TRABAJO DE GRADO

Opción Seminario-Diplomado.

informe final

Gestión de ciberseguridad en servicios tercerizados(outsourcing) en entornos organizacionales.

Corporación Universitaria Remington.

Nombre de la facultad: Ingenierías.

Nombre del programa académico: Ingeniería de Sistemas.

Karolain Martinez Nieto.
Andrea Nieto Castellano.

Opción de Trabajo de grado Seminario-Diplomado.

2026.

Dedicatoria

Escribe en esta página a quién dedicas tu trabajo.

*Esta sección es opcional.

Agradecimientos

En caso de considerarse necesario, puede agradecer a personas o instituciones por el apoyo recibido en su trabajo de grado.

*Esta sección es opcional.

Tabla de Contenidos

Resumen

Marco conceptual y contextual

Desarrollo e implementación del aprendizaje

1. Contexto operativo y necesidad del ANS.
2. Estructura del servicio y tipos de infraestructura.
3. Niveles de soporte técnico (estructura del Help Desk).
4. Proceso de gestión de incidencias (flujo operativo).
5. Tipos de mantenimiento dentro del ANS
6. Disponibilidad del servicio
7. Tiempos de respuesta y resolución
8. Tabla 1. Tiempos de atención.
9. Tabla 2. Indicadores de desempeño (KPIs)
10. Gestión de incumplimientos
11. _Gestión_de_Riesgos
12. Plan de contingencia y mitigación de Riesgos

Conclusiones

Referencias

Resumen

El presente informe técnico tiene como objetivo establecer un Acuerdo de Nivel de Servicio (ANS) para la prestación del servicio de soporte técnico y mesa de ayuda, mediante un modelo de outsourcing en la empresa Distrihayder.com. Se definen los niveles de servicio, tiempos de respuesta, tiempos de solución y métricas de desempeño que garantizan la calidad del servicio.Asimismo, se describen los procesos de atención de incidentes, la clasificación por niveles de criticidad y los mecanismos de seguimiento y mejora continua. La implementación de este modelo permite optimizar los recursos tecnológicos, mejorar la experiencia del usuario y asegurar la continuidad operativa.

Finalmente, el informe presenta indicadores clave de desempeño (KPIs) y lineamientos de cumplimiento que permiten evaluar la eficiencia del proveedor del servicio.

Palabras clave: Outsourcing, Help Desk, ANS, SLA, soporte técnico.

Marco conceptual y contextual

El presente informe técnico se desarrolla en el contexto de la gestión y monitoreo de infraestructuras de Tecnologías de la Información (TI), un aspecto fundamental en las

organizaciones modernas debido a la creciente dependencia de los sistemas tecnológicos para la operación de sus procesos.

En este sentido, uno de los conceptos clave es el monitoreo de infraestructuras TI, el cual hace referencia al conjunto de herramientas y prácticas utilizadas para supervisar el estado, rendimiento y disponibilidad de los recursos tecnológicos, como servidores, redes, bases de datos y aplicaciones (Casanova et al., 2020). Este monitoreo permite detectar fallas de manera temprana y garantizar la continuidad del servicio.

Otro concepto relevante es el monitoreo inteligente, el cual incorpora automatización y análisis de datos para generar alertas oportunas, facilitando la toma de decisiones y reduciendo la intervención manual. Este enfoque mejora significativamente la eficiencia en la gestión de incidentes tecnológicos. Asimismo, se aborda el concepto de outsourcing TI, que consiste en la contratación de proveedores externos especializados para la gestión, soporte y monitoreo de los sistemas tecnológicos. Esta estrategia permite a las organizaciones optimizar recursos, reducir costos operativos y acceder a personal altamente capacitado sin necesidad de mantener un equipo interno robusto (Andrade Castro & Mandrillo, 2009).

También se consideran los Acuerdos de Nivel de Servicio (SLA), los cuales establecen los niveles de calidad, disponibilidad y tiempos de respuesta que deben

cumplir los proveedores de servicios tecnológicos, garantizando así un servicio eficiente y confiable (Wu & Buyya, 2010).

En cuanto al contexto, este proyecto se puede aplicar en organizaciones que dependen de infraestructuras tecnológicas para su funcionamiento, como empresas del sector salud, donde la disponibilidad de los sistemas es crítica. En este tipo de entornos, la implementación de un sistema de monitoreo inteligente apoyado en outsourcing permite mejorar la continuidad del servicio, minimizar riesgos y fortalecer la resiliencia tecnológica. De esta manera, el presente trabajo integra los conceptos aprendidos en el área de sistemas para proponer una solución tecnológica que responda a las necesidades actuales de supervisión, control y optimización de infraestructuras TI.

