PRESENTADO POR:

JOSE ELIAS IBAÑEZ DAGUER

HENRY DAVID MACEA CABALLERO

ANDRES SANTIAGO RAMOS

INFORME TECNICO
Ingeniería de sistemas

PARA: ING. JORGE MAURICIO SEPULVEDA CASTAÑO

SEMINARIO DE GRADO

OUTSOURCING TI

DICIEMBRE 2025

SERVICIO DE CIBERSEGURIDAD BAJO MODELO DE OUTSOURCING OASIS ALIMENTOS S.A.S.

Dedicatoria

La orientación proporcionada por nuestras familias, cuyo apoyo y motivación ayudaron en completar este proceso académico y profesional, es apreciada en este trabajo. Cada paso del camino, su confianza y paciencia han sido esenciales.

Agradecimientos

Nuestro reconocimiento va a la Corporación Universitaria Remington, a los profesores del programa de Ingeniería de Sistemas y al tutor asignado, por la orientación, acompañamiento y exigencia académica.

A Oasis Alimentos S.A.S. por otorgar el estudio técnico del servicio de ciberseguridad y por proporcionar información relevante para la elaboración de este informe.

Tabla de contenido

1. RESUMEN

Este informe técnico tiene como finalidad analizar la puesta en marcha de un servicio de ciberseguridad de tipo outsourcing para una empresa del sector alimentario, en este caso para la empresa Oasis Alimentos S.A.S. Esta empresa colombiana del sector de alimentos ha crecido, junto con su infraestructura tecnológica, y ha aumentado de esta manera su exposición a amenazas informáticas. La finalidad del informe técnico es determinar las necesidades de protección digital de la empresa, así como describir la adopción del servicio tercerizado administrado por un proveedor de seguridad informática (MSSP - Managed Security Service Provider).

El informe técnico describe el marco conceptual del outsourcing, de la ciberseguridad, de la gestión del riesgo, de los marcos normativos como ISO/IEC 27001, NIST Cybersecurity Framework, CIS Critical Security Controls y su aplicación práctica al contexto organizacional.

A continuación, se contextualiza el estado tecnológico de la empresa Oasis Alimentos S.A.S., donde se presentan problemáticas como un bajo nivel de madurez en cuanto a la seguridad, falta de un monitoreo centralizado, políticas incompletas, carencia de respaldos estructurados, y amenazas a las que están expuestas como el phishing, el malware y el ransomware.

Tal como se evidencia en el diagnóstico realizado, se detallan el proceso de escogencia, la contratación y la implementación del servicio tercerizado en seguridad, mostrando actividades como el inventario de los activos críticos, la evaluación de vulnerabilidades, la implementación del EDR, el refuerzo de políticas, la creación de planes para la respuesta a incidentes y la capacitación del personal. Finalmente se muestran los resultados y las conclusiones alcanzadas de acuerdo con el contenido del seminario de outsourcing y seguridad.

2. Palabras clave

Ciberseguridad; Outsourcing; Gestión de riesgos; Seguridad informática; MSSP.

3. INTRODUCCIÓN

La ciberseguridad se ha convertido en una necesidad en el modo de funcionamiento de cualquier tipo de organización, en especial de aquellas que tienen información en sistemas, datos y requieren protegerla. Junto a esto, el crecimiento y la sofisticación de los ataques cibernéticos como el ransomware, el phishing y el data leak han hecho que las organizaciones tengan que redefinir sus estrategias de la ciberseguridad. (Microsoft, 2023; NIST, 2023)

Vista la anterior reflexión, en este sentido, la ciberseguridad como servicio también es una opción válida y real para organizaciones que no tienen recursos, personal y conocimiento para afrontar el anterior riesgo. El presente informe relata el proceso que se realizó, el proceso técnico de ciberseguridad como servicio que se realizó en Oasis Alimentos S.A.S. Los pasos que se hicieron fueron un diagnóstico, la descripción del proceso de ciberseguridad como servicio, implementación y evaluación de los resultados obtenidos.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Se evaluará y documentará la puesta en práctica de un modelo de outsourcing en ciberseguridad que permita incrementar la protección tecnológica de la empresa Oasis Alimentos S.A.S.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar brechas y los riesgos de seguridad existentes en la organización.
- Analizar los servicios que ofrece el proveedor MSSP.
- Documentar las actividades que se ejecutan durante el proceso de la implementación.
- Evaluar los resultados que se obtienen una vez implantado el modelo.

