10.1 Etapas del proceso de respuesta

- **Identificación:** Detección de eventos sospechosos o anómalos mediante sistemas de monitoreo y plataformas SIEM.
- **Análisis:** Clasificación del incidente según su origen, tipo, impacto y alcance.
- **Contención:** Aislamiento de los sistemas o dispositivos comprometidos para evitar la propagación del ataque.
- **Erradicación:** Eliminación de la amenaza y reparación de las vulnerabilidades explotadas.
- **Recuperación:** Restauración segura de los servicios afectados y verificación de la integridad de los sistemas.
- **Lecciones aprendidas:** Documentación del incidente, análisis post mortem y aplicación de mejoras preventivas.

10.2 Herramientas y metodologías aplicadas

- Trabajamos con una marca que nos permite tener toda la gestión centralizada en la nube, la cual no permite una visibilidad y con relación en eventos de ciberseguridad para el respecto al tema de seguridad perimetral, seguridad *endpoints* y seguridad de correo electrónicos.
- Sistemas IDS/IPS para detección y prevención de intrusiones.
- Planes de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP).
- Protocolos de notificación y gestión de incidentes conforme a la **Ley 1581 de 2012** sobre protección de datos personales **(Gobierno de Colombia, 2012)** y estándares internacionales como ISO 27035 y NIST SP 800-61.

10.3 Objetivo general

- Nuestro compromiso es responder de forma efectiva, de acuerdo a las buenas prácticas de ciberseguridad; coordinando y documentado debidamente ante cualquier incidente de seguridad, procurando reducir al máximo su impacto operativo, legal y reputacional sobre la organización.

11. Protección de datos

Security Tech Solutions S.A.S garantiza la protección de la información que gestiona dentro de los servicios de ciberseguridad, cumpliendo con los principios de confidencialidad, integridad y disponibilidad de los datos; de acuerdo con las normas internacionales establecidas por la **ISO/IEC 27001:2022** y la legislación colombiana vigente sobre protección de datos personales (**ISO, 2021; Gobierno de Colombia, 2012**)

Toda la información tratada en nombre de cuál sea el cliente se considera confidencial y será utilizada exclusivamente para los fines establecidos en el contrato de prestación de servicios (**MinTIC, 2024**).

Figura 3. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

La empresa aplica controles técnicos y administrativos para evitar el acceso no autorizado, la pérdida o la alteración de la información entre ellos se incluyen:

- Políticas de cifrado, autenticación de múltiples factores, segmentación de red y copias de seguridad automatizadas (**Ambit, 2020; ISO, 2021**).

- Política de control de accesos se asignará de acuerdo con las funciones y responsabilidades de cada colaborador, se aplicarán mecanismos de autenticación segura, contraseñas robustas y validaciones periódicas para garantizar que

únicamente los usuarios autorizados ingresen a los sistemas mediante VPN (**Ministerio TIC, 2022; MinTIC, 2024**).

- Política de respaldo y recuperación de copias de seguridad y configuraciones del firewall; contarán con copias de seguridad automáticas y verificadas de forma periódica, los respaldos se almacenarán en entornos seguros, tanto locales como en la nube, y se realizarán pruebas de recuperación para asegurar disponibilidad ante cualquier incidente (**ISO, 2021; MinTIC, 2024**).

- Política de notificación de incidentes de seguridad, todo evento que afecte la seguridad de la información deberá reportarse inmediatamente al área de soporte o ciberseguridad, se documentará el incidente, las acciones tomadas y las medidas preventivas implementadas (**Gobierno de Colombia, 2012; Ministerio TIC, 2022**).

- Política de uso responsable de los recursos tecnológicos, los equipos, redes, correos institucionales y demás herramientas tecnológicas deben utilizarse exclusivamente para fines laborales, queda prohibido el uso de software no autorizado o prácticas que comprometan la seguridad de la información (**MinTIC, 2024; ISO, 2021**.

Además, la empresa Security Tech Solutions S.A.S cumple con la Ley 1581 de 2012 y el Decreto 1377 de 2013, que regulan la protección de datos personales en Colombia **(Gobierno de Colombia, 2012)**, asegurando el manejo responsable de la información tanto de los usuarios como de los colaboradores; cualquier incidente relacionado con la seguridad de los datos será comunicado de manera inmediata a la entidad contratante y se gestionará conforme a los protocolos de respuesta establecidos en el acuerdo de servicio.

12. Normatividad vigente legal en la tercerización de servicios de ciberseguridad.

Los servicios de ciberseguridad prestados por la empresa Security Tech Solutions S.A.S se desarrollan bajo el cumplimiento de las normas nacionales e internacionales aplicables al sector tecnológico.