Desarrollo e implementación del aprendizaje

En esta sección se presentan los resultados obtenidos a partir de la aplicación de los conocimientos adquiridos durante el curso, enfocados en la implementación de un sistema de monitoreo inteligente de infraestructuras TI apoyado en outsourcing, dentro de un entorno empresarial simulado de comercio electrónico.

1. Contexto operativo y necesidad del ANS.

En una empresa dedicada a la comercialización de productos a través de internet, la operación depende de manera directa y continua de la infraestructura

tecnológica. Elementos como la plataforma web, los sistemas de pago en línea, las bases de datos de clientes y los sistemas logísticos constituyen el núcleo del negocio digital.

En este tipo de organizaciones, cualquier interrupción del servicio puede generar pérdidas económicas inmediatas, afectar la confianza del cliente y deteriorar la reputación corporativa. Por esta razón, se hace necesario implementar mecanismos que garanticen la continuidad del servicio. En este contexto, la implementación de un Acuerdo de Nivel de Servicio (ANS) resulta fundamental, ya que permite establecer de manera formal los niveles de calidad del servicio, definiendo indicadores medibles como disponibilidad, tiempos de respuesta y resolución de incidentes.(Ramirez, s. f.). Esto facilita una gestión eficiente del soporte técnico y fortalece la relación entre proveedor y cliente.

Dentro del desarrollo del proyecto, el ANS se integra con el sistema de monitoreo inteligente, permitiendo no solo supervisar el estado de la infraestructura en tiempo real, sino también evaluar el cumplimiento de los niveles de servicio establecidos.

2. Estructura del servicio y tipos de infraestructura.

El sistema propuesto se apoya en diferentes modelos de infraestructura tecnológica, los cuales permiten garantizar la operación eficiente del entorno digital.

2.1.1 Software como Servicio (SaaS): En este modelo, las aplicaciones utilizadas por la empresa, como la plataforma de comercio electrónico y el sistema de gestión de pedidos, se encuentran alojadas en la nube y son administradas por proveedores externos (Chávez et al., 2012). Esto permite a la organización acceder a servicios actualizados, con mantenimiento continuo y altos niveles de seguridad, sin necesidad de gestionar directamente la infraestructura. En este caso, el proveedor es responsable de la disponibilidad del software, actualizaciones y protección de la información.

2.1.2 Infraestructura como Servicio (IaaS): Este modelo permite a la empresa utilizar recursos tecnológicos como servidores, almacenamiento y redes en entornos virtualizados(Campos Andia et al., 2016). Dentro del proyecto, el sistema de monitoreo inteligente se integra con estos recursos para supervisar variables como uso de CPU, memoria, almacenamiento y tráfico de red. Esto permite detectar fallas de manera temprana y mejorar la toma de decisiones. Además, este modelo facilita la escalabilidad, permitiendo adaptarse a picos de demanda en momentos críticos como campañas comerciales o temporadas de alto tráfico.

2.1.3 Infraestructura propia o ajena: En algunos escenarios, la empresa puede contar con infraestructura propia o híbrida, donde parte de los servicios se alojan internamente. En estos casos, el ANS debe definir claramente las responsabilidades entre la empresa y el proveedor externo, especialmente en aspectos como energía, conectividad y mantenimiento físico. Esto garantiza una adecuada gestión del servicio y evita conflictos ante posibles fallas.

3. Niveles de soporte técnico (estructura del Help Desk).

Para garantizar una atención eficiente de incidentes, se implementa una estructura de soporte técnico basada en niveles, integrada con el sistema de monitoreo.

3.1.1 Nivel 1 (Soporte inicial): Corresponde al primer punto de contacto con el usuario. En este nivel se reciben las incidencias, se recopila la información necesaria y se realiza una clasificación inicial del problema. Su función principal es resolver incidentes básicos, como fallos de acceso o errores simples, o escalar los casos a niveles superiores cuando se requiere mayor especialización.

3.1.2 Nivel 2 (Soporte especializado): En este nivel se atienden problemas más complejos relacionados con la configuración de sistemas,

fallos en aplicaciones o errores en la infraestructura. El personal de este nivel cuenta con mayor conocimiento técnico y utiliza herramientas de monitoreo para diagnosticar y solucionar incidentes de manera más precisa.