5. METODOLOGÍA

El desarrollo del presente informe técnico se articula desde una metodología descriptiva–aplicada, configurándose mediante un ciclo formal de análisis, diseño,

implementación y evaluación del servicio de ciberseguridad externalizado. La metodología se desarrolló en las siguientes fases:

Fase 1. Análisis y revisión de referentes

Se llevó a cabo una revisión de la documentación relativa a estándares, marcos normativos y literatura especializada en relación a ciberseguridad y en tercerización; como principales referentes se consideraron ISO/IEC 27001, NIST Cybersecurity Framework y CIS Critical Security Controls. Esta fase sirvió para constituir la base conceptual que guía el análisis técnico del servicio.

Fase 2. Diagnóstico del estado inicial

Se realizó el diagnóstico de la situación de ciberseguridad de la empresa Oasis Alimentos S.A.S. realizando entrevistas semiestructuradas con el personal del área de TI, observación directa de la infraestructura tecnológica y recogida de la información técnica. En esta fase se definieron activos críticos, brechas de seguridad, riesgos prioritarios y nivel de la madurez inicial de la organización.

Fase 3. Planteamiento del modelo de outsourcing

A partir de la información recopilada y la bibliografía consultada, se determinaron los servicios de ciberseguridad a outsourciar, conformándolos con las funciones del NIST CSF y los controles del CIS. En esta fase también se llevó a cabo el seleccionamiento del proveedor MSSP y la determinación de las actuaciones a realizar.

Fase 4. Ejecución del servicio

Se realizaron las actividades técnicas especificadas, como la realización de las soluciones EDR, la modificación del firewall, el despliegue de SIEM, el reforzamiento de las políticas de seguridad, la automatización de las copias de seguridad y la capacitación de los usuarios finales.

Fase 5. Evaluación de los resultados

Finalmente, se llevó a cabo la evaluación comparativa del estado de la organización antes y después de la ejecución del servicio, mediante indicadores de reducción de alertas, disminución de los riesgos críticos y escalado del nivel de madurez de la ciberseguridad.

.

Este ciclo metodológico permitió formalizar la manera del desarrollo del informe y mostrar la aplicación práctica de los conocimientos adquiridos durante el seminario, en coherencia con un trabajo académico de manera cooperativa.

6. MARCO CONCEPTUAL Y CONTEXTUAL

Marco conceptual

La ciberseguridad es el conjunto de estrategias, procesos, tecnologías y prácticas que se utilizan para proteger los activos de información de las amenazas (internas y externas), buscando garantizar la confidencialidad, integridad y disponibilidad de la información. En la actualidad de las organizaciones, donde los procesos productivos y los administrativos se encuentran digitalizados, la ciberseguridad deja de ser un aspecto sólo técnico para convertirse en un eje estratégico del negocio.

El incremento sostenido de incidentes como ransomware, phishing, fuga de información o compromisos de la infraestructura crítica ha mostrado que es necesario adoptar modelos formales de gestión de la seguridad de la información. En este sentido, estándares de referencia como ISO/IEC 27001, el NIST Cybersecurity Framework (CSF) y los CIS Critical Security Controls son el sustrato conceptual y técnico que da pie a la elaboración del presente informe.

La norma ISO/IEC 27001 establece las directrices para el establecimiento, funcionamiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), posibilitando a las organizaciones que son capaces de identificar

riesgos, de definir controles y de poder dar la protección de la información de una manera sistemática. No obstante, en este trabajo no se implementa un SGSI completo; no obstante, se toma como referencia para la identificación de controles prioritarios y de buenas prácticas.

El marco hoy en día que es el NIST Cybersecurity Framework da pautas para un enfoque de su gestión basado en cinco funciones básicas de la ciberseguridad: identificar, proteger, detectar, responder y recuperar. Este marco permite considerar el proceso de evaluación del nivel de madurez en ciberseguridad, así como las mejoras que se van logrando como fruto de la implementación del servicio de ciberseguridad sufragado.