En el ámbito colombiano e internacional, se da cumplimiento a las disposiciones de:

Normatividad Colombiana

- **Ley 1581 de 2012** – Regula la **protección de datos personales (Gobierno de Colombia, 2012)**, estableciendo principios, derechos y procedimientos para el tratamiento responsable de la información.

- **Decreto 1377 de 2013** – Reglamenta parcialmente la Ley 1581, precisando el manejo del consentimiento y las obligaciones de las entidades que tratan datos personales.

- **Ley 1273 de 2009** – Modifica el código cenal e incorpora delitos informáticos, sancionando el acceso no autorizado, la alteración o el uso indebido de datos.

- **Ley 1266 de 2008** – Regula el manejo de información financiera, crediticia y comercial.

- **Decreto 620 de 2020** – Define los lineamientos para la implementación de la Política nacional de confianza y seguridad digital en entidades públicas.

- **Circular Externa 007 de 2018** Superintendencia de industria y comercio – establece directrices sobre seguridad y reporte de incidentes en el tratamiento de datos personales.

- **Ley 1341 de 2009** (Modificada por la Ley 1978 de 2019) – crea el marco general de las tecnologías de la Información y las comunicaciones en Colombia, fomentando la protección de los usuarios digitales.

- Política Nacional de Confianza y Seguridad Digital – **MinTIC (2021**)

A nivel internacional, la empresa adopta buenas prácticas de los estándares **ISO/IEC 27001:2022** e **ISO/IEC 20000-1:2018**, orientadas a fortalecer la gestión de la seguridad de la información y la calidad en los servicios TI **(International Organization for Standardization [ISO], 2021)**.

Estas normas permiten establecer controles internos, acuerdos de nivel de servicio (SLA) **(Raza, 2024)** y auditorías periódicas que garantizan la transparencia y la continuidad operativa dentro del modelo de outsourcing tecnológico.

Normas Internacionales y Estándares Técnicos

- **ISO/IEC 27001:2022** – establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) **(**International Organization for Standardization **[ISO], 2021)**, aplicable a cualquier organización que maneje información sensible.

- **ISO/IEC 20000-1:2018** – define los lineamientos para la gestión de servicios de TI, asegurando la calidad, continuidad y mejora de los procesos tecnológicos.

- **ISO/IEC 27002:2022** –ofrece controles prácticos y directrices complementarias para implementar las políticas del SGSI.

- **NIST SP 800-53 Rev. 5** – publicación del Instituto Nacional de estándares y tecnología de EE. UU., que proporciona un marco de referencia para la protección de sistemas de información federales y privados.

- **Reglamento General de Protección de Datos (GDPR) – Unión Europea (2018)** – marco internacional que regula la protección de datos personales y es referente para contratos internacionales de outsourcing.

13. Exclusiones

En todo servicio de outsourcing tecnológico es importante dejar claramente definidos los aspectos que no hacen parte del alcance del contrato; por tal motivo nuestra empresa nos permitimos comunicarles y hacerles publico dichas exclusiones para establecer límites precisos, evitar interpretaciones erróneas y garantizar que tanto nosotros como proveedor como el cliente comprenda sus responsabilidades (**MinTIC, 2024; ISO, 2021**). Las exclusiones detallan aquellas situaciones o tareas que no están cubiertas dentro de la propuesta de gestión de ciberseguridad; el propósito es mantener la transparencia en la prestación del servicio y asegurar que los recursos se destinen correctamente a las actividades contempladas en el acuerdo (**Ministerio TIC, 2022; Ambit, 2020**).

El presente servicio no cubre las siguientes situaciones:

- No asumimos responsabilidad por los segmentos de red, equipos de cómputo o buzones de correo electrónico que no hayan sido incluidos en el acta de reconocimiento establecida al inicio del contrato. De igual forma, no se considerarán dentro del alcance los equipos adquiridos posteriormente y que no se hayan reportado, los buzones creados y no reportados o configuraciones de red que no se reportaron posterior a su configuración (**ISO, 2021**).

- No se cubrirán daños ocasionados por el uso inadecuado de los equipos tipo firewall, por condiciones inadecuadas del entorno donde se encuentren instalados, como humedad, sobrecalentamiento, exceso de polvo, variaciones eléctricas (**Sophos, 2025**).

- No se cubrirán daños ocasionados o afectaciones a las operaciones por acceso no restringidos a los firewalls (**Navarro, 2024**).

- No se consideran dentro del servicio los incidentes provocados por cortes de energía, desastres naturales o fallas externas que afecten la operación de la infraestructura tecnológica (**Ministerio TIC, 2022**).