3.1.3 Nivel 3 (Soporte avanzado): Este nivel está compuesto por expertos o proveedores externos (outsourcing), encargados de resolver problemas críticos o estructurales del sistema. Aquí se gestionan fallas complejas que requieren intervención directa en servidores, bases de datos o código del sistema. Este nivel es clave para garantizar la continuidad del servicio y el cumplimiento de los ANS.

4. Proceso de gestión de incidencias (flujo operativo).

El proceso de gestión de incidentes dentro del Help Desk se basa en un modelo estructurado que garantiza la trazabilidad, el control y la eficiencia en la gestión de cada incidente reportado (Masongsong,2016). Durante el desarrollo del proyecto, este proceso se integra con el sistema de monitorización inteligente, lo que permite la detección automatizada de fallos y una resolución optimizada.

Etapas del proceso:

4.1.1 Recepción del incidente: El usuario reporta el problema a través de los canales establecidos, como correo electrónico, plataforma web o sistema de monitoreo automatizado.

4.1.2 Registro en el sistema: Se genera un ticket en el sistema de gestión, donde se documenta toda la información relevante del incidente, incluyendo fecha, descripción y usuario afectado.

4.1.3 Clasificación y priorización: El incidente es analizado para determinar su nivel de impacto y urgencia, clasificándolo como crítico, alto, medio o bajo.

4.1.4 Asignación del incidente: El ticket es asignado al nivel de soporte correspondiente (Nivel 1, 2 o 3), según su complejidad.

4.1.5 Resolución o escalamiento: El incidente es atendido por el personal asignado. En caso de no poder resolverse en ese nivel, se escala a un nivel superior.

4.1.6 Validación con el usuario: Una vez solucionado el problema, se verifica con el usuario que el servicio ha sido restaurado correctamente.

4.1.7 Cierre del ticket: Se documenta la solución final y se cierra el incidente en el sistema. Este flujo permite un control eficiente del

servicio, facilita la medición de tiempos de respuesta y garantiza la calidad en la atención de los usuarios.

5. Tipos de mantenimiento dentro del ANS

El Acuerdo de Nivel de Servicio (ANS) establece diferentes tipos de mantenimiento que garantizan la continuidad y evolución del sistema.

5.1.1 Mantenimiento preventivo: Consiste en la ejecución de actividades periódicas destinadas a evitar fallas antes de que ocurran. Incluye tareas como monitoreo constante, copias de seguridad, actualizaciones de software y revisión de la infraestructura. Este tipo de mantenimiento es fundamental para reducir riesgos y garantizar la estabilidad del sistema.

5.1.2 Mantenimiento correctivo: Se realiza cuando ocurre una falla en el sistema. Su objetivo principal es restaurar el funcionamiento normal en el menor tiempo posible. Incluye la reparación de errores en hardware, software o configuraciones que afectan la operación del servicio.

5.1.3 Mantenimiento evolutivo: Está orientado a la mejora continua del sistema mediante la incorporación de nuevas funcionalidades o adaptaciones según las necesidades del negocio.

Este tipo de mantenimiento permite la innovación, escalabilidad y competitividad de la organización.

6. Disponibilidad del servicio

La disponibilidad del servicio es un indicador crítico dentro del ANS, ya que garantiza la continuidad operativa de la organización. Para su medición, se recomienda incorporar métricas avanzadas como el MTTR (Mean Time to Repair), que representa el tiempo promedio de reparación de fallas, y el MTBF (Mean Time Between Failures), que mide el tiempo promedio entre fallos del sistema. Estos indicadores permiten evaluar con mayor precisión el desempeño del servicio y la confiabilidad de la infraestructura.

7. Tiempos de respuesta y resolución

El Acuerdo de Nivel de Servicio (ANS) establece tiempos específicos de respuesta y resolución para la gestión de incidentes, garantizando un manejo eficiente y oportuno según el nivel de criticidad del problema. Estos tiempos permiten priorizar los recursos disponibles, minimizar el impacto en las operaciones comerciales y asegurar la continuidad del servicio. Para una gestión adecuada, se distinguen dos conceptos clave: el tiempo de respuesta, que es el intervalo entre la notificación del incidente y el inicio de su resolución, y el tiempo de resolución, que se refiere al

período necesario para resolver completamente el incidente y restablecer el servicio. En este contexto, los incidentes se clasifican de la siguiente manera:

7.1.1 Incidentes críticos: Corresponden a fallas que afectan de manera total o significativa la operación del sistema, como la caída de la plataforma principal o la indisponibilidad de servicios esenciales. Estos incidentes requieren atención inmediata, con tiempos de respuesta inferiores a 1 o 2 horas y tiempos de resolución prioritarios, con el objetivo de restablecer el servicio en el menor tiempo posible y reducir el impacto en el negocio.