Los CIS Critical Security Controls aportan un conjunto de controles técnicos priorizados que sirven para complementar los marcos anteriores, su uso está orientado a reducir con rapidez los riesgos más habituales de una forma eficaz. Su uso es particularmente relevante en aquellos contextos donde se requieren mejorar las condiciones de seguridad de la organización en periodos de tiempo cortos y sin contar con eventuales recursos.

En este contexto el outsourcing en ciberseguridad se presenta como una estrategia organizativa destinada a subcontratar las reglas de gestión de las funciones especializadas que proporciona un proveedor externo con alta experticia técnica (Managed Security Service Provider - MSSP) el cual va a suponer tener monitoreos continuos, respuesta a incidentes y disposiciones con altas capacidades defensivas sin contar con el coste ni los tiempos que supone la puesta en marcha de un equipo interno especializado.

El objeto de estudio del presente informe es, por tanto, el análisis técnico de la implementación de un servicio de ciberseguridad bajo el modelo de outsourcing, evaluando su impacto en la reducción de riesgos, el fortalecimiento de controles y la mejora del nivel de madurez en seguridad de la información dentro de una organización

del sector alimentario.

Marco contextual

Oasis Alimentos S.A.S. es una empresa colombiana del sector de alimentos procesados, cuya operación depende, en cierta medida, de plataformas tecnológicas como sistemas ERP y facturación electrónica, bases de datos de la compañía, herramientas de comunicación digital, etc.

El crecimiento de la infraestructura tecnológica de la organización no fue acompañado en sus etapas iniciales de una estrategia formal de ciberseguridad. Antes de la puesta en marcha del servicio tercerizado se evidenciaban debilidades como la carencia de monitoreo continuo, políticas de seguridad incompletas, controles de acceso laxos, falta de soluciones de detección y respuesta de amenazas avanzadas y esquemas de copias de seguridad poco estructurados.

En este contexto, unido a la proliferación de amenazas concretas contra el sector empresarial colombiano, aparecieron necesidades urgentes de discutir alternativas para fortalecer la seguridad de la información, en el que el enfoque de ciberseguridad en outsourcing quedó como la solución más acorde con la capacidad operativa y económica de la organización, de forma que en su aplicación se elevaría la postura de seguridad y la exposición a incidentes críticos se reduciría.

6.1 CONCEPTOS CLAVE

Outsourcing: Estrategia utilizada por una organización que, con la intención de mejorar los resultados y optimizar los recursos, realiza procesos especializados en un tercero. En este proyecto, el outsourcing le permitió a Oasis Alimentos S.A.S. acceder a capacidades avanzadas de ciberseguridad sin crear su propio equipo interno.

ISO/IEC 27001: Estuvo adaptado en este proyecto y tomado como un elemento de referencia que le permite identificar controles prioritarios como la gestión de

accesos, la protección de los activos críticos, las copias de seguridad o la reacción ante incidentes, pero sin la necesidad de implementar un SGSI completo.

NIST Cybersecurity Framework: Guía práctica utilizada por el MSSP para organizar las actividades en las funciones de identificación, protección, detección, respuesta y recuperación, a la vez que permite evaluar el estado inicial y las mejoras que se van realizándose.

CIS Critical Security Controls: Utilizadas como lista de verificación técnica para priorizar unos controles considerados de rápida implementación como por ejemplo la existencia de inventario de activos, la protección contra malware, la autenticación multifactor o la concientización de usuarios.

MSSP: Proveedor de servicios de seguridad gestionada para realizar la monitorización continua, la gestión de incidentes y la mitigación del riesgo tecnológico.

6.2 CONTEXTO DE LA ORGANIZACIÓN: OASIS ALIMENTOS S.A.S.

Oasis Alimentos S.A.S. es una sociedad de origen colombiano, cuya actividad principal es la producción, distribución y comercialización de alimentos procesados, y para el cual depende de sistemas de información como ERP, facturación electrónica, bases de datos de clientes y proveedores, plataformas logísticas, etc.

Antes del outsourcing, la organización que se analizó tenía carencias en el monitoreo continuo de seguridad, soluciones EDR, políticas documentadas, gestión de accesos, análisis de vulnerabilidades, copias de seguridad.

7. MODELO DE OUTSOURCING APLICADO A LA CIBERSEGURIDAD

7.1 CARACTERÍSTICAS DEL SERVICIO TERCERIZADO

El MSSP que se eligió como proveedor ofrece,

- Monitoreo de seguridad 24/7.
- Gestión y respuesta a incidentes.

