UNIVERSIDAD ESTATAL A DISTANCIA

ESCUELA DE CIENCIAS DE LA ADMINISTRACIÓN

CÁTEDRA DE ADMINISTRACIÓN

Asignatura: PRINCIPIOS DE ADMINISTRACION

Código: 004038 **Créditos: 3**

Centro Universitario: San Vito

Grupo: 01

Nombre Completo: Francisco Campos Sandí

Número de cédula:114750560

III Cuatrimestre

Contenido

1. **Hechos Relevantes** 3
2. **Problema central** 4
3. **Análisis del problema central** 5
4. **Alternativas de solución** 6
5. **Solución, Instrumentalización y Recomendaciones** 7
6. **Recomendaciones** 8

1. Hechos Relevantes

a. La empresa "Seguridad Inteligente" brinda servicios de alta calidad a grandes empresas y garantiza la seguridad de los datos que resguardan.
b. Los informes de auditoría señalan que los productos no cumplen con las necesidades y preferencias de los clientes.
c. Al contratar personal joven con poca capacitación acorde a la empresa con necesidades técnicas esenciales para brindar servicios de gran calidad a los clientes.
d. La empresa ha realizado despidos y contrataciones de personal profesional.
e. La falta de credibilidad generada por clientes al contratar personal con escasa preparación técnica en el manejo de datos por parte de la empresa repercute en la filtración de datos confidenciales de la empresa que contrata los servicios en el manejo de datos y queda vulnerable.
f. La implementación de una versión gemela del sistema para brindar una solución rápida a los problemas provocados por la falta de preparación de la empresa es meramente insuficiente y la ciberseguridad es comprometida con ataques a los clientes.
g. La responsabilidad legal por parte de la empresa "Seguridad Inteligente" genera pérdidas económicas significativas debido a los incumplimientos de las cláusulas del contrato.
h. La falta de personal bien capacitado en temas de ciberseguridad y el manejo de datos pueden tener consecuencias legales para la empresa en temas contractuales.

2. Problema central

¿Qué medidas puede tomar “Seguridad Inteligente” que permita resolver de manera efectiva los problemas de insatisfacción de los clientes y los desafíos operativos que enfrenta?

3. Análisis del problema central

El problema central radica en la insatisfacción de los clientes de "Seguridad Inteligente," lo cual ha desencadenado una serie de complicaciones tanto en la operación como en la salud financiera de la empresa. Para abordar esta problemática de manera efectiva, es necesario realizar varias acciones clave:

La empresa debe de mejorar significativamente la calidad de los productos y servicios que ofrecen en el mercado. La insatisfacción de los clientes da a conocer las deficiencias en dichas áreas, lo que exige una revisión exhaustiva de los métodos usados en la recopilación y análisis de datos utilizando Big Data.

Además, es imperativo proporcionar capacitación adecuada al nuevo personal. Estos empleados necesitan adquirir habilidades técnicas y conocimientos especializados en la gestión de datos y Big Data. Así, la empresa debe establecer un sólido sistema de soporte técnico para garantizar un rendimiento óptimo y una resolución eficiente de problemas.

La gestión de datos debe ser eficaz para evitar errores en la recolección y el manejo de información sensible de los clientes. Esto implica la implementación de procedimientos en el control de calidad y la realización de auditorías regulares para mantener la integridad y la confidencialidad de los datos.

La vulnerabilidad de la empresa ante posibles ataques cibernéticos debe ser resuelta con rapidez. Esto involucra la implementación de medidas de seguridad sólidas, como firewalls y sistemas de detección de intrusos, así como la formación continua del personal en el tema de ciberseguridad.

El cumplimiento de todas las cláusulas en los contratos es esencial para evitar pérdidas financieras y mantener la reputación de la empresa. Además de las capacitaciones para el personal del cliente, conforme a lo establecido en los acuerdos, así ayudará a prevenir posibles demandas en temas legales y reducir las posibles pérdidas financieras significativas.

Por último, la implementación de una versión gemela del sistema debe ser revisada minuciosamente para garantizar la protección contra vulnerabilidades y errores que puedan comprometer la seguridad de los datos y la satisfacción del cliente.