7.1.2 Incidentes de prioridad alta o normal: Incluyen fallas que afectan parcialmente la operación del sistema o a un grupo específico de usuarios, sin detener completamente el servicio. En estos casos, los tiempos de respuesta pueden ser de hasta 4 horas, mientras que los tiempos de resolución son más amplios, dependiendo de la complejidad del incidente.

Adicionalmente, es recomendable establecer categorías intermedias (media y baja) que permitan una mejor clasificación de los incidentes y una asignación más eficiente de los recursos técnicos. La correcta definición de estos tiempos, junto con su

monitoreo constante, permite evaluar el desempeño del proveedor del servicio, mejorar la calidad de la atención y garantizar el cumplimiento de los niveles de servicio establecidos en el ANS.

Tabla 1. Acuerdo de Nivel de Servicio (ANS).

Nivel de Incidente	**Tiempo de Respuesta**	**Tiempo de Solución**	**Disponibilidad**	**Canal de Atención**
Crítico	≤ 1 hora	≤ 4 horas	99.9%	Teléfono / Web
Alto	≤ 2 horas	≤ 8 horas	99.7%	Web / Correo
Medio	≤ 4 horas	≤ 24 horas	99.5%	Correo
Bajo	≤ 8 horas	≤ 48 horas	99%	Correo

Tabla 2. Indicadores de desempeño (KPIs)

Indicador	Descripción	Fórmula	Meta
Tiempo promedio de respuesta	Tiempo promedio en atender incidentes	Total tiempo respuesta / Nº incidentes	≤ 2 horas
Tiempo promedio de resolución	Tiempo promedio en solucionar incidentes	Total tiempo solución / Nº incidentes	≤ 8 horas
Disponibilidad del servicio	Porcentaje de tiempo operativo	(Tiempo activo / Tiempo total) x 100	≥ 99.5%
Nivel de cumplimiento del ANS	Incidentes atendidos dentro del ANS	(Incidentes cumplidos / Total) x 100	≥ 95%
Satisfacción del usuario	Nivel de satisfacción del cliente	Encuestas	≥ 90%

8. Gestión de incumplimientos

El ANS establece mecanismos de control en caso de incumplimiento de los niveles de servicio acordados.

En estos casos, se aplican medidas de compensación como descuentos o créditos en el servicio, proporcionales al impacto generado por la falla. Esto garantiza el compromiso del proveedor y protege los intereses de la empresa contratante.

9. Seguridad y control del servicio

El servicio debe garantizar la protección de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos (ISO/IEC, 2022). Para ello, se implementan controles de acceso, mecanismos de autenticación y sistemas de monitoreo continuo que permiten detectar incidentes de seguridad de manera temprana. Este aspecto es fundamental en entornos digitales, donde la información es un activo crítico.

10. Mejora continua del servicio

El ANS incorpora un enfoque de mejora continua, basado en el análisis constante de incidentes y el rendimiento del servicio (Medina Cárdenas et al., 2017). Mediante este proceso, se identifican fallos recurrentes, se implementan acciones correctivas y se optimizan los procesos de prestación del servicio. Esto

permite mantener altos niveles de calidad, adaptarse a las necesidades del negocio y fortalecer la eficiencia operativa del sistema.

11. Gestión de Riesgos

La implementación de un modelo de outsourcing en servicios de Tecnologías de la Información (TI) implica diversos riesgos que pueden afectar la calidad del servicio y la continuidad operativa de la organización. Por esta razón, es fundamental identificar, analizar y gestionar dichos riesgos de manera oportuna.

Uno de los principales riesgos es la dependencia del proveedor externo, ya que la organización delega funciones críticas, lo que puede generar vulnerabilidad ante incumplimientos o fallas en el servicio. Asimismo, existe el riesgo de incumplimiento de los niveles de servicio establecidos en el ANS, lo cual puede afectar la disponibilidad y el desempeño del sistema.

Otro riesgo relevante es la seguridad de la información, debido a la posible exposición de datos sensibles durante la gestión del servicio, lo que podría comprometer la confidencialidad e integridad de la información. Además, se deben considerar riesgos operativos como fallas en la infraestructura tecnológica, interrupciones del servicio y errores humanos en la gestión de incidencias.

La adecuada gestión de estos riesgos permite anticipar posibles fallas, reducir su impacto y garantizar la estabilidad del servicio.

