El "Punto Ciego" de los Navegadores en Soluciones Logísticas Interoceánicas (SLI)

Corporación Universitaria Remington.
Facultad de Ingeniería
Ingeniería de Sistemas
Seminario en Gestión de Ciberseguridad en las Organizaciones

Richard Stiven Ramírez Leguizamón
Tutor: Jorge Leonardo Ramirez Restrepo
Seminario
Año 2026

Tabla de Contenidos

Lista de Tablas

Lista de Ilustraciones

Resumen

Esta investigación tiene como propósito tener un análisis de ciberseguridad para la empresa Soluciones Logísticas Interoceánicas (SLI). SLI es una compañía del sector logístico y de transporte de mediano tamaño. El objetivo principal es analizar y evitar riesgos que se producen en el uso descontrolado de extensiones de navegador en el ambiente operativo-funcional, es un fenómeno denominado como Shadow IT que pone en un riesgo inminente en la integridad de la cadena de suministros.

Durante el proceso, se aplicó un enfoque de ciberseguridad organizacional que permite identificar los activos críticos de información, destacando el acceso a portales aduaneros y manifiestos de carga y adicional, se realizó un análisis de las amenazas y vulnerabilidades que puede tener dichos procesos, centrándonos en el riesgo de filtración de datos, pérdida de información, robo de datos como de identidad digital mediante extensiones de terceros con permisos privilegiados o excesivos.

En este documento, se evidencia como una debilidad en los procesos de gestión de software y falta de control técnico sobre los navegadores, puede afectar y ocasionar incidentes con un alto impacto financiero y operativo. Como resultado principal, se propone un plan de ejecución con controles técnicos, como una administración centralizada en políticas de navegación y en la implementación de listas blancas, junto con un programa de concientización para el personal. Dichos resultados demuestran que la seguridad de la información en SLI no solo depende del personal de seguridad y de firewalls perimetrales, sino de una gobernanza

estricta sobre las herramientas implementadas, así, permitiendo una continuidad del negocio y la confianza de los socios comerciales en un entorno digital cada vez más hostil.

Palabras clave

Ciberseguridad Organizacional: Representa el marco global del informe y el enfoque sistémico aplicado a SLI.

Gestión de Riesgos: El núcleo del seminario, centrado en identificar, evaluar y mitigar las amenazas del entorno logístico.

Shadow IT: Concepto clave para describir el uso de extensiones y software no autorizado por el departamento de TI.

Activos de Información: Define los elementos de valor que buscamos proteger, como datos aduaneros y financieros.

Políticas de Seguridad: El conjunto de reglas y controles propuestos para regular el uso de herramientas digitales en la empresa.

Marco conceptual y contextual

1. **Marco Conceptual**

Debemos entender en este informe que la seguridad se fundamenta en la ciberseguridad Organizacional, no solo como una implementación de barreras técnicas, sino como un sistema de gestión que protege y salvaguarda los objetivos del negocio Soluciones Logísticas Interoceánicas (SLI). "La gestión de riesgos de seguridad de la información es un proceso sistemático que permite a la organización identificar debilidades y aplicar controles proporcionales a la importancia de los activos" (Organización Internacional de Normalización [ISO], 2022).

En este entorno, los activos de información son el núcleo de más importancia y de mucho valor (como los manifiestos de carga y bases de datos de clientes, proveedores, etc..), cualquier cometido a su confidencialidad, integridad o disponibilidad representa un posible riesgo directo.

Este análisis se basa en la tríada fundamental:

- Vulnerabilidades: Debilidades propias de la infraestructura o procesos, como el uso de navegadores no administrados.
- Amenazas: Factores externos o internos, como el malware embebido en extensiones de terceros, que pueden explotar dichas debilidades.
- Riesgos: La probabilidad de que una amenaza explote una vulnerabilidad, resultando en impactos financieros o legales.

Para minimizar dichos riesgos, se proponen algunos controles de seguridad que se rigen en las prácticas de la Norma ISO 27001, en el apartado del control de software en equipos de usuarios y gestión de accesos. Así mismo, en el contexto del país colombiano, se intentará alinear con la ley 1581 cuyo valor es la protección de datos personales, ya que el manejo de información de

clientes y de proveedores, en el cúal exigen un tratamiento de datos seguros para el tema de sanciones legales y garantizar la privacidad de seguridad.