4. Alternativas de solución

Alternativa	Ventaja	desventaja
Implementar capaciones técnicas en el tema de ciberseguridad y manejo de datos.	i. Se mejora las habilidades técnicas del personal en temas de ciberseguridad. ii. Manejo de datos de forma eficiente y ágil para la toma de decisiones. ii. Aumenta el grado de satisfacción de los clientes. iv. Reduce errores futuros por desconocimiento en el manejo de sistemas con información confidencial.	i. Se debe de requerir tiempo e inversión significativa para las capacitaciones constantes. ii. En algunos casos puede haber rechazo al cambio por parte del personal al recibir las capacitaciones. iii. Las soluciones son a largo plazo dado que se debe tener mucha capacitación para cubrir muchas necesidades en el ámbito de ciberseguridad y el manejo de datos. iv. No garantiza un 100% libre de errores
Reevaluación y mejora de la calidad en temas de ciberseguridad	i. Reduce perdidas futuras por mal manejo de sistemas o filtraciones de datos. ii. Mejora la reputación de la empresa en los productos o servicios que ofrece y puede atraer nuevos clientes. iii. Al estar reevaluando la calidad se pueden ofrecer nuevos productos para atraer nuevos clientes. iv. Se ofrecen servicios de mayor calidad que podrá permitir a la empresa cobrar precios más altos y así aumentar sus ingresos.	i. Atrasos en la capacitación del personal y la Seguridad Cibernética ii. Se debe de contratar nuevo personal que sustituya a los que están capacitándose iii. Las capacitaciones constantes pueden ser un proceso complejo y demandar mucho tiempo. iv. Al incrementar precios se pueden perder futuros clientes.

5. Solución, Instrumentalización y Recomendaciones

Solución: Implementar capaciones técnicas en el tema de ciberseguridad y manejo de datos.

Justificar: Esta alternativa aborda directamente las causas fundamentales de los problemas, que son la falta de habilidades del personal y la vulnerabilidad cibernética. La capacitación mejora la competencia del personal, mientras que el fortalecimiento de la seguridad cibernética protege los datos y la reputación de la empresa**.**

Instrumentalización

Quién	Cómo	cuándo
El departamento de Recursos Humanos y el equipo de (tecnologías de la información) TI son los responsables de implementar esta alternativa.	La capacitación se llevará a cabo mediante programas específicos para el personal nuevo, impartidos por expertos internos o externos. La seguridad cibernética se mejorará con la evaluación de vulnerabilidades y la implementación de medidas de seguridad avanzadas.	La capacitación debe comenzar de inmediato y continuar a medida que se incorporen nuevos empleados. Las medidas de seguridad cibernética deben implementarse progresivamente en un plazo de tres meses.

Solución: Reevaluación y mejora de la calidad en temas de ciberseguridad

Justificar: Esta alternativa se enfoca en abordar directamente la insatisfacción del cliente al mejorar la calidad de los productos y servicios. La revisión permitirá identificar áreas de mejora, y las mejoras aumentarán la satisfacción del cliente y el potencial de ingresos de la empresa.

Instrumentalización

Quién	Cómo	cuándo
El equipo de gestión y el departamento de análisis de datos son los responsables de esta alternativa.	La reevaluación implica una evaluación integral de los procesos de recolección y análisis de datos. Las mejoras se implementarán progresivamente y pueden incluir la adopción de herramientas avanzadas de análisis de datos.	La reevaluación debe comenzar de inmediato y completarse con las mejoras en un plazo de un año.

6. Recomendaciones

1. Establecer medidas sólidas de seguridad cibernética, como firewalls, sistemas de detección de intrusiones y políticas de autenticación seguras para proteger los datos de los clientes.

2. El equipo de gestión debe llevar a cabo una revisión integral de los procesos de recolección y análisis de datos para identificar áreas de mejora y optimización.

3. Implementar mecanismos de evaluación de los servicios o productos que se ofrecen a los clientes para futuras mejoras.

4. Verificar el cumplimiento de todas las cláusulas de los contratos, incluida la capacitación del personal del cliente, para evitar litigios y pérdidas financieras.

5. Mantener una comunicación abierta y transparente con los clientes afectados por los problemas y brindarles información sobre las medidas tomadas para resolver los inconvenientes.

6. Motivación en constantes en los empleados para obtener mejores resultados en temas de capacitación.