- Análisis periódico de vulnerabilidades.
- Implementación y administración de EDR.
- Gestión de firewall y seguridad perimetral.
- Apoyo básico en análisis forense digital.
- Acompañamiento en creación de políticas acordes a ISO/IEC 27001

8. DESARROLLO E IMPLEMENTACIÓN DEL SERVICIO

Se da cuentas de este proceso paso a paso para mostrar qué competencias aprendida con el diplomado/ seminario se aplicaron.

8.1 DIAGNÓSTICO INICIAL

En esta etapa se llevó a cabo un inventario de activos tecnológicos, su clasificación según criticidad, la identificación de brechas y la priorización de riesgos mediante la ejecución de entrevistas al personal de TI. En relación al nivel de madurez inicial, este se estimó en un 1,8 sobre 5, siendo valorado como bajo.

8.2 IMPLEMENTACIÓN DEL SERVICIO

Las principales actividades llevadas a cabo fueron:

- Instalación de solución EDR en 52 equipos.
- Configuración de firewall con reglas segmentadas.
- Implementación de monitoreo de eventos mediante SIEM.
- Definición de políticas de contraseñas y de accesos.
- Actualización de parches críticos.
- Automatización de copias de seguridad diarias.
- Pruebas internas de phishing.
- Capacitación a usuarios finales.
- Implementación de autenticación multifactor.
- Endurecimiento de servidores (hardening).

8.3 RESULTADOS OBTENIDOS

- Reducir en un 90 % en alertas por malware.
- Reducción en un 60 % de riesgos críticos.
- Mejora del nivel de madurez de 1,8 a 3,7 sobre 5.
- Cumple aproximadamente un 45 % de controles ISO/IEC 27001.

9. FIGURAS Y TABLAS

Tabla 1. Resultados antes y después del outsourcing

Control	Antes	Después
Malware detectado	86	8
Riesgos críticos	14	5
Nivel de madurez	1.8	3.7
Política de seguridad	No	Sí
Copias de seguridad	Parcial	Completa

10. CONCLUSIONES

El uso del modelo de outsourcing en ciberseguridad de Oasis Alimentos S.A.S. ha hecho que su postura de seguridad de la información mejorara notablemente, aún demostrando que el outsourcing de servicios especializados es una opción válida para organizaciones que no poseen un equipo interno. Con respecto al diagnóstico inicial y el servicio administrado, se alcanzó una reducción de los riesgos, un aumento del nivel de madurez en ciberseguridad y una mayor capacidad de detección y respuesta ante un eventual incidente.

Los resultados obtenidos demuestran que el uso de marcos de referencia como ISO/IEC 27001, el NIST Cybersecurity Framework y los CIS Critical Security Controls –incluso sin una implementación de un SGSI completo– permite estructurar acciones que mejoran la seguridad de la organización, la forma en que se plantea la metodología facilitó un diagnóstico del estado inicial, del diseño del servicio y de los beneficios que

se han conseguido.

Sin embargo, el modelo de outsourcing, además de tener sus ventajas, también tiene sus inconvenientes, siendo la dependencia del proveedor externo y la supervisión continua de los SLAs las más destacadas. De esta manera, el outsourcing no exime a la organización de su responsabilidad interna sobre la gestión dela seguridad de la información, sino que supone una implicación extrema por parte de la alta dirección y el personal implicado.

Como trabajo futuro se nos propone avanzar hacia una mayor alineación con la norma ISO/IEC 27001, hacer más intensa la gestión permanente de riesgos y ampliar los programas de concienciación y formación del personal, ya que ciberseguridad no es una acción única, sino un proceso permanente y estratégico para el interior de la organización.

11. REFERENCIAS

- ISO/IEC. (2022). ISO/IEC 27001:2022 Information security management systems. International Organization for Standardization.
- National Institute of Standards and Technology. (2023). Cybersecurity Framework (CSF) 2.0. NIST.
- Center for Internet Security. (2021). CIS Critical Security Controls (Version 8). CIS.
- Gartner. (2024). Market guide for managed security services. Gartner Research.
- Microsoft. (2023). Microsoft Security Intelligence Report. Microsoft.