2. Marco Contextual

Soluciones Logísticas Interoceánicas (SLI) es una empresa colombiana con sede operativa central en Cúcuta, Norte de Santander, aprovecha su posición estratégica para un comercio binacional. Su principal actividad económica se basa en el transporte de carga por medio de carretera y gestión aduanera internacional. Debido a que SLI opera en la frontera y maneja datos de terceros, el tratamiento de la información debe alinearse con la normativa nacional, la cual busca "garantizar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas" (Congreso de la República de Colombia, 2012).

- Estructura y procesos: SLI cuenta con varios departamentos, como lo son el departamento de operaciones aduaneras, área logística y equipo administrativo-contable. Su ejecución más crítica es nacionalizar su mercancía, con cúal requiere que su personal esté un 80% de su jornada laboral interactuando con plataformas y entidades gubernamentales como la DIAN y VUCE, como también portales bancarios a través de consumo y navegadores web
- Entorno tecnológico: La Organización está en un proceso operativo de modelo híbrido, esto permite que los equipos, se interconecten de manera local mediante la red local del proveedor, pero también se conecten a servicios totalmente alojados en la nube (SaaS).

- Situación actual de seguridad: Actualmente, SLI carece de un control en el inventario de software de navegador. En el análisis se detectó que los empleados, instalan extensiones de diversas fuentes y páginas para “facilitar” tareas como la conversión de divisas, traducción de contratos, entre otras. Esta práctica se ha hecho sin supervisión y/o aprobación del área de IT, por lo que se crea una brecha de seguridad (Shadow IT) bastante significativa. Con este caso, se genera una necesidad urgente de formalizar una política que permita administrar el uso de herramientas digitales para prevenir incidentes que puedan afectar el flujo y operatividad de la organización, generando así pérdida de integridad de datos y funcionalidad.

Desarrollo e implementación del aprendizaje

Aquí vamos a poder evaluar de manera detallada la metodología aplicada para gestionar los riesgos derivados de las extensiones de navegador en SLI, integrando la identificación de activos, análisis y propuestas de controles antes las vulnerabilidades

1. Identificación de Activos de Información

1.1. ¿Qué son Activos de Información?

Los activos de información son todos aquellos elementos que procesan, contienen o transportan información que tienen un valor para la organización. En este campo de la ciberseguridad, un activo no solamente es algo físico (Como un equipo de cómputo) sino todo aquel conocimiento y todos los datos que permiten que la organización funcione de la mejor manera. Según la Guía de Gestión de Riesgos del Ministerio de Tecnologías de la Información y las Comunicaciones (2022), un activo de información es aquel elemento que tiene valor para la entidad y cuya pérdida o compromiso afecta directamente la prestación del servicio.

1.2. Clasificación de los activos

Dentro de la organización no toda la información es igual, por lo que se puede clasificar mediante su naturaleza:

- Información Digital: Bases de datos, archivos PDF, correos electrónicos, códigos fuente o registros de configuración.
- Activos físicos (Hardware): Servidores, Portátiles, Equipos de mesa, tablets, discos duros y memorias USB donde se almacena la información
- Servicios de Software: Aplicaciones (ERP, CRM), plataformas en la nube (SaaS) y servicios de red que permiten el flujo de los datos.
- Recurso Humano: Es el conocimiento especializado que poseen los empleados respecto a la organización.
- Activos Intangibles: La reputación de la marca y la propiedad intelectual

La identificación de los activos es el primer paso para poder tener una estrategia de seguridad (Como la ISO 27001), ya que si sabes qué tienes, no vas a poder protegerlo. Al identificarlos, permite saber qué es lo que es más valioso (Criticidad), se entiende dónde están las debilidades y se asigna el presupuesto para la seguridad de forma eficiente.

1.3. Identificación de Activos de Información

En base en toda la información obtenida en este documento, se determinaron los activos que interactúan directamente con los navegadores web en las estaciones de trabajo del área operativa y administrativa.

Tabla 1 *Activos de Información*

Activo	Tipo	Descripción	Criticidad

Credenciales VUCE/DIAN	Datos	Accesos a la ventanilla Única de Comercio exterior y DIAN	Muy Alta
Manifiestos de Carga	Información	Documentación digital con detalles de clientes y mercancía	Alta
Tokens de Sesión Bancaria	Datos	Cookies y sesiones activas en portales de banca corporativa	Muy Alta
Historial de Navegación	Información	Registro de movimientos logísticos y consultas de rutas	Media
Servidor de Datos Local	Hardware	Centralización de almacenamiento de la operación	Alta
Certificados de Firma Digital	Software	Trámites legales	Muy Alta
Rutas de Transporte	Datos	Documentación digital con detalles de rutas de transporte y almacenamiento de productos	Alta
Agentes Aduaneros	Humano	Poseen el conocimiento crítico de los trámites	Media
Equipos de computo	Hardware	Equipos suministrados a los usuarios para su manejo de información y gestión	Alta
Servicio de correo Electrónico Corporativo	Lógico/Datos	Plataforma de comunicación oficial y almacenamiento de históricos de negociación	Muy Alta