- Quedan excluidas las instalaciones o el uso de programas sin licencia o de procedencia no verificada que puedan poner en riesgo la seguridad de los equipos de punto final (**Gobierno de Colombia, 2012; ISO, 2021**).

- No se cubrirán incidentes o fallas en equipos que ya no cuenten con soporte del fabricante o sistemas operativos obsoletos, estos deberán contar con una licencia y ser reportado con soporte extendido (**MinTIC, 2024**).
- No se asume responsabilidad por modificaciones, configuraciones o intervenciones efectuadas por personal ajeno al equipo técnico autorizado (**Navarro, 2024**).

- Quedan fuera de la cobertura los incidentes ocasionados por accesos indebidos, uso personal de recursos institucionales o prácticas contrarias a las políticas de seguridad (**Ambit, 2020**).

- No se incluye la atención de problemas causados por operadores de internet, telefonía, servicios en la nube u otros terceros que afecten la conectividad o el desempeño del sistema (**ITSM.tools, 2025**).

- Se excluyen los incidentes provocados por la falta de reporte oportuno, el incumplimiento de políticas de seguridad o la manipulación no autorizada de dispositivos perimetrales (**ISO, 2021; MinTIC, 2024**).

14. Conclusiones

La gestión de la ciberseguridad en servicios tercerizados representa un desafío estratégico que exige la integración equilibrada de tecnología, procesos y talento humano (**Navarro, 2024**). A lo largo de este trabajo se evidenció que una planificación adecuada permite a las organizaciones mantener el control sobre su información, aun cuando los servicios de seguridad son prestados por un tercero (**MinTIC, 2024**).

El análisis y mapeo de la infraestructura tecnológica, junto con la correcta gestión de vulnerabilidades y la adopción de soluciones avanzadas como XDR, demostraron ser pilares fundamentales para reducir la superficie de ataque y responder de manera efectiva ante incidentes (**Sophos, 2025**). Asimismo, los acuerdos de nivel de servicio (ANS) se consolidan como una herramienta esencial para garantizar la transparencia, la calidad y la continuidad operativa entre proveedor y cliente (**Raza, 2024**).

El cumplimiento de la normatividad vigente, tanto nacional como internacional, fortalece la confianza digital y asegura que el tratamiento de los datos personales se realice bajo principios de confidencialidad, integridad y disponibilidad (**Gobierno de Colombia, 2012; ISO, 2021; MinTIC, 2024**). Estos marcos legales y técnicos constituyen la base para un modelo de ciberseguridad sostenible y adaptable a los entornos empresariales actuales (**Ambit, 2020; Ministerio TIC, 2022**).

En conclusión, la tercerización de servicios tecnológicos, cuando se gestiona con estándares adecuados y una supervisión constante, no solo optimiza recursos y mejora la eficiencia operativa, sino que también eleva el nivel de protección frente a las amenazas cibernéticas emergentes (**ISO, 2021; ITSM. tools, 2025**). Este trabajo evidencia que la combinación de

buenas prácticas, normativas y capacitación continua permite construir un entorno digital más seguro y resiliente para las organizaciones (**Navarro, 2024; Sophos, 2025**).

15. REFERENCIAS

- Ambit. (2020, marzo 25). *Normas ISO: qué son y cuáles son las más importantes.* Ambit Iberia. https://www.ambit-iberia.com/blog/normas-iso.-qu%C3%A9-son-y-cu%C3%A1les-son-las-m%C3%A1s-importantes

- Gobierno de Colombia. (2012, octubre 17). *Ley 1581 de 2012 - Protección de datos personales.* Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

- Gobierno de Colombia – Ministerio de Ambiente y Desarrollo Sostenible. (2012). *Política de protección de datos personales.* https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

- International Organization for Standardization (ISO). (2021). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection.* https://www.iso.org/standard/27001.html

- ITSM.tools. (2025, enero 6). *ITIL 4 explained: key principles and benefits.* https://itsm.tools/itil-4-explained/

- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2024, junio 25). *Políticas de privacidad y condiciones de uso.* https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

- Navarro, A. (2024, mayo 3). *Mejores prácticas y estrategias de gestión de servicios de TI.* Innevo. https://innevo.com/blog/mejores-practicas-estrategias-de-gestion-de-servicios-de-ti

- Raza, M. (2024, marzo 15). *SLA template examples.* HelixOps Blog. https://blogs.helixops.ai/sla-template-examples/

- Sophos. (2025). *Endpoint security products and solutions.* https://www.sophos.com/en-us/products/endpoint-security

- Ministerio TIC. (2022, julio 18). *Decreto 1227 de 2022 – Normograma de políticas de seguridad digital.* Normograma MinTIC. https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_1227_2022.htm