12. Plan de contingencia y mitigación de Riesgos

Con el fin de mitigar los riesgos identificados y garantizar la continuidad del servicio, se establece un plan de contingencia que define las acciones a seguir en caso de incidentes críticos o fallas en la operación (Cusick, 2017)..

En primer lugar, se implementan estrategias de respaldo de información (backups) periódicos, que permiten recuperar los datos en caso de pérdida o corrupción. Asimismo, se establecen mecanismos de recuperación ante desastres (Disaster Recovery Plan - DRP), que permiten restablecer el servicio en el menor tiempo posible ante fallas graves.

Adicionalmente, se recomienda contar con proveedores alternos o planes de soporte adicional, con el fin de reducir la dependencia de un único proveedor. También se definen protocolos de actuación ante incidentes críticos, los cuales incluyen procedimientos claros para la identificación, escalamiento y solución de fallas.

Por otra parte, se implementan medidas de seguridad como controles de acceso, cifrado de datos y monitoreo continuo, con el objetivo de proteger la información y prevenir incidentes de seguridad.

Finalmente, el plan de contingencia debe ser evaluado y actualizado de manera periódica, garantizando su efectividad y adaptación a las necesidades del entorno tecnológico.

Conclusiones

El desarrollo de este trabajo permitió la aplicación práctica de conceptos relacionados con la gestión de servicios de TI y el modelo de externalización, destacando la importancia de establecer Acuerdos de Nivel de Servicio (ANS) claros y medibles dentro de una organización.

Se concluye que la implementación de un modelo de soporte técnico basado en la externalización ofrece beneficios significativos, como la optimización de recursos, la reducción de costos operativos y el acceso a personal especializado, lo que mejora la eficiencia en la gestión de incidentes y la continuidad del servicio.

Además, el uso de Indicadores Clave de Rendimiento (KPIs) permite monitorear la calidad del servicio y tomar decisiones basadas en datos, fortaleciendo los procesos de mejora continua y asegurando el cumplimiento de los niveles de servicio establecidos.

Sin embargo, también se identifican riesgos asociados con este modelo, como la dependencia del proveedor externo, posibles incumplimientos de los ANS y la necesidad

de una supervisión adecuada del servicio. Por lo tanto, es esencial establecer mecanismos de control, monitoreo y penalización en caso de fallas.

En general, el ejercicio nos permitió comprender la importancia de integrar herramientas tecnológicas, monitoreo inteligente y buenas prácticas de gestión para garantizar un servicio eficiente, seguro y alineado con las necesidades del negocio.

Referencias

Andrade Castro, J. A., & Mandrillo, C. (2009). El outsourcing de los sistemas de información en las organizaciones públicas. *Revista Venezolana de Gerencia, 9*(28). https://doi.org/10.31876/revista.v9i28.9796

Campos Andia, O. K., Correa Lerzundi, J. M., & Zevallos Duran, G. (2016). Implementar un sistema de infraestructura como servicio (IaaS) en cloud computing que sirva de alojamiento al ERP en una empresa comercial. Universidad Peruana de Ciencias Aplicadas (UPC). https://doi.org/10.13140/RG.2.1.2443.1120

Casanova, M. P., & Calderón, C. A. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. TecnoLógicas, 23(48), 32–54. https://doi.org/10.22430/22565337.1449

Medina Cárdenas, Y., Areniz Arévalo, Y., & Rico Bautista, D. W. (2017). Alineación estratégica bajo un enfoque organizacional de gestión tecnológica: ITIL & ISO 20000. *Tecnura, 20*(Edición especial). https://doi.org/10.14483/22487638.11681

Chávez, S. B., Martín, A. E., Rodríguez, N. R., Murazzo, M. A., & Valenzuela, A. (2012). Metodología ágil para el desarrollo SaaS. XIV Workshop de Investigadores en Ciencias de la Computación. http://sedici.unlp.edu.ar/handle/10915/18977

Masongsong, R. P., & Damian, M. A. E. (2016). Help desk management system.

Ramírez, M. V. V. (s. f.). Los acuerdos de nivel de servicio (ANS) como elementos generadores de competitividad organizacional.

Wu, L., & Buyya, R. (2010). Service level agreement (SLA) in utility computing systems. Future Generation Computer Systems. https://arxiv.org/abs/1010.2881

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

Cusick, J. J. (2017). Achieving and managing availability SLAs with ITIL-driven processes. arXiv. https://arxiv.org/abs/1705.04906