2. Análisis de Amenazas y Vulnerabilidades

En esta sección, el análisis se centró en cómo las extensiones de navegador interactúan directa e indirectamente como un puente para explotar debilidades en la organización. El fenómeno del Shadow IT mediante extensiones representa un riesgo latente, ya que, como indica el SANS Institute (2023), muchas de estas herramientas operan fuera del perímetro de seguridad convencional, permitiendo la interceptación de datos directamente desde la interfaz del usuario

- Amenaza**:** Malware de exfiltración de datos (Spyware) camuflado en extensiones con un índice de “productividad”.

- Vulnerabilidad Técnica: Navegadores Google Chrome con permisos de instalación abiertos para el usuario estándar y falta de políticas de grupo (GPO) para restringir el Web Store
- Vulnerabilidad Humana**:** Bajo conocimiento técnico del personal sobre los permisos de “Lectura y modificación de datos en los sitios web visitados”.

3. Matriz de Evaluación de Riesgos para extensiones del Navegador

Utilizando una escala de 1 a 5 para Probabilidad e Impacto, se evaluó el escenario de riesgo principal. El riesgo de las extensiones maliciosas se clasifica como una vulnerabilidad crítica de aplicaciones web, alineándose con los hallazgos de la Fundación OWASP (2021), que destaca las fallas en el control de acceso y la integridad del software como amenazas de alto impacto

Tabla 2 *Matriz de Riesgos*

Escenario de Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Robo de credenciales aduaneras vía extensión maliciosa	Alta (4)	Alto (5)	Crítico (20)
Inyección de publicidad maliciosa (Adware) que ralentiza el ERP.	Alta (5)	Bajo (2)	Medio (10)
Fuga de bases de datos de clientes mediante extensiones de "lectura de PDF"	Media (3)	Alto (4)	Alto (12)

4. Propuesta de Controles y Políticas de Seguridad

Basado en la información recolectada de manera hipotética, se diseñó un plan de mitigación basado en tres niveles de estructuración.

4.1. Controles Técnicos (Implementación de GPO)

Se propone implementar una plantilla de administración para Google Chrome que ejecuten las siguientes acciones)

- Lista de Bloqueo de instalación de Extensiones: Bloqueo total de todas las extensiones (usando el valor *).
- Lista Blanca de Instalación de Extensiones: Habilitación exclusiva de extensiones verificadas por el CISO (director de seguridad de la información).
- Configuración de Extensiones: Se forza la instalación de herramientas de seguridad necesarias sin intervención del usuario (Endpoint Verification).

4.3. Gestión de Incidentes

Se establece un protocolo de respuesta inmediata en caso de detectar una extensión maliciosa mediante MITM.

- Identificación: Al detectarse tráfico anómalo desde una extensión donde hay exfiltración de credenciales aduaneras vía MITM, se procede a ejecutar los controles de seguridad propuestos.
- Contención: Deshabilitación remota del perfil del usuario en el navegador y desconexión de la sesión de red.
- Notificación externa: Se informa de manera inmediata con la DIAN y VUCE para solicitar el bloqueo preventivo del usuario de aduanas comprometido, evitando que se firmen manifiestos de carga fraudulentos.
- Erradicación: Eliminación de la extensión y escaneo de malware en el equipo
- Recuperación: Cambio obligatorio de contraseñas que fueron parcialmente expuestas mediante la persistencia de la extensión.
- Análisis de Impacto: Se realiza revisión de los últimos logs de actividad en el portal bancario para verificar si hubo internos de transferencias no autorizadas.
- Continuidad de la operación: Se activa una estación de trabajo de contingencia (limpia) para asegurar la disponibilidad en el despacho de camiones en la frontera y no se detenga por un periodo de tiempo considerable.

4.4. Cultura Organizacional y Concientización

En base al peligro detectado mediante las extensiones de navegador, se diseñó una campaña de sensibilización denominada NSAC (Navegación Segura, Asegura la Carga)

- Talleres prácticos sobre cómo identificar los datos y permisos de una aplicación web.
- Infografías en puntos estratégicos de trabajo sobre el peligro de las herramientas “gratuitas” de internet (Como puntos de impresoras, pasillos, carteles informativos, etc…)
- Desde la alta gerencia General de SLI se emitirá un comunicado oficial de seguridad donde se establece que la ciberseguridad es un pilar estratégico para la competitividad en el sector logístico. La dirección de alta gerencia asignará un presupuesto anual para las herramientas de auditoría y será la encargada de aprobar sanciones por incumplimiento de las políticas de seguridad
- Se propondrá unas métricas de efectividad (KPIs) donde se evaluará una tasa de incidencia que permita determinar el porcentaje de estaciones de trabajo con software no autorizado en auditorías; tendrá la meta del menos del 5%.
- En los resultados obtenidos en la prueba de phishing simulado después de los talleres trimestrales, se evaluará el nivel de concientización, este deberá tener una meta mayor al 80% de aprobación.

4.5. Gobernanza y Administración de Controles

La administración de las listas blancas (allowlists) de extensiones será responsable de manera exclusiva el área de Sistemas (IT) a través de consolas de administración de Google (GPO).

- Validación de cumplimiento: Se ejecutará un script de auditoría automatizado cada 15 días que permita generar un reporte de discrepancia entre las extensiones instaladas y la política autorizada.

- Gestión de Incidencias: En caso de que se presente un intento de vulnerar las políticas y restricciones mediante navegadores portables o perfiles personales, se tomará el caso para ser escalado a la dirección de operaciones donde se revocará de manera temporal los accesos a portales críticos dentro de sus labores hasta completar una re-inducción respecto a las políticas de seguridad implementadas en la organización.

5. Evidencia de Aplicación (Simulacro Hipotético)

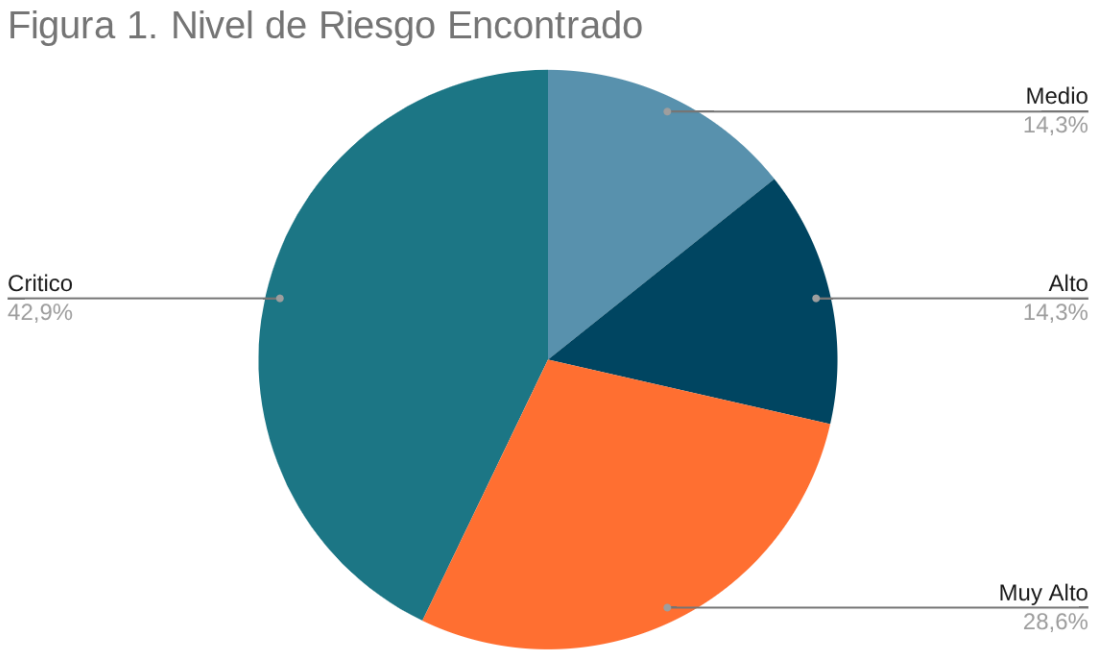
Como parte del ejercicio, se realizó un simulacro de auditoría en una estación de trabajo del área de logística de SLI, encontrando 7 extensiones instaladas de las cuales 3 tenían permisos de acceso total a datos de portales financieros. Tras la aplicación de los controles propuestos, el número de extensiones no autorizadas se redujo a cero, centralizando la administración en el departamento de TI.

Tabla 3 *Extensiones Peligrosas Encontradas*

Extensión	**Función Declarada**	**Permiso de Riesgo Detectado**	**Clasificación del Riesgo**
PDF Converter & Editor Free	Edición de documentos	Leer y modificar todos los datos	Alto (Exfiltración)
Flash Theme Custom	Personalización visual	Acceso al historial de navegación	Medio (Privacidad)
Web Translator Pro	Traducción de sitios	Leer datos en todos los sitios Web (Paginas de proveedores, clientes, etc…)	Muy Alto (Espionaje)

VPN Proxy Unlim	Navegación anónima	Modificar configuración de red/proxy	Crítico (MITM)
Auto Video Downloader	Descarga de videos (Tutoriales, publicidad)	Permisos de lectura, inyección de código en páginas, captura de cookies	Crítico (Malware y Espionaje)
Coupon Finder /Shopping Assistant	Compras personales	Monitoreo de navegación en busca de “ofertas”	Muy Alto (Espionaje)
Screen Recorder & Screenshot Tool	Captura de pantalla	Captura de información(Tokens de seguridad, contraseñas, BD)	Crítico (Exfiltración)

Ilustración 1 *Nivel de Riesgo Encontrado*



Aunque las extensiones se ven útiles, podemos ver cómo es un riesgo ya que el desarrollador desconocido pide acceso e información con la función que realizan, esto refuerza la necesidad de utilizar listas blancas gestionadas por el área de IT.

Conclusiones

En este análisis basado en la organización Soluciones Logísticas Interoceánicas (SLI) permite concluir que la seguridad no es un juego, no es un estado estático en el que solo interviene el área de IT, sino un proceso de gestión continua y compartida. En la identificación de activos **(Ver tabla 1)**, demuestra que la información crítica se establece en gran medida en el entorno web, lo que convierte al navegador, en un activo tecnológico más vulnerable y extrañamente, el menos supervisado.

Se determinó que faltaba una política de gobernanza sobre el Shadow IT en base a las extensiones, elevaba el nivel de riesgo de forma "crítica", como se observa en la identificación de riesgos **(Ver tabla 2)**. La explotación de vulnerabilidades no sólo comprometería la privacidad de los datos, sino que influye en la interrupción de la operación logística en la frontera, generando retrasos y pérdidas financieras directas. La implementación de controles preventivos, como las políticas de administración centralizada, medidas eficientes y de menor costo que reduce los ataques en este contexto.

Recomendaciones

1. Automatización del control: Se recomienda que el departamento de IT de SLI adopte medidas de manera urgente e inmediata las políticas de grupo (GPO) sugeridas en el apartado de la propuesta de controles y políticas de seguridad, para restringir de manera inmediata la instalación de software no autorizado en los navegadores corporativos
2. Programa de educación continua: Se recomienda establecer sesiones periódicas, en lo posible en un margen máximo de 3 meses (Trimestral) en el que se capacite al personal en temas de ciberseguridad higiénica, enfocadas en el reconocimiento de permisos de aplicaciones y la importancia de usar únicamente herramientas aprobadas por el área de IT.

3. Auditorías periódicas: Realizar un análisis semestral de los perfiles de usuario en las estaciones de trabajo para asegurar que el inventario de activos de software se mantenga alineado conforme a las políticas de seguridad y así, tener continuidad de la operación.

Referencias

DIAN. (2024). Manual de Usuario: Sistema Informático Electrónico de Aduanas y servicios en línea. Ministerio de Hacienda y Crédito Público. https://www.dian.gov.co

Congreso de la República de Colombia. (2012, 17 de octubre). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587.

Google Chrome Enterprise. (2024). Administrar extensiones en el entorno empresarial. Ayuda de Chrome Enterprise. https://support.google.com/chrome/a/answer/6304825

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2022). Guía de Gestión de Riesgos de Seguridad de la Información: Modelo de Seguridad y Privacidad de la Información (MSPI). Gobierno de Colombia.

Organización Internacional de Normalización (ISO). (2022). Sistemas de gestión de la seguridad de la información — Requisitos (ISO/IEC 27001:2022). Ginebra, Suiza: Secretaría Central de ISO.

OWASP Foundation. (2021). OWASP Top 10:2021 - Los diez riesgos de seguridad más críticos en aplicaciones web. https://owasp.org/www-project-top-ten/

SANS Institute. (2023). Controlling Shadow IT: A Guide to Secure Browser Extensions. SANS Reading Room. https://www.sans.org/white-papers/

Almeida, F., & Santos, J. (2023). The challenges and risks of Shadow IT in corporate environments: A cybersecurity perspective. Journal of Cybersecurity and Privacy, 3(2), 145-159. https://doi.org/10.3390/jcp3020010